Die Chiffriermaschine ENIGMA

Trügerische Sicherheit

Ein Beitrag zur Geschichte der Nachrichtendienste

Vom Fachbereich Mathematik und Informatik

der Technischen Universität Carolo-Wilhelmina

zu Braunschweig

zur Erlangung des Grades eines

Doktors der Naturwissenschaften

(Dr.rer.nat.)

genehmigte

D i s s e r t a t i o n

Von Heinz Ulbricht, Dipl.-Math.
aus Dresden-Loschwitz

1. Referent: Prof. Dr. T. Sonar

2. Referent: Prof. Dr. H. Hischer

3. Referent: Prof. Dr. F.L. Bauer

eingereicht am: 8. 2. 2005

mündliche Prüfung (Disputation) am: 14. 4. 2005

2005

Vorwort

Diese Arbeit wurde von Herrn Professor Dr. H. Homuth, Universität der Bundeswehr, Hamburg, angeregt und bis zu seinem Tode wohlwollend begleitet. Es sollte zusammengefasst und z.T. mittels Computer-Simulation „nachgespielt“ werden, mit welchen Methoden und auf welchen Wegen die deutsche Chiffriermaschine ENIGMA von der Mitte der 20er Jahre ab trotz ständiger Verbesserung der Chiffrierverfahren ihrer Geheimnisse entkleidet wurde.[1] Nicht beabsichtigt war eine Serie von Darstellungen der Erfolge der Alliierten in den Kämpfen, die durch die Kenntnis der deutschen Funksprüche ermöglicht worden waren. Dazu gibt es bereits zusammenfassende Werke genug.

Notwendig war hierbei auch die Darstellung von Schlüsseln, die nicht auf der ENIGMA beruhten, weil bei ihnen gewonnene Erkenntnisse halfen, die mit der ENIGMA chiffrierten Sprüche zu lesen.

Die hier vorliegende Darstellung wurde wesentlich gefördert durch das freundliche Entgegenkommen von Sammlungen und Archiven, z.B. dem Deutschen Museum München, dem Forsvarsmuseet Oslo - hier besonders Herrn Professor Ulvensoen -, dem Bundesarchiv/Militärarchiv (BA/MA), dem Militärischen Forschungsamt, dem Schweizerischen Bundesarchiv, der Heeresnachrichtenschule in Feldafing, der Marinefernmeldeschule in Flensburg sowie der Bibliothek für Zeitgeschichte in Stuttgart. Dank darf ich anfügen an die Herren G. Bloch (Paris), Dipl.-Ing. Mache, Dr. Niedermeyer, Professor Dr. Rohwer, Dr. Schomburg, Mr. Alan Stripp (Cambridge), Mr. Erskine für intensiven Gedankenaustausch, Mr. Hamer und Mr. Weierud, um nur die wichtigsten zu nennen. Ganz besonderer Dank gebührt Herrn Professor Dr. F.L. Bauer für seine intensive Betreuung dieser Arbeit. Verzichtet wurde auch auf Einzelbeschreibungen von kryptologischen Standardmethoden und -Geräten, wie sie z.B. bei Jensen dargestellt sind.[2] Die bei ROHRBACH aufgelisteten Druckschriften[3] sind leider noch als „Geheim“ eingestuft und somit unzugänglich. Ähnlich übertriebene Geheimhaltung wird auch noch seitens der ehemaligen Alliierten der Jahre 1939 bis 1945 geübt[4], sodass manche Ergänzungen bzw. sogar Berichtigungen, im Laufe der Zeit nötig werden dürften.

Herrn Professor Dr. Hischer bin ich besonders zu Dank verpflichtet, weil er mich ermuntert hat, diese Arbeit als Dissertation einzureichen.

Zum Schluss gilt mein Dank meiner Frau, die durch viele Monate manchen Verzicht geleistet hat.

[1] BLOCH a)

[2] JENSEN, S. 45 ff. der Zusammenfassung aus der von Dipl.-Ing. Willi Jensen als Doktor-Dissertation eingereichten Arbeit „Hilfsgeräte der Kryptographie“. (Die Arbeit soll zurückgezogen worden sein.). Mr. B. Randell gilt mein Dank für die Überlassung einer Fotokopie dieser Arbeit, die in der Handschriften-Abteilung der Bayerischen Staatsbibliothek, München, (Signatur Cgm 9303) aufbewahrt wird.

[3] ROHRBACH, S. 257

[4] z.B. bei COWAN: GCHQ, An official history of Bletchley Park

Inhaltsverzeichnis

Kapitel 1

Chiffrierverfahren

1.1 Enigma-Versionen

Die zwischen 1926 und 1945 von der deutschen Wehrmacht (und anderen Organisationen) verwendete Chiffriermaschine („Schlüsselmaschine“) ENIGMA wurde als Walzenmaschine von SCHERBIUS entwickelt. SCHERBIUS hatte am 23. 2. 1918 ein Patent für eine elektrische Chiffriermaschine angemeldet, das Patent wurde im Februar 1923 erteilt.
Der zu chiffrierende Text wurde über eine Schreibmaschinen-Tastatur eingegeben. Der eigentliche Chiffrierteil bestand aus Durchgangsrädern (Walzen, „Rotoren“), deren auf jeder der beiden Endflächen kreisförmig entlang des Umfangs angeordneten Kontakte der Eingangsseite mit denen der Ausgangsseite wie regellos verbunden waren; die so entstehende Permutation bildete einen geordneten Zeichensatz. Die inneren Verbindungen, die Verdrahtungen der Walzen, waren geheim. Die rechtsseitigen Eingangskontakte der Chiffrierwalzen bestanden aus Kontaktstiften und waren den Buchstaben A ... Z zugeordnet. Auf der Ausgangsseite links waren Kontaktflächen angebracht. In der Patentanmeldung wies SCHERBIUS bereits darauf hin, dass durch Hintereinanderschalten mehrerer solcher Rotoren die Anzahl der erreichbaren Permutationen - und damit die Sicherheit - vergrössert werden könnte. Bei einem Zeichenvorrat Z je Rotor und n Rotoren wären das Z^n Permutationen.
Im April 1918 hatte er die Maschine dem Reichs-Marineamt angeboten, das lehnte die Übernahme ab, ebenso das Auswärtige Amt. Beim Angebot an die Marine war SCHERBIUS von 10 Rotoren mit $Z = 25$ (Alphabet ohne J) ausgegangen[1]. SCHERBIUS war damals mit der Firma Gewerkschaft Securitas, später mit der Firma Chiffriermaschinen AG verbunden.

1.1.1 Modell A.

Ein frühes Modell A, hergestellt von der Firma Gewerkschaft Securitas in Berlin, besass 4 Walzen, die nicht austauschbar waren. Die Walzen drehten sich bei jedem Chiffrierschritt auf einer gemeinsamen Achse unregelmässig um verschiedene Winkel. Drei Walzen drehten in derselben Richtung, die vierte umgekehrt mit einer Art Rückkopplung in die Bewegungen der ersten drei Walzen[2]. Eine erste Version wurde von SCHERBIUS 1924 in Bern vorgestellt, beim Kongress der Internationalen Postunion 1924 offiziell vorgeführt.

Jede der vier Walzen besass längs des Umfanges 28 Kontakte (Alphabet, dazu Ä,Ö,Ü, aber ohne X). Die einstellbare Anfangsstellung jeder der vier Walzen, wie sie in einem Fenster über der jeweiligen Walze sichtbar war, stellte den Schlüssel dar. Es wurden acht Buchstaben benötigt, vier für das Chiffrieren, vier für das Dechiffrieren. Eine entscheidende Erschwerung für unbefugte Dechiffrierung war durch die beim Chiffrieren entstehende Gleichverteilung der Buchstaben

[1] KAHN a)
[2] KRÖNCKE, dort auch eine Abb. der ENIGMA A; ROHWER a), S. 231

gegeben, die einen Rückschluss auf den Klartext über die normale Häufigkeitsverteilung eines Alphabets ausschloss. Zudem war die Periode der Chiffrierung so immens gross, dass die bis dahin bekannten Verfahren zur Lösung periodischer Schlüssel bei gebührender Vorsicht versagen mussten. Das Ergebnis der Chiffrierung/Dechiffrierung wurde auf eine Schreibvorrichtung (Schreibmaschine mit Typenrad) übertragen. Man konnte nach dem Einschalten des Antriebsmotors wie auf einer Schreibmaschine schreiben, der geschriebene Text war dann sofort der Geheimtext.[3] Der Antrieb der Rotoren erfolgte nach eingestellter (Anfangs-) Grundstellung mittels Zahnrädern wie bei einem Zählwerk: Nach jeder vollen Umdrehung des Rotors wurde der links benachbarte um einen Zahn weitergedreht. Die vier Antriebsräder hatten Lücken (5 Zähne und 6 Lücken; 9 Zähne und 6 Lücken; 11 Zähne und 6 bzw. 8 Lücken).[4]
Die ersten Veröffentlichungen über diese Chiffriermaschine stammten von 1923[5] Im Mai 1924 wurde in der Zeitschrift „Der Funker" in Heft 5 auf Seite 83 in einem Inserat die ENIGMA A von der Chiffriermaschinen-Aktiengesellschaft zum Kauf angeboten.

1.1.2 Modell B.

1924 wurde auch die ENIGMA B vorgestellt: Sie war ebenfalls mit einer Schreibvorrichtung (Typenhebel) ausgestattet. Das Tastenfeld enthielt 57 Tasten, darunter Umschalttasten, die Gross- und Kleinschreibung ermöglichten für insgesamt 83 Schriftzeichen. Die Chiffrierwalzen waren untereinander austauschbar und wurden über Zahnräder wie bei der ENIGMA A bewegt.
Als Schlüssel mussten 8 Buchstaben eingestellt werden: 4 aus A $\cdots$ Z, 1 aus A $\cdots$ K, 1 aus A $\cdots$ O, 1 aus A $\cdots$ Q und 1 aus A $\cdots$ S. Die Chiffrierwalzen waren untereinander austauschbar, Bei den Modellen A und B war der Ausgang der linken Chiffrierwalze über eine Ausgangswalze mit der Ergebnisanzeige verbunden.

1.1.3 Modell C.

Das Modell ENIGMA C brachte einige entscheidende Neuerungen. Die Schreibvorrichtung entfiel, dafür wiurde das Ergebnis über ein Glühlampenfeld angezeigt. Die Anordnung der Buchstaben im Glühlampenfeld entsprach dem Tastenfeld. (Daher die englische Bezeichnung «Glowlamp Enigma»).

1.1.4 Umkehrwalze.

SCHERBIUS' Mitarbeiter KORN brachte als Neuerung statt der vierten Walze eine nicht bewegte Umkehrwalze an mit Kontakten nur auf einer Seitenfläche, die paarweise miteinander verbunden waren.
Diese Umkehrwalze führte dazu, dass die Maschine sowohl zum Chiffrieren als auch zum Dechiffrieren mit derselben Anfangsstellung benutzt werden konnte. Der Vorteil schien darin zu bestehen, dass man jede Walze doppelt nutzen konnte. Der Schlüssel bestand also nur noch aus drei Buchstaben. Dadurch entstand die Selbstreziprozität der Maschine (d.h. wenn in einem Chiffrierschritt zum Klarbuchstaben `g` der Geheimbuchstabe `W` gehörte, dann war in diesem Schritt ebenso dem Klarbuchstaben `w` der Geheimbuchstabe `G` zugeordnet - gleichzeitig bedeutete das, dass niemals ein Klarelement und sein zugeordnetes Geheimelement gleich sein konnten.) Die Selbstreziprozität sollte sich jedoch als Eigenschaft herausstellen, der der Sicherheit der Chiffrierung abträglich war, weil damit die mögliche Lage eines vermuteten Klartextes im Geheimtext eingegrenzt werden

[3] KRUH/DEAVOURS b)
[4] Die unregelmässige Fortschaltung der Walzen geht auf ein Patent von DAMM (10.10.1919 !) zurück.
[5] Fritz HANSEN: „Die Chiffriermaschine" in: Der Radio-Amateur, Nov.1923, Heft 4, S. 76 -78; SCHERBIUS: Ein Aufsatz in der Zeitschrift für Fernmeldetechnik, Heft 7, 1923.

konnte. Diese Umkehrwalze konnte nur in zwei festen Stellungen, um 180 Grad versetzt, eingesetzt werden[6]. Die Umkehrwalze war bei geschlossener Maschine von aussen nicht sichtbar. Das Tastenfeld war nach dem Alphabet ausgerichtet: Die oberste Reihe A bis I, die zweite J bis Q, die dritte R bis Z.

Die drei Chiffrierwalzen waren untereinander austauschbar.

1.1.5 Walzenring

Ein anderer Mitarbeiter, BERNSTEIN, führte einen um den Umfang der Walze gelegten drehbaren „Schlüsselring“ ein[7]. Auf diesem Ring waren Zahlen oder Buchstaben eingraviert. Er konnte durch eine am Walzenkörper angebrachte Blattfeder, die mit einem Stift in Bohrungen des Schlüsselrings eingriff, in beliebiger Stellung gehalten werden. Der im Fenster über jeder Walze sichtbare Buchstabe war nun nicht mehr in jedem Falle der durch die Stellung des Walzenkörpers gegebene. Die Lage des Ringes jeder der vier Walzen wurde somit zum Bestandteil des Schlüssels.

Die Chiffrierwalzen und auch die Umkehrwalze sassen auf einer gemeinsamen Achse. Walzen und Umkehrwalze wurden so aneinander und gegen die Eingangswalze mit 26 Kontakten gepresst, dass von einem Eingangskontakt der ersten Walze, die vom Bediener aus gesehen rechts lag, Stromfluss durch alle drei Walzen, durch die Umkehrwalze und wieder – in umgekehrter Reihenfolge – durch die drei Walzen zurück möglich war.
Die Weiterschaltung der Walzen erfolgte mittels Schubhebeln, die in Kerben an den Walzen eigreifen konnten.
Beim Drücken der Taste eines Klarbuchstabens rückte zunächst die erste Walze um einen Schritt weiter, dann wurde der Stromkreis geschlossen vom Kontakt der Eingangswalze, der zum Klarbuchstaben gehörte, über Eingangs- und Ausgangskontakt der 1. Walze, von da zu dem anliegenden Eingangskontakt der 2. Walze, vom zugeordneten Ausgangskontakt zum anliegenden Eingangskontakt der 3. Walze, von dessen zugeordnetem Ausgangskontakt zur Umkehrwalze und von deren Ausgang durch die Walzen 3, 2 und 1 zurück und über die Eingangswalze zum Glühlampenfeld. Dort leuchtete nun der die Substitution des Klarbuchstabens darstellende Geheimbuchstabe auf. Da die erste Walze bei jedem Tastendruck weiterrückte, die zweite ,wenn die erste eine volle Umdrehung gemacht hatte und die dritte nach einer vollen Umdrehung der zweiten, ergab sich jedesmal eine andere Substitution. Auf diese Weise wurde eine polyalphabetische Substitution mit sehr hoher Periode erzeugt. Infolge einer konstruktiven Besonderheit rückte die zweite Walze nach ihrem Rücken noch einmal weiter[8], die Periode war also $26 \cdot 25 \cdot 26 = 16900$.

In jeder einzelnen Walzenstellung war die Permutation also eine Involution, ein Produkt von 13 Zweierzyklen.

Mit dem Körper jeder Chiffrierwalze war fest verbunden

> ein Zahnkranz rechts, in den beim Niederdrücken einer Taste des Tastenfeldes ein Schubhebel eingreifen konnte, der die Walze um eine Position weiterdrehte,
>
> ein Stellrad von grösserem Durchmesser als der Walzenkörper, mit gekerbtem Umfang, in dessen Kerbe ein Rasthebel eingriff. Bei geschlossenem Deckel ragten diese Stellräder durch Schlitze aus dem Gehäuse der Maschine und erlaubten, die Stellung der Walzen zu verändern, wobei deren Position in einem Fenster links von dem jeweiligen Schlitz an der Zahl oder dem Buchstaben des Schlüsselrings erkennbar war,
>
> eine „Sperrscheibe“ mit einer Kerbe, links, die bewirkte, dass eine Chiffrierwalze erst dann durch Eingriff des zugehörigen Schubhebels um einen Schritt weitergedreht werden konnte, wenn der Schubhebel in die Kerbe der rechts von ihr stehende Walze eingreifen konnte. Das trat jeweils nach einer vollen Umdrehung der rechts stehenden Walze ein. Das Weiterrücken wurde vom Körper der Walzen aus gesteuert.

[6] TÜRKEL, S.85
[7] KAHN a), S. 37
[8] HAMER, auch DEAVOURS–KRUH a), S.95

Hinter den Schubhebeln lagen die unter Federzug stehenden Rasthebel, die mit Rollen in die Aussparungen der Stellräder eingriffen und sicherstellten, dass das Fortschreiten der Walzen nur schrittweise erfolgte.

Die Tastatur war mit 26 Kontakten auf einer zylindrischen Kunststoffscheibe (Eingangswalze) verbunden, die die elektrischen Verbindungen zur rechten der drei Chiffrierwalzen herstellte. Die Verdrahtung von der Tastatur aus war direkt, d.h. in der Reihenfolge der Tastatur waren die Verbindungen zu den Kontakten der Eingangswalze gelegt. (A zu Kontakt 1, B zu Kontakt 2, C zu Kontakt 3 usw.)

1.1.6 Funkschlüssel C.

Für die Reichsmarine wurde ab 1925 eine militärische Testversion des Modells C produziert.

Ihr Aufbau: Das Tastenfeld war in drei Reihen nicht wie bei einer Schreibmaschine, sondern alphabetisch angeordnet, durch die Hinzunahme der Umlaute `Ä`, `Ö` und `Ü`, also mit 29 Tasten. Die Umlaute waren nötig, weil die Funksprüche vor dem Chiffrieren mit der Chiffriermaschine mit Hilfe eines Kenngruppenbuches in Vierergruppen codiert wurden, die auch Umlaute enthielten.

In die Maschine konnten jeweils drei von fünf verfügbaren Walzen eingesetzt werden. Die Ringe dieser Walzen (von I bis V) waren mit Buchstaben `A` bis `Z`, `Ä`, `Ü`, mit den Zahlen 01 bis 28, 29 bis 56, 57 bis 84 und mit Buchstabenpaaren gekennzeichnet. An den Ringen konnte man so die Walzen unterscheiden. Wie beim zivilen Modell C war die Sperrscheibe mit dem Walzenkörper fest verbunden. Die Umkehrwalze bewegte sich nicht. Sie konnte jedoch in vier verschiedenen Positionen (Alpha, Beta, Gamma, Delta) eingesetzt werden.

Der Stromweg war von der Taste `X` unter Umgehung der Walzen direkt zur Glühlampe des Buchstabens `X` geschaltet. Daher durchliefen nur die Stromwege von 28 Buchstaben die Walzen. Somit bestand jeder Chiffrierschritt wegen der Umkehrwalze aus einem von 14 Zweierzyklen. Zum Ablesen der Chiffrierergebnisse diente ein Glühlampenfeld mit 29 Glühlampenfenstern.

Diese ENIGMA-Version wurde im Februar 1926 als „Funkschlüssel C“ bei der Marine eingeführt[9].

1.1.7 Modell D.

Es ist noch das Modell D zu erwähnen, bei dem die Umkehrwalze in 26 verschiedenen Stellungen eingesetzt werden konnte.[10]. Weil auch die Stellung der Umkehrwalze, die im übrigen verdrehbar war, aber beim Tasten nicht weitergeschaltet wurde, in einem Fenster sichtbar war, sprechen einige Autoren davon, dass diese Version eine Maschine mit vier Walzen gewesen sei. Die Tastatur war, bis auf die Lage des Buchstaben `P`, die einer normalen Schreibmaschine. Bei der der Eingangswalze führte nun `Q` zum Kontakt #1, `W` zum Kontakt #2, `E` zum Kontakt #3 usw.

Die Eingangswalze repräsentierte also die Permutation

$$\begin{pmatrix} q\ w\ e\ r\ t\ z\ u\ i\ o\ a\ s\ d\ f\ g\ h\ j\ k\ p\ y\ x\ c\ v\ b\ n\ m\ l \\ a\ b\ c\ d\ e\ f\ g\ h\ i\ j\ k\ l\ m\ n\ o\ p\ q\ r\ s\ t\ u\ v\ w\ x\ y\ z \end{pmatrix}$$

Als Besonderheit wurde im Zusammenhang mit dieser Maschine in einem Werksprospekt (ohne Datumsangabe) der sog. Influenzbuchstabe erwähnt. Wenn er gedrückt wurde, musste der die Maschine Bedienende die Umkehrwalze um einen Schritt nach vorn drehen (z.B. von `G` auf `F`). Dadurch änderte sich die Periode, abhängig von der Häufigkeit des frei gewählten Buchstabens im Text.

Derselbe Werksprospekt gibt an, dass die Tasten der obersten Reihe auch Ziffern aufweisen konnten.

Ein wesentlicher Unterschied war, dass die Steuerung der Weiterschaltung der benachbarten Walzen nun von dem Walzenring übernommen wurde, mit dem die Sperrscheibe fest verbunden war.

---

[9] DER FUNKSCHLÜSSEL C; Die hier gemachten Angaben beruhen aber auf Deckblättern unbekannten Datums

[10] TÜRKEL, S. 88

1.1.8 ENIGMA K.

Aus der ENIGMA D ist die auch an die Schweizer Chiffrierdienste verkaufte ENIGMA K abgeleitet. Eine „Analyse der Chiffriermaschine ENIGMA K“ (Verfasser und Datum unbekannt)[11] kommt zu dem Schluss, dass diese Maschine Sicherheitsanforderungen nicht gerecht wird. Um solche zu erreichen, müssten einige Forderungen erhoben werden

1) die regelmässige Weiterschaltung der Walzen müsste einstellbar unregelmässig werden
2) Die Verbindungen der Umkehrwalze müssten leicht veränderbar sein
3) Das Alphabet der Eingangswalze müsste durch Steckerverbindungen zwischen Tastatur und dem Walzeneingang veränderlich sein
4) Die Selbstreziprozität bei der Chiffrierung müsste wegfallen.

Eine ENIGMA ohne Stecker mit stellbarer Umkehrwalze, deren Tastatur auch Ziffern enthielt (ENIGMA K), benutzten auch die Schweizer Flieger- und Fliegerabwehrtruppen und andere Schweizer Dienststellen, nachgewiesen ab 1941[12].

1.1.9 ENIGMA G.

Beim Heer wurde am 15.7.1928 eine Chiffriermaschine mit Namen „ENIGMA G mit Stöpselstellung“ eingeführt.
Es gab eine Dienstvorschrift „Gebrauchsanleitung für die Chiffriermaschine Enigma-G“, herausgegeben vom Reichswehrministerium (Heeresleitung), Berlin 1928. Leider war diese Dienstvorschrift nirgends zu finden. Sie hätte die Frage beantworten können, ob bei dieser Version die Chiffrierwalzen mit Schubhebeln oder mit Zahnrädern weitergerückt worden sind.
Aus der Tatsache, dass die spätere Abwehr-ENIGMA G-Nummern trug und mit Zahnrad-Antrieb ausgerüstet war, lässt sich schliessen, dass hier auch Zahnrad-Antrieb vorlag. Weitere Stütze erhält dieses Argument durch ein Angebot der Chiffriermaschinen-AG vom September 1929 an

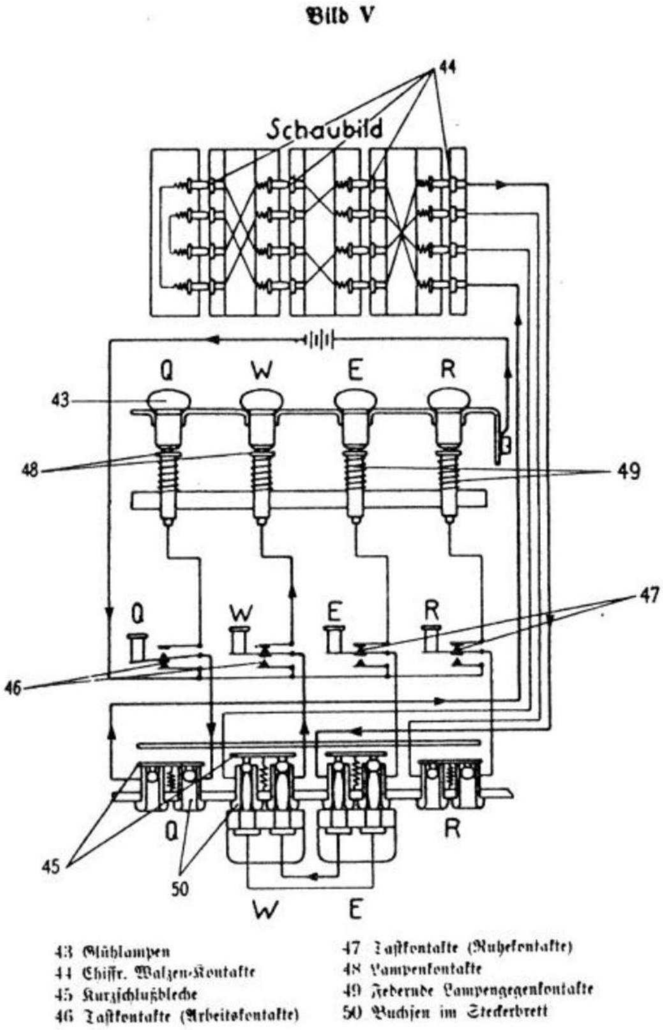


Abbildung 1.1: ENIGMA I (1930)

[11] NARA Dokument Box CBQM33, Nr. 3448 «Analysis of the cipher machine ENIGMA type K»
[12] Quelle: Schweizerisches Bundesarchiv und LANDWEHR: „Das Rätsel um die «Neue Maschine»“ Internet 2001

einen privaten Kunden, in dem von einer Glühlampen-Chiffriermaschine mit Zählwerk die Rede ist. Auch die Umkehrwalze konnte in 26 verschiedenen Stellungen eingesetzt werden und wurde von der Nachbarwalze weiterbewegt. Das Weiterschalten geschah über die Buchstabenringe. Wortzwischenräume konnten durch X, Zahlen durch vorheriges Eingeben von Y markiert werden. (Ähnliche Anweisungen sind später in den Dinstvorschriften der Wehrmacht zu finden.) Entscheidend erscheint aber der Hinweis, dass man beim Vertippen das Chiffrierwalzensystem mit einer Kurbel zurückdrehen konnte bis zum letzten richtigen Buchstaben (Kontrolle durch ein Zählwerk!)[13]

Andererseits könnte aber das Argument gelten, dass wohl kaum ein Modell öffentlich verkauft worden sein konnte, das bei den Streitkräften so in Benutzung war.

Die ENIGMA-G hatte (bis auf die Lage des Buchstabens `P`) das Tastenfeld einer Standard-Schreibmaschine mit 26 Buchstaben. Sie hatte nur drei Walzen, die untereinander vertauscht werden konnten[14]. Die Umkehrwalze konnte nur in einer Stellung eingesetzt werden. Die Eingangswalze war so verändert, dass nun der Buchstabe `A` des Tastenfeldes mit Kontakt 1 verbunden war, Buchstabe `B` mit Kontakt 2 usw. Sie besass ein Feld mit 26 Doppelsteckerkontakten, wahrscheinlich eine Vorform des Steckerbrettes der späteren ENIGMA I (s.u.)[15]. Leider liegt keine nähere Beschreibung dieser Maschine vor.(s.o.)
1930 wurde seitens der Marineleitung erkannt, dass die beim Heer verwendete Enigma besser war, und es notwendig erschien, ein Verfahren zu betreiben, das einen Spruchaustausch zwischen Marine und Heer mittels der Chiffriermaschinen ermöglichte.

Ab 1933 lauteten beim Funkschlüssel C der Marine die Bezeichnungen der fünf Chiffrierwalzen Walze I bis V. Die Ringe trugen einheitlich die Beschriftung `A` bis `Z, Ä, Ö, Ü`. Noch immer war die Sperrscheibe mit dem Walzenkörper fest verbunden.

1.1.10 ENIGMA I

Aus der ENIGMA C wurde für das Heer eine weitere Version entwickelt, die ab 12.5.1930 eingesetzt wurde. Zwei, allerdings nur als handschriftliche Übersetzungen vorliegende, offenbar zusammengehörige Dokumente weisen sie als ENIGMA I aus[16].

1.1.10.1 Steckerbrett.

Zwischen Tastenfeld und Eingangswalze war ein Steckerbrett geschaltet. Es befand sich an der Vorderseite des Gerätes. Es umfasste 26 Doppelbuchsen, mit Buchstaben bzw. Zahlen bezeichnet, die mittels Doppelsteckerpaaren an den Enden von zweiadrigen Verbindungskabeln miteinander verbunden werden konnten. Hinter jeder Doppelbuchse lag eine Kurzschlussbrücke, die die beiden Buchsen des Paares kurzschloss, wenn kein Doppelstecker eingeführt war. Die Doppelstecker waren unverwechselbar: Der eine Steckerstift hatte einen Durchmesser von 3 mm, der andere von 4 mm. Der 3 mm-Stift des einen Doppelsteckers eines jeden Kabels war mit dem 4 mm-Stift des anderen Doppelsteckers verbunden und umgekehrt. Die 3 mm-Buchse war mit der Eingangswalze verbunden, die 4 mm-Buchse mit Taste bzw. Lampe. Entsprechend waren die Doppelbuchsen gestaltet. (Abb.1.1)

Das Steckerbrett führte zu einer Vor- bzw. Nach-Chiffrierung durch (reziproke) Substitution einiger Buchstaben zwischen Tastenfeld und Eingangswalze und zwischen Eingangswalze und Glühlampenfeld. Die selbstreziproke Substitution war allerdings ein Schwachpunkt des Steckersystems, der auch prompt von den alliierten Kryptologen ausgenutzt worden ist. Besser wäre es gewesen, Kabel

[13] Die Kopie des Angebotes wurde dem Autor freundlicherweise von Frode WEIERUD überlassen

[14] KAHN a), S.41; Die Stöpselstellung wies auf das spätere Steckerbrett hin

[15] Über die Existenz des Steckerbretts gehen die Meinungen auseinander,vgl. Lewin und West

[16] «Directions for use of the „ENIGMA“Cypher Machine. Berlin, 1930»und «DIRECTIONS FOR USE OF KEYS ON THE CYPHER MACHINE „ENIGMA I“»aus PRO 25/9. Sie wurden freundlicherweise von R.ERSKINE zur Kenntnis gegeben.

mit Einzelsteckern zu verwenden, an einem Ende den 3 mm-Stift, am anderen Ende den 4 mm-Stift. Die selbstreziproke Eigenschaft der gesamten Maschine wäre dvon unbeeinflusst geblieben.

Die Sperrscheibe war wie bei der ENIGMA D fest mit dem Ring verbunden, sodass für das Weiterschalten der benachbarten Walzen die Ringstellung der Walzen, nicht aber die Stellung des Walzenkörpers bestimmend war.

Die Schaltstellen lagen bei Walze I bis V an den Stellen `Q, E, V, J` und `Z`.

Wie oben bereits erwähnt, konnte bei bestimmten Stellungen (z.B. bei der Grundstellung `L D O` mit Ringstellung `A A A` bei den Walzen III II I) die mittlere Walze zweimal nacheinander rücken[17].

```
L D O
L D P
L D Q
L E R
M F S
```

Die Walzenringe der ENIGMA des Heeres und (ab 1935) der Luftwaffe trugen i.a. die Bezeichnungen 01 bis 26.

Mit dem 1.10.1934 trat eine weitere Veränderung bei der Marine in Kraft:

1.1.11 Funkschlüssel M.

Der Funkschlüssel M, kurz „Schlüssel M“ . Er glich praktisch der Chiffriermaschine ENIGMA I, allerdings standen hier - mit Sicherheit lässt sich dies erst für die Zeit nach Mai 1936 sagen[18] - sieben Walzen I bis VII zur Auswahl. Die Walzen I bis V waren identisch mit denen des Heeres, wobei die Walzen IV und V, wie dort auch, zunächst nicht benutzt werden durften. Die Walzen VI und VII durften nur innerhalb der Marine benutzt werden. Entsprechend der ENIGMA I waren die Sperrscheiben fest mit den Schlüsselringen verbunden. Die Walzen VI und VII hatten, im Gegensatz zu den Nrn. I bis V, zwei Kerben in den Sperrscheiben (Ob sie zunächst auch nur eine Kerbe hatten und die zweite im Rahmen einer Rückrufaktion 1939 bekamen, wie KAHN schreibt[19], ist nicht festzustellen). 1939, kurz vor Kriegsausbruch kam noch die Walze VIII als reine Marinewalze mit zwei Kerben (wie bei VI und VII) hinzu. Die Schaltstellen der drei Walzen VI bis VIII waren gleich und lagen bei `M` und `Z`. Wie die ENIGMA I war der Funkschlüssel M auch mit einem Steckerbrett ausgestattet.

Für die Aufgabe der Ermittlung des Klartextes aus einem Geheimtext ist es oft hilfreich, manchmal unerlässlich, die Verdrahtung der Chiffrierwalzen zu kennen. Im einfachsten Falle schreibt man die Verdrahtung tabellarisch. (Siehe Kap. 2.1)

Für die bei den deutschen Streitkräften verwendeten Chiffrierwalzen ergeben sich dabei folgende Listen. (Die Bezeichnungen beziehen sich auf die Stellung der Eingangswalze, sodass von der rechten Seite der ENIGMA (bezogen auf den Bediener der Maschine) der Buchstabe A oben liegt und die Zählung im Uhrzeigersinn erfolgt.)

[17] DEAVOURS/KRUH a), S.101
[18] DER FUNKSCHLÜSSEL M, 1934, Deckblatt 2 vom 18. Mai 1936
[19] KAHN a), S.43

CHIFFRIERWALZEN

Wehrmacht - ENIGMA

jew. Eingang:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ausgang Eing.-Walze:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ausgang Walze I :	E	K	M	F	L	G	D	Q	V	Z	N	T	O	W	Y	H	X	U	S	P	A	I	B	R	C	J
" Walze II :	A	J	D	K	S	I	R	U	X	B	L	H	W	T	M	C	Q	G	Z	N	P	Y	F	V	O	E
" Walze III :	B	D	F	H	J	L	C	P	R	T	X	V	Z	N	Y	E	I	W	G	A	K	M	U	S	Q	O
" Walze IV :	E	S	O	V	P	Z	J	A	Y	Q	U	I	R	H	X	L	N	F	T	G	K	D	C	M	W	B
" Walze V :	V	Z	B	R	G	I	T	Y	U	P	S	D	N	H	L	X	A	W	M	J	Q	O	F	E	C	K
" Walze VI :	J	P	G	V	O	U	M	F	Y	Q	B	E	N	H	Z	R	D	K	A	S	X	L	I	C	T	W
" Walze VII :	N	Z	J	H	G	R	C	X	M	Y	S	W	B	O	U	F	A	I	V	L	P	E	K	Q	D	T
" Walze VIII:	F	K	Q	H	T	L	X	O	C	B	J	S	P	D	Z	R	A	M	E	W	N	I	U	Y	G	V

Die Angaben bei den einzelnen Walzen geben die Walzenausgänge für die jeweiligen darüberstehenden Buchstaben der Eingangswalze als Walzeneingang an. Dabei ist vorausgesetzt, dass die Chiffrierwalzen sich auch in der „Normstellung“ befinden, d.h. mit dem Eingang `A` oben. In dieser so vorausgesetzten Stellung ist demnach der Ausgang der Walze I beim Buchstaben `A` der Eingangswalze der Buchstabe `E`, d.h. der Ausgang liegt hier um 4 Schritte im Uhrzeigersinn versetzt.

Bemerkenswert ist, dass in einigen Fällen der Walzenausgang dem Walzeneingang direkt gegenüber liegt: Bei Walze I führt der Eingang `S` direkt zum Ausgang `S`, bei Walze II liegen Ein- und Ausgang beim Buchstaben `A` und beim Buchstaben `Q` nicht versetzt.

1.1.11.1 Umkehrwalzen.

Anfang November 1937 wurde bei ENIGMA I und bei Funkschlüssel M die bisherige Umkehrwalze ersetzt durch eine neue Umkehrwalze B[20] (weshalb die erste Umkehrwalze, die 1937 komplett eliminiert wurde, oft als Umkehrwalze A bezeichnet wird), ab der zweiten Hälfte 1940 wurde auch eine Umkehrwalze C verwendet, beim Heer und bei der Luftwaffe jedoch nur kurzzeitig.[21]

Für die Darstellung der Umkehrwalzen reicht die Beschreibung relativ zu `ABCDEF....`

UMKEHRWALZEN

Umkehrwalze A

Eingang:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ausgang:	E	J	M	Z	A	L	Y	X	V	B	W	F	C	R	Q	U	O	N	T	S	P	I	K	H	G	D

Diese Umkehrwalze ist im Nachhinein als Umkehrwalze A bezeichnet worden.[22]

Nach 1937 wurde bei der Wehrmacht die Umkehrwalze B verwendet:

Umkehrwalze B

Eingang:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ausgang:	Y	R	U	H	Q	L	S	D	P	X	N	G	O	K	M	I	E	B	F	Z	C	W	V	J	A	T

[20] MARKS u. WEIERUD, S. 55, Fussnote 1

[21] WELCHMAN b), S.113, Die Bemerkung von WELCHMAN: «That, oddly enough, was the end of Uncle Walter. We never met him again.» soll wohl bedeuten, dass das Problem, die Verdrahtung einer neuen Umkehrwalze zu finden, nicht mehr auftrat.; KOZACZUK a), App. F, S.303

[22] Diese Verdrahtung ist indirekt bestimmt worden, denn bisher ist noch keine solche gefunden worden. Die Bestimmung beruht auf Notizen in MARKS u. WEIERUD S. 55 - 66

Die in der zweiten Hälfte 1940 eingeführte Umkehrwalze C hatte die Verdrahtung:

Umkehrwalze C

Eingang:	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Ausgang:	F V P J I A O Y E D R Z X W G C T K U Q S B N M H L

Hiess die Maschine 1937 noch „Chiffriermaschine ENIGMA“, so trug die entsprechende Dienstvorschrift 1940 die deutschtümelnde Überschrift „Schlüsselmaschine ENIGMA“. Die auf diese Dienstvorschriften bezogenen Angaben beruhen allerdings auf späteren Deckblättern und sind somit verändert. Der ursprüngliche Wortlaut ist nicht immer feststellbar gewesen.

Zum 15.12.1938 wurden die bislang gesperrten Walzen IV und V zum Gebrauch freigegeben.

Ab Oktober 1941 wurden bei der Luftwaffe alle 12 Stunden die Walzen rechts und links miteinander vertauscht. Im Mai 1942 wurden die Walzen bei der Luftwaffe und beim Heer alle acht Stunden zyklisch vertauscht, und zwar rückte dabei die rechte Walze in die linke Position, die beiden anderen wurden nach rechts verschoben. Diese feste Regel erbrachte natürlich keine zusätzliche Geheimhaltung der Walzenlage.[23]

1.1.11.2 Griechenwalzen.

Bei der Marine wurde, beginnend ab 5.10.1941, für einige Schlüsselbereiche eine neue, dünne Umkehrwalze B mit einer Zusatzwalze Beta eingeführt[24]. Dies betraf die Chiffriermaschinen ab Nr. M 2802. (Schlüssel M Form M 4) Die vierte Walze wurde im beengten Raum dadurch realisiert, dass die bisher dicke Umkehrwalze durch die dünne ersetzt wurde und dazu zwischen diese und die dritte Chiffrierwalze eine dünne Zusatzwalze eingefügt wurde. Sie konnte dünner gehalten werden, weil sie nicht für aktives oder passives Weiterdrehen während des Chiffrierens ausgelegt war. Die dünnen Zusatzwalzen erhielten griechische Buchstaben als Kennung („Griechenwalzen“). Die Zusatzwalze besass einen Stellring und konnte in 26 verschiedenen Stellungen zusammen mit der dünnen Umkehrwalze B fest eingesetzt werden. Um sicherzustellen, dass Verkehr auch mit Funkstellen möglich war, die nicht eine solche „gesplittete“ Umkehrwalze hatten, ergab die Kombination mit der Zusatzwalze in der Stellung A mit Ringstellung A genau die Konfiguration der „normalen“ Umkehrwalze B.

Ab 1. Februar 1942 war diese Zusatzwalze im Einsatz im Schlüsselkreis Triton (U-Boote im Atlantik und im Mittelmeer).[25] Ab 1.7.1943 kam noch eine weitere Zusatzwalze Gamma mit der zugehörigen dünnen Umkehrwalze C hinzu. Beide Walzen wurden offenbar abwechselnd im monatlichen Wechsel eingesetzt. Allerdings blieb die Ringstellung hierbei – bis auf die letzten beiden Monate des Krieges – immer auf A[26].

Die Verdrahtung der Griechenwalze Beta war jedoch schon vor ihrer Aktivierung in BP bekannt. Z.B. hatte am 17. 12. 1941 ein U-Boot eine Spruch mit falsch eingestellter Griechenwalze abgesetzt, was zur Rüge seitens des BdU führte, der Spruch sei falsch chiffriert. Die Antwort: „Von Müller. Spruch Nr. 551 ist mit Stellung B chiffriert.“

Die „Griechenwalzen“ und die dünnen Umkehrwalzen zeigten folgende inneren Verdrahtungen:

Eingang:	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Ausgang Beta	L E Y J V C N I X W P B Q M D R T A K Z G F U H O S
Ausgang B dünn	E N K Q A U Y W J I C O P B L M D X Z V F T H R G S
Ausgang Gamma	F S O K A N U E R H M B T I Y C W L Q P Z X V G J D
Ausgang C dünn	R D O B J N T K V E H M L F C W Z A X G Y I P S U Q

[23]NARA Dokument Box CBTE28, No. 3620,«E operations of the GC&CS at Bletchley Park, Cryptanalysis of German Army & German Air Force ENIGMA Traffic», S.37
[24]ERSKINE a), Anmerkung 69, S.180
[25]ERSKINE a), S. 169
[26]ALEXANDER, S. 83, Abschnitt 21

Auswirkung der Griechenwalze Beta

mit:

Ringstellung der Griechenwalze: A

Einstellung der Griechenwalze: A

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Y R U H Q S L D P X N G O K M I E B F Z C W V J A T

mit:

Ringstellung der Griechenwalze: F

Einstellung der Griechenwalze: A

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

N L X R S H T F Z Y U B O A M W V D E G K Q P C J I

mit:

Ringstellung der Griechenwalze: A

Einstellung der Griechenwalze: F

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

E T Z W A S I L G V R H X O N U Y K F B P J D M Q C

Auswirkung der Griechenwalze Gamma

mit:

Ringstellung der Griechenwalze: A

Einstellung der Griechenwalze: A

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

F V P J I A O Y E D R Z X W G C T K U Q S B N M H L

mit:

Ringstellung der Griechenwalze: K

Einstellung der Griechenwalze: A

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

I Y T H Q O J D A G U R N M F X E L W C K Z S P B V

mit:

Ringstellung der Griechenwalze: A

Einstellung der Griechenwalze: K

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

E T S X A Z M V P L N J G K U I R Q C B O H Y D W F

Es waren auch Kombinationen von dünner Walze C mit der Zusatzwalze Beta und umgekehrt im Gebrauch.[27]. Natürlich konnte damit der Verkehr nur innerhalb eines Schlüsselkreises abgewickelt werden.

1.1.12 Umkehrwalze Dora.

Im zum Schlüssel M Form M 4 gehörigen Walzenkasten II (Walzenkasten I enthielt die Walzen I bis VII) war Platz vorgesehen für die Chiffrierwalze VIII, zwei Umkehrwalzen (B und C), zwei Zusatzwalzen (Beta und Gamma), drei Einsätze und eine besondere Umkehrwalze D[28]. Auch die Neufassung der Vorschrift „Allgemeine Schlüsselregeln für die Wehrmacht vom 1.4.1944“ erwähnt die Existenz der Umkehrwalze Dora (im folgenden abgekürzt UD), die allerdings nicht durchgehend eingeführt gewesen sein konnte. Das geht aus dem Satz „Falls verwendet, immer alphabetisch stecken: `AB CD ... XZ`“ hervor. Die Umkehrwalze Dora war eine veränderbare Umkehrwalze. Sie konnte, wie ihre Vorgänger B und C, nur in einer Stellung in die Chiffriermaschine eingesetzt werden. Ein Kontakt oben war mit dem gegenüberliegenden elektrisch fest verbunden. Alle anderen Kontakte, sie waren ohne die Buchstaben J und Y fortlaufend alphabetisch bezeichnet, mussten paarweise durch 12 dünne Kabel mit Steckern an den Enden miteinander verbunden

[27] Schlüssel M - Ägäis, Allgemein. Gültig vom 6. bis 23. 5. 45

[28] Anlage zu O.K.M. Skl/2.Abt. Nc 400/41 g.Kdos.

werden. Im Gegensatz zu den Chiffrierwalzen, bei denen das Alphabet (von der Eingangswalze her gesehen) im Uhrzeigersinn lief, war hier das Alphabet gegen den Uhrzeiger orientiert. Wegen der festen Verbindung war eine Simulation der Umkehrwalze B bzw. C nicht möglich. Die UD wurde im Januar 1944 in einem Schlüsselbereich der Luftwaffe erstmals verwendet. Im März dechiffrierten die Briten einen Funkspruch an den Fliegerführer Albanien, in dem die Ausweitung der Anwendung der UD auf weitere Schlüsselbereiche erwogen wurde (was dann auch tatsächlich geschah). In einem Bericht vom 13.7.1944 wurden 43 Befehlsbereiche der Luftwaffe genannt, die die UD besassen, wovon 22 auch Gebrauch gemacht hatten[29]. Allerdings war den Alliierten die Existenz der UD seit dem 27.12.1943 bekannt, als in einem Klarspruch (!) eine Einheit gefragt wurde, ob sie die Umkehrwalze Dora hätte. Ab 1.5.1944 wurden die Stecker der Umkehrwalze 3mal täglich gewechselt, was ab 10.6. wieder zugunsten eines Wechsels alle 10 Tage geändert wurde. Später wurde der Gebrauch der UD ausgedehnt auf viele weitere Schlüssel.

1.1.13 ENIGMA-Uhr.

Im Bericht vom 13.7.1944 wurde eine weitere apparative Ergänzung der ENIGMA erwähnt, die in einigen Luftwaffenschlüsseln erstmals aufgetreten war: die ENIGMA - Uhr[30]. Sie diente dazu, eine einmal hergestellte Steckerverbindung auf 39 verschiedenen Arten zu verändern. Sie wurde elektrisch bei jedem der 10 Steckerpaare zwischen den Stecker des jeweils ersten Buchstabens und den des zweiten geschaltet. Sie bewirkte – je nach Stellung – eine Veränderung der Steckerpaarung. Die ungesteckerten Buchstaben blieben ungeändert erhalten. Für jede durch 4 ohne Rest teilbare Uhrstellung blieb die Steckerstellung unbeeinflusst durch die Uhr erhalten.

Die Uhr bestand aus einer Chiffrierscheibe mit zwei konzentrischen Kreisen von je 40 Kontaktflächen auf der Unterseite der Scheibe und fest verdrahteten Verbindungen von je zwei dieser Flächen auf der Oberseite. Diese

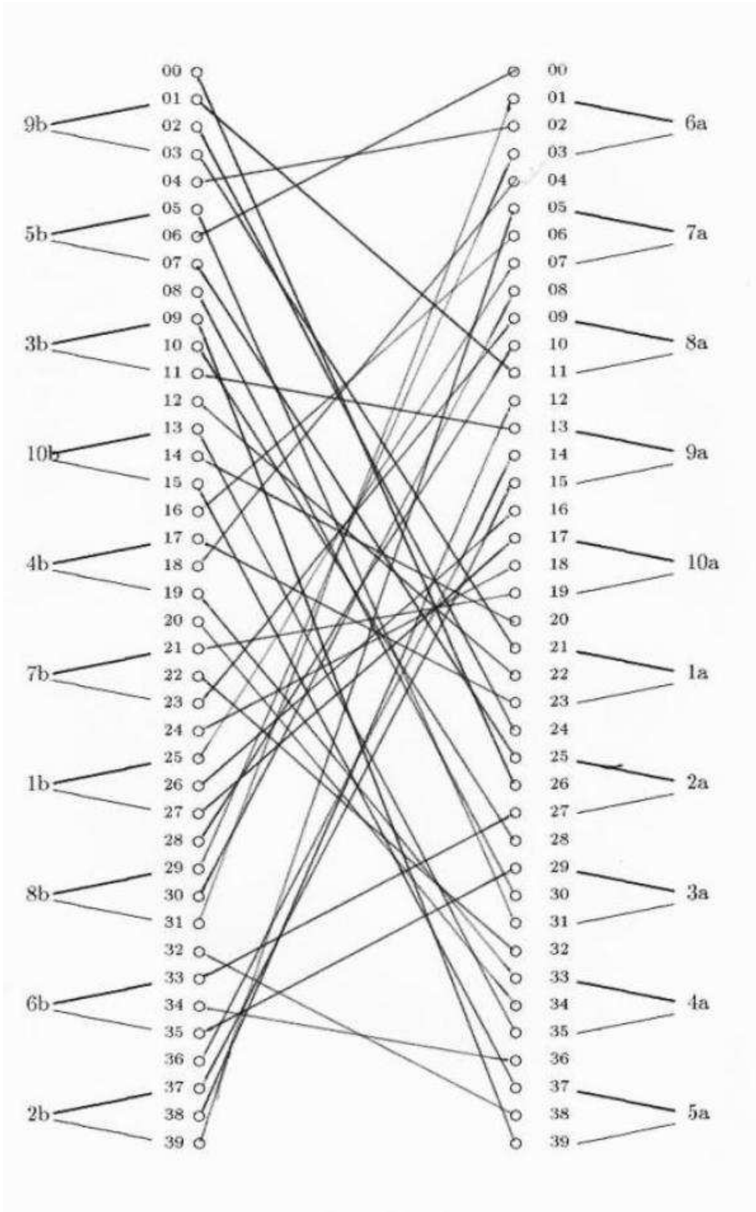


Abbildung 1.2: ENIGMA-Uhr, Schema

[29] ERSKINE/WEIERUD, S.243, Ausführliche Darstellung bei MARKS

[30] HINSLEY III/2, App. 15, S.847

Scheibe konnte durch einen Drehknopf an der Oberseite der Uhr in eine von 40 Stellungen gerastet werden (Bezeichnung 00 bis 39). Die Uhr war durch 20 Kabel mit der „Aussenwelt“ verbunden, an einem Ende mit zwei aus in zwei konzentrischen Kreisen von je 20 Kontakten angeordneten Kontaktstiften, am anderen Ende mit einem Doppelstecker mit dickem und dünnem Stift zum Einstecken in das Steckerbrett der ENIGMA. Die Stecker waren bezeichnet mit `a1` (rot), `b1` (weiss), `a2` (rot), `b2` (weiss) usw bis `a10` (rot), `b10` (weiss). Sie mussten in der Reihenfolge der Steckerverbindungen des Tagesschlüssels gesteckt werden, der `a`-Stecker (rot) jeweils für den ersten Buchstaben des Paares, der `b`-Stecker (weiss) für den zweiten Buchstaben. Abbildung 1.2 gibt schematisch die Verdrahtung der Uhr für die Stellung 21 wieder.[31] Der erste Buchstabe (`A`) des ersten Steckerpaares (`a1` rot, dick) wird vom Anschluss Nr. 21 rechts zum Anschluss Nr. 3 links bei `9b` weiss, dünn, geführt, also zum zweiten Buchstaben des neunten Steckerpaares: `Z`. Der zweite Buchstabe `F` des ersten Steckerpaares (`b1` weiss, dick) führt vom Anschluss Nr. 25 links zum Anschluss `7a` rot, dünn rechts, also zum ersten Buchstaben des 7. Steckerpaares: `Q`.
Ein Vergleich zeigt die Auswirkung der ENIGMA-Uhr (hier Stellung 21) auf die Chiffrierung ohne Benutzung der Uhr[32].

Wirkungsbild der ENIGMA - Uhr

Steckerstellungen:	Zuordnungen für Uhrstellung 21:	
A / F	A / Z	F / Q
H / P	C / Y	G / S
L / Y	H / X	P / L
Q / T	J / U	U / A
S / Z	L / B	Y / H
C / G	N / V	X / C
J / U	Q / G	T / W
N / X	R / T	V / N
R / V	S / P	Z / R
W / B	W / F	B / J
	Taste → Walzen	Taste → Walzen
	Lampe ← Walzen	Lampe ← Walzen

Verfahrenssimulation (Klartext: `abcd`)

Walzenanordnung (schnelle Walze rechts): 321; Ringstellung: `AAA`, Grundstellung: `AAA`
Umkehrwalze: `B`
Steckerverbindungen: `(AF) (CG) (HP) (JU) (LY) (NX) (QT) (RV) (SZ) (WB)`
Uhrstellung: 21

Stellung der Walzen: `AAB`

$A \mapsto D$ $D \mapsto K$ $K \mapsto X$ $X \gg J$ $J \mapsto E$ $E \mapsto Z$ $A \mapsto T$

Spruchbuchstabe: `R`

Stellung der Walzen: `AAC`

$L \mapsto R$ $R \mapsto G$ $G \mapsto C$ $C \gg U$ $U \mapsto W$ $W \mapsto M$ $O \mapsto K$

Spruchbuchstabe: `K`

Stellung der Walzen: `AAD`

$B \mapsto H$ $H \mapsto U$ $U \mapsto K$ $K \gg N$ $N \mapsto N$ $N \mapsto T$ $W \mapsto K$

Spruchbuchstabe: `K`

Stellung der Walzen:`AAE`

$H \mapsto M$ $M \mapsto W$ $W \mapsto U$ $U \gg C$ $C \mapsto G$ $G \mapsto R$ $V \mapsto E$

Spruchbuchstabe: `E`

Geheimtext: `RKKE`

Bei der Uhrstellung 0 erhält man als Geheimtext `FXME`
In der Literatur findet man gelegentlich, dass die ENIGMA-Uhr die Chiffrierung mit der ENIGMA aus der Fessel der Selbstreziprozität befreit hätte.

[31] ULBRICHT, siehe Fussnote 28
[32] Diese Schaltungseinzelheiten beruhen auf Messungen des Verfassers an einer ENIGMA-Uhr im Forsvarsmuseet Oslo.

Das war nicht der Fall, lediglich die Reziprozität der Stecker war aufgehoben. Einen Hinweis auf die Verwendung der Uhr bekommt man durch ein Schild auf der Innenseite des Deckels der Uhr. (Abb. 1.3) Die Buchstabengruppen I und II zeigen, dass hier eine Vorschrift vorlag, für die Übersetzung von Steckerpaaren in Uhrstellungen (00 bis 39). Anfangs begannen die Sprüche, bei denen die ENIGMA-Uhr benutzt wurde, mit einer in Buchstaben ausgedrückten Zahl („null“ bis „dreineun“), um so die Stellung der Uhr für den folgenden Text festzulegen. Die Wahl der Einstellung oblag wahrscheinlich dem Absender. Später (ab 2.11.1944) wurde die Uhrstellung durch vier Buchstaben übermittelt, wobei das erste Bigramm entsprechend dem genannten Schild die erste Ziffer der Uhrstellung definierte, das zweite Bigramm die zweite Ziffer (z.B. `HLDE` $\mapsto$ 11). Dieses Zusatzgerät erschwerte die Arbeit der alliierten Dechiffrierungsdienste erheblich. Eine Tageseinstellung im eigentlichen Sinne existierte nicht mehr.

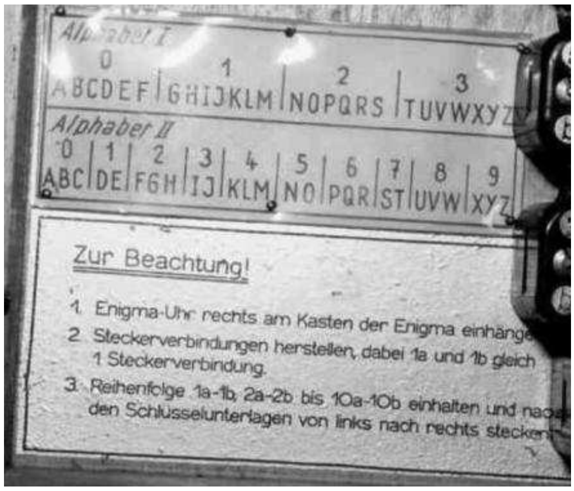


Abbildung 1.3: ENIGMA-Uhr, Deckel

Abb. 1.4 zeigt, dass es im Bereich des Schlüssels M Form M 4 Chiffriermaschinen mit Schreibvorrichtungen gegeben hat. Ausserdem trugen die Tasten der obersten Reihe ausser den Buchstaben `Q` bis `O` zusätzlich die Ziffern 1 bis 9, die Taste `P` die Ziffer 0. Allerdings soll sich die Schreibvorrichtung nicht bewährt haben.

Abbildung 1.4: Tastatur mit Ziffern

1.1.14 Abwehr-ENIGMA.

Die Abwehr hat (schon 1939) eine ENIGMA ähnlichen Typs ohne Stecker benutzt. Die Walzen hatten dabei mehr Schaltstellen für das Weiterrücken der nächsten Walze: 11, 15 und 17, dabei wurde das Weiterschalten nicht durch Schubhebel bewirkt, sondern durch Zahnräder. Auch die Umkehrwalze rückte weiter[33]. Abgesetzt vom eigentlichen Spruchtext, der in 5er-Gruppen erschien, wurde der Spruch eingeleitet von einer Gruppe von acht Buchstaben, die durch Chiffrieren des verdoppelten Spruchschlüssels entstand. Weiter hat die Abwehr auch zwei anders verdrahtete Typen der ENIGMA K verwendet.

[33] TWINN, S.124

In Kap. 6.2.3.4 wird im Zusammenhang mit ihrer Dechiffrierung genauer auf die Abwehr-ENIGMA eingegangen. Die Walzenverdrahtung der Abwehr-ENIGMA war

Abwehr - ENIGMA

jew.Eingang:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ausgang Eing.-Walze:	Q	W	E	R	T	Z	U	I	O	A	S	D	F	G	H	J	K	P	Y	X	C	V	B	N	M	L
“ Walze I :	D	M	T	W	S	I	L	R	U	Y	Q	N	K	F	E	J	C	A	Z	B	P	G	X	O	H	V
“ Walze II :	H	Q	Z	G	P	J	T	M	O	B	L	N	C	I	F	D	Y	A	W	V	E	U	S	R	K	X
“ Walze III :	U	Q	N	T	L	S	Z	F	M	R	E	H	D	P	X	K	I	B	V	Y	G	J	C	W	O	A

Die Umkehrwalze der Abwehr - ENIGMA hatte die Verdrahtung[34]

Abwehr - ENIGMA

Eingang:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ausgang Umkehrwalze :	R	U	L	Q	M	Z	J	S	Y	G	O	C	E	T	K	W	D	A	H	N	B	X	P	V	I	F

Bei der kommerziellen ENIGMA (ENIGMA D) war die Verdrahtung der Walzen

Kommerzielle ENIGMA - ENIGMA D

jew. Eingang:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ausgang Eing.-Walze:	Q	W	E	R	T	Z	U	I	O	A	S	D	F	G	H	J	K	P	Y	X	C	V	B	N	M	L
Ausgang Walze I :	H	R	W	Y	I	P	C	G	V	X	L	A	F	U	J	B	K	O	D	T	S	M	Z	N	Q	E
“ Walze II :	S	E	W	Y	M	G	D	L	O	I	U	B	T	X	K	V	J	P	A	F	Z	C	N	H	R	Q
“ Walze III :	L	V	A	D	Z	P	C	G	Y	B	H	X	Q	S	U	E	T	K	F	I	J	W	M	O	R	N

Umkehrwalze der ENIGMA D

Eingang:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ausgang Umkehrwalze :	I	M	E	T	C	G	F	R	A	Y	S	Q	B	Z	X	W	L	H	K	D	V	U	P	O	J	N

Die schweizer Streitkräfte änderten mehrmals die Verdrahtungen der Walzen der gekauften ENIGMA K, z.B. im Dezember 1942 zur „Verdrahtung 4“:[35]

Verdrahtung 4, ENIGMA K

jew. Eingang:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ausgang Eing.-Walze:	Q	W	E	R	T	Z	U	I	O	A	S	D	F	G	H	J	K	P	Y	X	C	V	B	N	M	L
“ Walze I :	F	K	O	Q	B	L	H	N	A	P	W	D	D	R	U	Y	S	V	G	J	E	X	M	T	Z	I
“ Walze II :	V	M	W	J	N	P	A	U	T	I	F	X	B	Y	G	D	Z	C	R	Q	K	H	O	L	S	E
“ Walze III :	C	F	R	W	A	O	M	T	J	Q	D	V	E	L	B	Z	S	H	K	G	P	N	V	U	X	I

Die Verdrahtung der Walzen der Wehrmacht-ENIGMA siehe S. 8.

Als Kuriosum sei noch erwähnt, dass der spanischen Botschaft in Berlin 1931 eine ENIGMA-Z

[34] HAMER a)

[35] Befehl des Kommandos der Flieger- & Fliegerabwehrtruppen vom 14.12.1942, Schweizer Bundesarchiv

angeboten wurde, die nur die Tasten 0 ··· 9 aufwies, ebenso das Glühlampenfeld.[36]

1.1.15 Reichsbahn-ENIGMA.

Die Reichsbahn benutzte eine steckerlose ENIGMA mit einstellbarer Umkehrwalze, die aber nicht weiterrücken konnte. Wegen der ungewöhnlichen und i.a. völlig unbekannten Klartexte (i.a. Zahlenfolgen) war die Dechiffrierung dieser Version extrem schwierig. Die Schaltung der Walzen war:

Reichsbahn - ENIGMA

jew. Eingang:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ausgang Eing.-Walze:	Q	W	E	R	T	Z	U	I	O	A	S	D	F	G	H	J	K	P	Y	X	C	V	B	N	M	L
Ausgang Walze I :	J	G	D	Q	O	X	U	S	C	A	M	I	F	R	V	T	P	N	E	W	K	B	L	Z	Y	H
" Walze II :	N	T	Z	P	S	F	B	O	K	M	W	R	C	J	D	I	V	L	A	E	Y	U	X	H	G	Q
" Walze III:	J	V	I	U	B	H	T	C	D	Y	A	K	E	Q	Z	P	O	S	G	X	N	R	M	W	F	L

Hier sind die Kontakte der Eingangswalze mit der Tastatur anders verbunden als bei der ENIGMA der Wehrmacht: Der Buchstabe A der Tastatur ist hier mit dem Kontakt verbunden, der um 9 Schritte im Uhrzeigersinn versetzt ist.
Bei der Reichsbahn - ENIGMA war die Verdrahtung der Umkehrwalze[37]

Reichsbahn - ENIGMA

Eingang:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ausgang Umkehrwalze :	Q	Y	H	O	G	N	E	C	V	P	U	Z	T	F	D	J	A	X	W	M	K	I	S	R	B	L

1.1.16 ENIGMA T.

Für die japanische Marine war eine besondere Abart gebaut worden, die ENIGMA T („Tirpitz“). Nur wenige Exemplare konnten ausgeliefert werden. Im Sommer 1944 wurden einige Exemplare in einem Lagerhaus in Frankreich erbeutet. „Tirpitz“ enthielt keine Stecker. Die Walzen hatten je 5 Kerben zum Weiterrücken, verwendet wurden jeweils drei von acht Walzen mit besonderer Verdrahtung. Die Umkehrwalze soll auch weitergerückt sein. Letzteres geht allerdings aus einem amerikanischen Dokument [38] nicht hervor. Sprüche, die mit dieser Abart hätten chiffriert sein können, waren nicht bekannt.
Die Verdrahtung der Chiffrierwalzen war:

ENIGMA T - „Tirpitz“

jew. Eingang,:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ausgang Eing.-Walze:	K	Z	R	O	U	Q	H	Y	A	I	G	B	L	W	V	S	T	D	X	F	P	N	M	C	J	E
Ausgang Walze I :	K	P	T	Y	U	E	L	O	C	V	G	R	F	Q	D	A	N	J	M	B	S	W	H	Z	X	I
" Walze II :	U	P	H	Z	L	W	E	Q	M	T	D	J	X	C	A	K	S	O	I	G	V	B	Y	F	N	R
" Walze III :	Q	U	D	L	Y	R	F	E	K	O	N	V	Z	A	X	W	H	M	G	P	J	B	S	I	C	T
" Walze V :	U	A	X	G	I	S	N	J	B	V	E	R	D	Y	L	F	Z	W	T	P	C	K	O	H	M	Q
" Walze VI :	X	F	U	Z	G	A	L	V	H	C	N	Y	S	E	W	Q	T	D	M	R	B	K	P	I	O	J
" Walze VII :	B	J	V	F	T	X	P	L	N	A	Y	O	Z	I	K	W	G	D	Q	E	R	U	C	H	S	M
" Walze VIII :	Y	M	T	P	N	Z	H	W	K	O	D	A	J	X	E	L	U	Q	V	G	C	B	I	S	F	R

[36] QUIRANTES
[37] HAMER a) u. HAMER,SULLIVAN,WEIERUD
[38] «Patterns of T–Wheels in ENIGMA Motion», NARA Dokument Box CBKH68, Nr. 1538

Die Verdrahtung der Walze IV ist nicht bekannt.

Die Umkehrwalze der ENIGMA - T hatte die Verdrahtung[39]

ENIGMA - T

Eingang:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Ausgang Umkehrwalze :	G	E	K	P	B	T	A	U	M	O	C	N	I	L	J	D	X	Z	Y	F	H	W	V	Q	S	R

Ab Januar 1945 tauchten auch Sprüche auf, die mit einer ENIGMA K D chiffriert worden waren. Diese Maschine nutzte drei von sechs Chiffrierwalzen mit je neun Schaltstellen. Die Eingangswalze entsprach der Tastatur, d.h. `Q` war zugeordnet der Position 1 , `W` der Position 2 , usw. Die Umkehrwalze entsprach der UD[40].

1.2 Allgemeine Chiffrierregeln

Zunächst, bis spätestens 1937 — das genaue Datum ist mangels beweisender Dokumente nicht feststellbar —, war beim Heer das Chiffrierverfahren recht einfach: Bevor ein Klartext mittels eines Schlüssels in den zugehörigen Geheimtext übergeführt werden konnte, musste er entsprechend der Vorschrift „Die Heeresschlüssel“ vom 27.6.1935 bearbeitet werden. Das betraf z.B. die Behandlung von Umlauten, die Umsetzung von Zahlen in Buchstaben. Diese Vorschrift wurde später ersetzt durch „Allgemeine Schlüsselregeln für die Wehrmacht“ (H.Dv.g.7, M.Dv.Nr. 534, L.Dv.g.7 vom 13.1.1940 und vom 1.4.1944). In diesen Vorschriften waren in den Abschnitten „III. Für alle Chiffrierverfahren gültige Bestimmungen“ bzw. „IX. Vorschriften für das Schlüsseln“ allgemeine Grundregeln niedergelegt, die bei der Abfassung eines Spruches, bei seiner evtl. Wiederholung, bei der Überschreitung der zulässigen Länge, bei aufgetretenen Chiffrierfehlern usw. beachtet werden mussten. Es hat sich gezeigt, dass Verstösse gegen diese Grundregeln verschiedentlich die Bemühungen der Alliierten zur Dechiffrierung der Sprüche erleichtert haben. Ungültige Schlüsseltafeln waren drei Tage nach Ablauf ihrer Gültigkeit zu vernichten. Offenbar ist dies auch konsequent geschehen, denn es sind kaum Unterlagen erhalten geblieben.

In der Neufassung der Vorschrift H.Dv.g.7 „Allgemeine Schlüsselregeln für die Wehrmacht vom 1.4.1944“ wurde u.a. angeordnet, dass bei kurzen Sprüchen oder wenn Absender oder Empfänger im Spruch genannt werden mussten, beliebige Wahlwörter voran- oder nachgestellt werden mussten. Zum Erkennen der Wahlwörter mussten ihre an den Spruchtext angrenzenden Buchstaben verdoppelt werden. Der Spruchkopf musste stets doppelt getastet werden. In ihm folgten auf die Uhrzeit und die Buchstabenzahl die Kenngruppe (wenn nötig), die Grundstellung und der chiffrierte Spruchschlüssel.

Es wurde besonders darauf hingewiesen, dass es für die Marine z.T. abweichende Vorschriften gab. Diese waren eingearbeitet in die Vorschriften „Der Funkschlüssel C“ von 1926 und „Der Funkschlüssel C (Vorschrift)“ von 1933, die die Behandlung von marinetypischen Begriffen regelten. In den weiteren Vorschriften „Der Funkschlüssel M (Vorschrift)“ M.Dv.Nr.32 von 1934, „Der Schlüssel M Verfahren M Allgemein“ M.Dv.Nr. 32/1 von 1940, „Der Schlüssel M Allgemeine Bestimmungen“ M.Dv.Nr. 32/3 von 1941 und „Ergänzende Anweisungen zu 'Der Schlüssel M Verfahren M Allgemein'“ von 1944 wurden diese Regelungen fortgeschrieben.

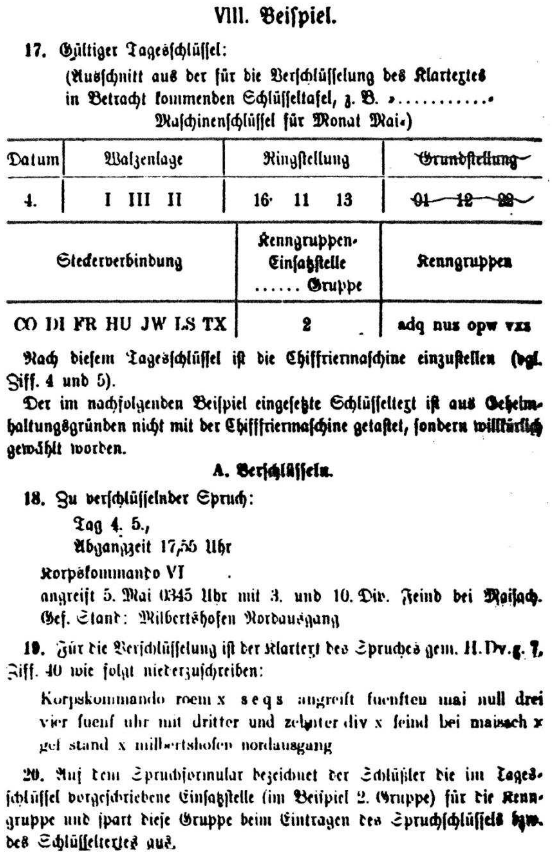
[39] HAMER,SULLIVAN,WEIERUD

[40] NARA Dokument Box CBKG77, Nr. 12656A «Tentative List of Enigma and other Machine Usages» und HAMER,SULLIVAN,WEIERUD

1.3 Maschinenschlüssel

1.3.1 Heer/Luftwaffe

Die früheste Vorschrift für die Verwendung der ENIGMA I datiert von 1930, abgesehen von der nicht auffindbaren von 1928.[41] In ihr wird festgelegt, dass die Walzenlage jeweils drei Monate konstant bleibt. Die Ringstellung wechselt täglich, Grundstellung und Steckerlage ebenfalls. Aus der späteren Chiffrieranleitung von 1937 stammt Abb.1.5.[42]



VIII. Beispiel.

17. Gültiger Tagesschlüssel:
(Ausschnitt aus der für die Verschlüsselung des Klartextes in Betracht kommenden Schlüsseltafel, z. B. »............ Maschinenschlüssel für Monat Mai«)

Datum	Walzenlage	Ringstellung	~~Grundstellung~~
4.	I III II	16 11 13	~~01 12 22~~

Steckerverbindung	Kenngruppen-Einsatzstelle ...... Gruppe	Kenngruppen
CO DI FR HU JW LS TX	2	adq nus opw vxz

Nach diesem Tagesschlüssel ist die Chiffriermaschine einzustellen (vgl. Ziff. 4 und 5).

Der im nachfolgenden Beispiel eingesetzte Schlüsseltext ist aus Geheimhaltungsgründen nicht mit der Chiffriermaschine getastet, sondern willkürlich gewählt worden.

A. Verschlüsseln.

18. Zu verschlüsselnder Spruch:
Tag 4. 5.,
Abgangzeit 17,55 Uhr
Korpskommando VI
angreift 5. Mai 0345 Uhr mit 3. und 10. Div. Feind bei Maisach. Gef. Stand: Milbertshofen Nordausgang

19. Für die Verschlüsselung ist der Klartext des Spruches gem. H.Dv.g. 7, Ziff. 40 wie folgt niederzuschreiben:

Korpskommando roem x seqs angreift fuenften mai null drei vier fuenf uhr mit dritter und zehnter div x feind bei maisach x gef stand x milbertshofen nordausgang

20. Auf dem Spruchformular bezeichnet der Schlüßler die im Tagesschlüssel vorgeschriebene Einsatzstelle (im Beispiel 2. Gruppe) für die Kenngruppe und spart diese Gruppe beim Eintragen des Spruchschlüssels bzw. des Schlüsseltextes aus.

Abbildung 1.5: Tagesschlüssel

Zur Einstellung der Grundstellung musste jede Walze mit Hilfe des Stellrades soweit gedreht werden, bis im Fenster neben dem Stellrad die vorgeschriebene Zahl (bzw. der Buchstabe) sichtbar war.
Die Wahl des Spruchschlüssels blieb dem Chiffrierer überlassen, jedoch musste jeder Spruch eines Tages einen eigenen Spruchschlüssel erhalten. dieser war zweimal mit der Grundstellung zu chiffrieren und dem Spruch nach der Präambel voranzustellen. Die durch Chiffrierung des verdoppelten Spruchschlüssels erhaltene Gruppe aus sechs Buchstaben wird im folgenden als Indikator bezeichnet. Die Präambel bestand aus der Zeitgruppe (4 Ziffern), der Anzahl der Buchstaben und einer willkürlichen dreiziffrigen Zahl als Hinweis auf ENIGMA-Chiffrierung.
später dienten zur Identifizierung des Schlüsselbereichs und damit des verwendeten Schlüssels dreistellige Gruppen (Kenngruppen), die durch zwei beliebige Buchstaben am Anfang zu einer fünfstelligen Gruppe ergänzt werden sollten. Dabei sollten bei den verschiedenen Sprüchen eines Tages die angegebenen dreistelligen Kenngruppen der Tafel abwechselnd verwendet werden, wobei die Reihenfolge der einzelnen Buchstaben verändert werden sollte. In der Schlüsseltafel wurde auch vorgeschrieben, als wievielte Fünfergruppe diese Kenngruppe in den Spruch einzufügen war („Einsatzstelle“). Diese Kenngruppe wurde bei der Zahl der Buchstaben des Spruches zwar mitgezählt, aber nicht mit chiffriert. Danach wurde die Maschine auf den gewählten Spruchschlüssel als Grundstellung (durch Drehen der Stellräder) eingestellt und der Klartext eingetastet.
Die Höchstlänge eines Spruchs betrug bis 13.1.1940 180 Buchstaben, sonst musste er in mehrere Teile verschiedener Länge zerlegt werden. Die Vorschrift für die Walzenlage hatte ab 1.1.1936 gewechselt: bis 30.9.1936 monatlich, ab 1.10.1936 täglich[43].
Bis zum 30.9.1936 wurden sechs Steckerpaare festgelegt, was 14 Buchstaben ungeändert liess. Ab 1.10.1936 bis Ende 1938 wechselte die Steckerzahl täglich zwischen 5 und 8 Paaren.

[41] Siehe Fussnote 10, S.4
[42] Schlüsselanleitung zur Chiffriermaschine Enigma vom 8.6.1937 mit Deckblättern für spätere Veränderungen, z.B. monatlichen Wechsel der Walzenlage
[43] BLOCH d), S. B5

Die freie Wahl des Spruchschlüssels war allerdings ab Ende 1932 insofern eingeschränkt, als Kombinationen dreier gleicher Buchstaben (`AAA`) verboten waren, ebenso Wörter (`IST`), eigene Rufzeichen, Verkehrszeichen (Q-Gruppen), Buchstaben, die auf der Tastatur benachbart liegen (`ERT`) oder in alphabetischer Folge vorwärts oder rückwärts. Über die Auswirkungen solcher Schlüsselwahlen für die unbefugte Dechiffrierung siehe Kap. 3.1.2.1 und 6.2.3.1.4.
Ursprünglich wurde zur Bildung eines Notschlüssels der Monat herangezogen, in dem der Notschlüssel verwendet wurde:

z.B. `F E B R U A R` , die auftretenden Buchstaben markiert
`4 3 2 5 7 1 6` ergab als Walzenlage III,II,1.

Die Ringstellung folgte aus 04, 03,02 zu `F E B`.
Die Stecker wurden mit einem Schlüsselwort bestimmt, z.B.

`REICHSWEHRMINISTERIUM BERLIN`, doppelte Buchstaben entfernt ergab
`REICHSWMNTUBL`, die Buchstaben in Zahlen umgesetzt :

18, 5, 9, 3, 8, 19, 23, 13, 14, 20, 21, 2, 12, ergaben die Steckerpaarungen
18/5, 9/3, 8,19, 23/13, 14/20 und 21/2. Die Grundstellung wurde aus den ersten drei Buchstaben bzw. Zahlen gebildet: R, E, I, bzw. 18, 5, 9.
In der Präambel wurde statt der dreiziffrigen Zahl eine zweiziffrige als Hinweis auf die Verwendung des Notschlüssels verwendet.

1.3.1.1 Änderung des Chiffrierverfahrens.

Mit dem 15.9.1938[44] trat eine Änderung des Verfahrens ein, die den Nachteil beseitigen sollte, dass alle Spruchschlüssel eines Tages mit derselben Grundstellung chiffriert waren.

Nun musste der Chiffrierer selbst für jeden Spruch eine besondere Grundstellung unter Beachtung der Beschränkungen wählen, die auch für die Wahl des Spruchschlüssels zu gelten hatten. Diese Grundstellung wurde zweimal am Ende des Spruchkopfes offen gesendet. Der Spruchkopf bestand also nun aus Datumsangabe, Uhrzeit (beides vierstellig), Buchstabenzahl und aus der zweimal angegebenen vom Chiffrierer gewählten Grundstellung.

Der Chiffrierer hatte sodann für jeden Spruch bzw. Teil eines mehrteiligen Spruches einen Spruchschlüssel zu wählen. Dieser Spruchschlüssel wurde zweimal nacheinander mit der vom Chiffrierer gewählten Grundstellung getastet und die sich ergebenden sechs Geheimbuchstaben vor den zu chiffrierenden Spruch gesetzt. Mit dem Spruchschlüssel als Grundstellung wurde dann der eigentliche Klartext chiffriert und zu Fünfergruppen zusammengefasst. Dabei musste allerdings die noch einzufügende Kenngruppe berücksichtigt werden. Diese diente zur Feststellung des angewandten Tagesschlüssels und wurde wie bisher aus mehreren Dreiergruppen des Tagesschlüssels ausgewählt, die drei Buchstaben verwürfelt und durch Voranstellen von zwei beliebigen Füllbuchstaben zu einer Fünfergruppe ergänzt. Diese Kenngruppe wurde nicht chiffriert, ihre Buchstaben wurden bei der Angabe der Buchstabenzahl im Spruchkopf mitgerechnet.

Das folgende Beispiel vom 21. September 1938 zeigt das Verfahren.[45]
Der Spruch lautet:

```
                2109 - 1750 -3 TLE - FRXFRX - 1Tl - 172 =
HCALN UQKRQ AXPWT WUQTZ KFXZO MJFOY RHYZW VBXYS IWMMV WBLEB
DMWUW BTVHM RFLKS DCCEX IYPAH RMPZI OVBBR VLNHZ UPOSY EIPWJ
TUGYO SLAOX RHKVC HQOSV DTRBP DJEUK SBBXH TYGVH GFICA CVGUV
                    OQFAQ WBKXZ JSQJF ZPEVJ RO -
```

Im hier gezeigten Beispiel ist nur der erste von 3 Teilen des Originalspruchs angegeben.[46] Im Einzelnen bedeuten:

[44] Deckblätter (August 1938) Nr. 1 bis 13 zur H.Dv.g. 14 v. 8.6.37 „Gültig ab 15.9.1938“

[45] Aus «The Turing Bombe: Was it Enough?», C.A. Deavours and Louis Kruh, Cryptologia, October 1990, Vol. XIV, No. 4, p. 342

[46] Zum Nachvollziehen der Chiffrierung: Walzenlage: II, I, III; Ringstellung: `ZWD`;
Steckerverbindungen: `(EZ), (BL), (XP), (WR), (IU), (VM), JO)`

2109: Datum 21. September; 1750: Zeit 17 Uhr 50; 3 TLE: der Spruch besteht aus drei Teilen; `FRXFRX`: die zweimal getastete Grundstellung `FRX`; 1Tl: der erste der drei Teile; 172: die Anzahl der Buchstaben des Spruches. Die geneigt gedruckte Gruppe *`AXPWT`* ist die Kenngruppe, die dem Empfänger angibt, zu welchem Schlüsselbereich der Spruch gehört.
Der Empfänger erhält mit der Grundtellung `FRX` aus dem Geheimtext `HCALNU` den Klartext `AGIAGI` und damit den Spruchschlüssel `AGI`. Damit dechiffriert er unter Weglassen der Kenngruppe den Spruch und erhält:

```
AUF BEFEHL DES OBERSTEN BEFEHLSHABERS SIND IM FALLE X Z X ZT X
UNWAHRSCHEINLICHEN X FRANZOESISQEN ANGRIFFS DIE WESTBEFESTIGUNGEN
JEDER ZAHELMAESSIGEN UEBERLEGENHEIT ZUM TROTZ ZU HALTEN X
```

Vermutlich ab 15.9.1938 wurden, täglich wechselnd, 10 Steckerpaare verwendet. Die Deckblätter vom August 1938 zur „Schlüsselanleitung zur Chiffriermaschine ENIGMA (v. 8.6.37)" sagen unter Nr. 5:

> *Nach Ausrüstung der Chiffriermaschine mit den erforderlichen Doppelsteckerschnüren müssen immer 10 Steckerverbindungen angewendet werden.*

REJEWSKI schreibt vom 1.Januar 1939 als Einführungsdatum für 10 Steckerpaare[47]. KAHN schreibt, es hätte im Jahre 1939 zwei Änderungen der Steckerzahl gegeben[48]. Es ist durchaus möglich, dass die im o.g. Deckblatt Nr. 5 genannte Bedingung erst am 1.1.1939 erfüllt war.

In der „Schlüsselanleitung zur Schlüsselmaschine Enigma" (H.Dv.g.14 vom 13.1.40) waren folgende Änderungen enthalten.:

1) Die Höchstlänge eines einzelnen Spruches (Spruchteils) wurde von 180 Buchstaben auf 250 Buchstaben erhöht.

2) Die Datumsangabe im Spruchkopf entfiel.

3) Die Kenngruppe (Fünfergruppe) wurde immer als erste Gruppe gesendet, nach dem Spruchkopf, aber vor dem chiffrierten Spruchschlüssel; der chiffrierte Klartext begann mit dem 12. Buchstaben nach dem Spruchkopf.

Im Funknetz des SD wurden aber nach dem 15.9.1938, auch nach Freigabe von Walze IV und V, die vorherigen Chiffriermethoden beibehalten. Der Schlüssel wechselte täglich 0000 Uhr, Die Schlüsseltafeln blieben, wie bisher, Monatstafeln. Mit den Deckblättern Nr. 1 - 8[49] wurde eine grundlegende Änderung des Verfahrens ab 1.5.1940 angeordnet: Die Verdopplung des Spruchschlüssel unterblieb fortan. Der Spruchkopf bestand also nur noch aus der Uhrzeit, der Buchstabenzahl, der vom Chiffrierer gewählten Grundstellung (einfach) und dem chiffrierten Spruchschlüssel (ebenfalls einfach). Der chiffrierte Klartext begann also nun mit dem 6. Buchstaben nach dem Spruchkopf.

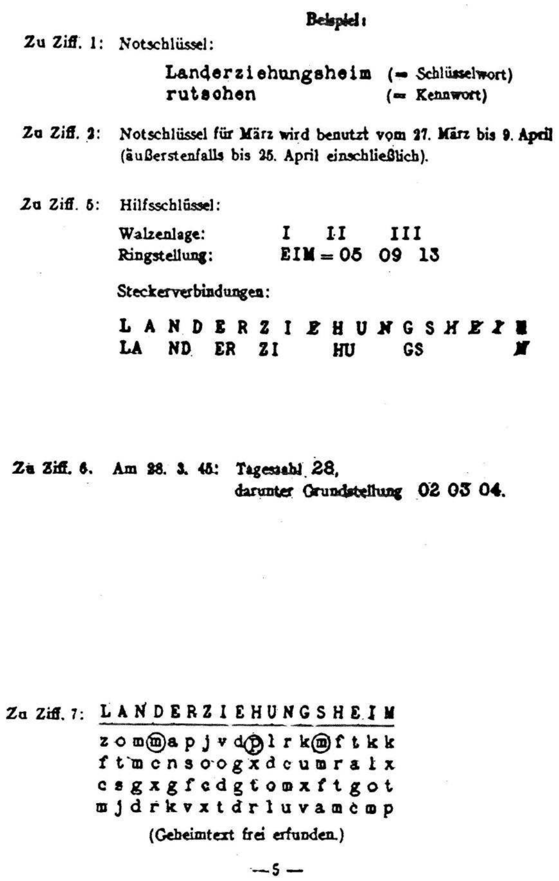
Mit dem 1.September 1942 wurden die Tagesschlüssel jeweils auch 0800 Uhr und 1600 Uhr geändert. Diese Änderung bestand darin, dass die benutzten Walzen jeweils (zyklisch) um einen Platz nach rechts verschoben wurden[50]. An der ursprünglichen Einstellung der Ringe der einzelnen Walzen änderte sich dabei nichts.

Beim Heer wurde mit dem 1.9.1943 auf die Kenngruppe verzichtet, bei der Luftwaffe ab 1.11.1943. Allerdings mussten bei der Benutzung der UD die Kenngruppen wieder verwendet werden.

[47]REJEWSKI e), S. 227. Es waren allerdings (zunächst) 7 bis 10 Steckerpaare
[48]KAHN b), S. 307
[49]vom April 1940, „Gültig ab 1.5.1940"
[50]Berichtigung zu H.Dv.g.14, Abs. 5 vom 30.7.42

1.3.1.2 Notschlüssel.

Die Vorschrift „Anleitung zum Ableiten des Notschlüssels für die Schlüsselmaschine ENIGMA, Ausgabe vom 7. Dezember 1944“ [51] beschreibt die Ableitung der Maschineneinstellung aus einem Schlüsselwort und der Kenngruppe aus einem Kennwort. Das Schlüsselwort, das mindestens 12 Buchstaben lang sein musste, lieferte die Walzenlage, die Ringstellung und die Steckerverbindungen. Die Grundstellungen für die verschiedenen Tage waren einer Tabelle im Deckel der Maschine zu entnehmen. Schlüsselwort und Kennwort blieben bis zu 30 Tagen gültig. Aus diesen langfristigen Angaben wurde die aktuellen Hilfsschlüssel erstellt. (Abb.1.6)


Beispiel:

Zu Ziff. 1: Notschlüssel:

Landerziehungsheim (= Schlüsselwort)
rutschen (= Kennwort)

Zu Ziff. 2: Notschlüssel für März wird benutzt vom 27. März bis 9. April (äußerstenfalls bis 25. April einschließlich).

Zu Ziff. 5: Hilfsschlüssel:

Walzenlage: I II III
Ringstellung: EIM = 05 09 13

Steckerverbindungen:

L A N D E R Z I E H U N G S H E I M
LA ND ER ZI HU GS M

Zu Ziff. 6. Am 28. 3. 45: Tageszahl 28, darunter Grundstellung 02 05 04.

Zu Ziff. 7: L A N D E R Z I E H U N G S H E I M

z o m m a p j v d p l r k m f t k k
f t m c n s o o g x d c u m r a l x
c s g x g f c d g t o m x f t g o t
m j d r k v x t d r l u v a m c m p

(Geheimtext frei erfunden.)

— 5 —

Abbildung 1.6: Notschlüssel

Mit der Walzenlage I, II, III, der Ringstellung aus den letzten drei Buchstaben des Schlüsselwortes und aus der Steckerverbindung, die durch Bildung von Paaren aus voneinander verschiedenen Buchstaben im Schlüsselwort in der Reihenfolge ihres Auftretens entstanden, wurde das Schlüsselwort viermal nacheinander getastet. In der Reihenfolge ihres Auftretens wurde die Buchstaben dieses Geheimtextes zu Paaren zusammengefasst, das lieferte die aktuellen Steckerverbindungen.

Die ersten drei der mehrfach aufgetretenen Buchstaben (die also nicht in Steckerpaare aufgenommen wurden) wurden markiert und als Ringstellung verwendet. Die letzten fünf Buchstaben des Geheimtextes zum Schlüsselwort wurden entsprechend ihrer relativen Reihenfolge im Alphabet numeriert (doppelt in der Reihenfolge ihres Auftretens). Die letzten drei Zahlen ergaben die Walzenlage. Als Kenngruppe galten für die gesamte Dauer der Gültigkeit des Notschlüssels der erste, dritte und fünfte Buchstabe im Kennwort. Ein ähnliches Verfahren zur Konstruktion von Notschlüsseln gab es für die Luftwaffe.[52] Es wird hier ausführlich dargestellt, weil es in Kap. 6.2.3.2.1 benötigt wird.

Anleitung zur Ableitung des Notschlüssels Zu: Lw. Masch. Schlüssel (Enigma)
Verteilung 1.5.44

I Allgemeines:
Zwei Schlüsselwörter werden ausgegeben, z.B. „Fensterbrett“ und „Zeisig“. Die Wörter sind in alphabetischer Reihenfolge zu benutzen. Sie sind immer verschieden, und soweit wie möglich soll zwischen ihnen kein Sinnzusammenhang bestehen, wie bei „Kirsch“ und „Wasser“. In diesen Wörtern dürfen -CH und -CK nicht durch Q ersetzt werden.

[51] BA/MA, RWD9/31
[52] NARA Dokument Box CBMH15, Nr. 1238A, «Capt. W.FRIED Reports» , F-80

1. Das erste der zwei Schlüsselwörter (Tagesschlüsselwort) wird gebraucht, um den Notschlüssel zu ermitteln. Es sollte wenigstens sechs verschiedene Buchstaben haben. Von mehrfach auftretenden Buchstaben wird nur der erste benutzt, die anderen werden gestrichen, z.B.

F E N S T E R B R E T T = FENSTRB

2. Das zweite der beiden Schlüsselwörtern (Kenngruppenwort) dient zur Ermittlung der Diskriminante[53]. Es muss mindestens fünf Buchstaben enthalten, soweit möglich verschieden. Falls bei einer Funkstation mehrere Notschlüssel entweder gleichzeitig oder an aufeinander folgenden Tagen verwendet werden, sollen die Kenngruppenwörter an der ersten, dritten und fünften Stelle nicht mehr als 2 gleiche Buchstaben enthalten.
II Ableitung des Tagesschlüssels:
1. Aus dem ersten Schlüsselwort wird ein Zahlenschlüssel gebildet, indem die Buchstaben in alphabetischer Ordnung, beginnend bei 1, durchnummeriert werden.
2. Unter das Schlüsselwort werden die nicht im Schlüsselwort enthaltenen Buchstaben zeilenweise in alphabetischer Ordnung geschrieben.
3. Die Buchstaben werden spaltenweise entsprechend dem Zahlenschlüssel, beginnend bei 1, ausgelesen und in zwei Zeilen zu je 13 Buchstaben geschrieben.
4. In der zweiten Zeile wird der in alphabetischer Ordnung erste Buchstabe mit 1 bezeichnet, der zweite mit 2 usw. bis 5. Die drei am weitesten links stehenden Ziffern ergeben die Walzenfolge.
5. Die drei Buchstaben über diesen drei Ziffern ergeben die Ringstellung.
6. Die drei Buchstaben, die die Ringstellung ergeben, sowie die direkt darunter werden gestrichen. Die übrigen jeweils übereinander stehenden Buchstabenpaare bilden die Steckerstellungen.

BEISPIEL

```
3 2 4 6 7 5 1          B E W
F E N S T R B         BJUECLWFAKVND
A C D G H I J         MXRIQSGOYTHPZ
K L M O P Q U         4  3  15  2
V W X Y Z
```

BEISPIEL für den TAGESSCHLÜSSEL

Walzenordnung `431`
Ringstellung `BEW`
Stecker: `J/X, U/R, C/Q, L/S, F/O, A/Y, K/T, V/H, N/P, D/Z`

III Ableitung der Diskriminante

Vom zweiten Schlüsselwort werden der erste, der dritte und der fünfte Buchstabe genommen. Diese drei Buchstaben werden in die Präambel des Spruches als Notschlüsseldiskriminante eingesetzt.

BEISPIEL Z E I S I G = ZII

Die Diskriminante darf nur so selten wie möglich benutzt werden, und muss immer weggelassen werden, wenn keine Zweifel bestehen, dass der Empfänger die Art des benutzten Schlüssels erkennt.

IV Verteilung des Notschlüssels

Der Notschlüssel darf dem Schlüsselpersonal, einschl. Funktruppführern nur mündlich gegeben werden. Die beiden Schlüsselworte sind auswendig zu lernen oder an einem sicheren Platz niederzuschreiben. (Siehe L.Dv.g. 60, Die Luftwaffenschlüssel)

Auffällig ist dabei, dass die Ringstellung aus ungesteckerten Buchstaben besteht und bei den Steckerpaaren benachbarte Buchstaben auftreten können.

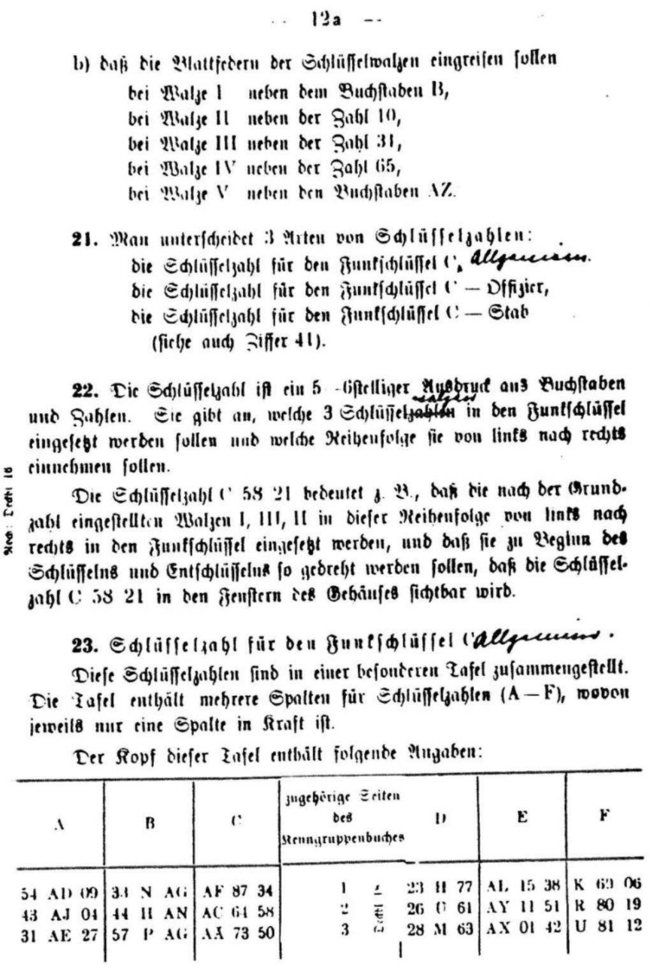
Am 15. September 1944 trat eine weitere Veränderung des Chiffrierverfahrens beim Heer in Kraft[54]. In Teil A wurde ein neues Verfahren zur Auswahl und zum Gebrauch des Indikators (Spruchschlüssel) beschrieben: Der Funkleiter muss einen allgemeinen Text wählen (aus Buch, Lied, usw.) und

[53] Die Diskriminante diente als Kenngruppe zur Unterscheidung der einzelnen Funknetze
[54] Chef H Rüst BdE, 47 p 12 Ag N/HNV/IV, Nr. 9879/44 geh. Vom 27.August 1944

mit der Chiffriermaschine in der Stellung Walzenlage: I II, III, Ringstellung 01, 01, 01, 10 zufällig ausgewählten Steckerverbindungen und einer zufällig ausgewählten Grundstellung chiffrieren. Die entstandenen chiffrierten Buchstaben werden nacheinander in Gruppen von je 6 Buchstaben in eine Spruchschlüsselliste eingetragen und nacheinander als Spruchschlüssel verwendet. Beim Gebrauch dieser Spruchschlüssel werden die ersten drei Buchstaben als Grundstellung verwendet, die letzten drei als eigentlichen Spruchschlüssel.

1.3.1.3 CY.

Teil B regelte das Umstellen der Walzen innerhalb eines Spruches. Nach der 70. bis 130. Stelle eines Spruches von über 150 Buchstaben wurde das Chiffrieren unterbrochen, danach die Stellung der linken Walze abgelesen. Dann wurde eine neue Stellung dieser Walze gewählt, die um mindestens 5 Positionen von der abgelesenen entfernt sein sollte, ohne vorerst die Stellung dieser Walze zu verändern. Danach wurde die Gruppe „CY“ chiffriert und darauf der Buchstabe, der der vorher neu gewählten Stelle entsprach, und schliesslich der im Alphabet darauf folgende Buchstabe. Der Chiffrierer stellte sodann die linke Walze auf die gewählte neue Stellung und setzte das Chiffrieren des Spruches fort. Es handelt sich um eine Variante des o.g. Influenzbuchstabens.


— 12a —

b) daß die Blattfedern der Schlüsselwalzen eingreifen sollen
bei Walze I neben dem Buchstaben B,
bei Walze II neben der Zahl 10,
bei Walze III neben der Zahl 31,
bei Walze IV neben der Zahl 65,
bei Walze V neben den Buchstaben AZ.

21. Man unterscheidet 3 Arten von Schlüsselzahlen:
die Schlüsselzahl für den Funkschlüssel C, Allgemein.
die Schlüsselzahl für den Funkschlüssel C — Offizier,
die Schlüsselzahl für den Funkschlüssel C — Stab
(siehe auch Ziffer 41).

22. Die Schlüsselzahl ist ein 5-6stelliger ~~Ausdruck~~ satzlos aus Buchstaben und Zahlen. Sie gibt an, welche 3 Schlüssel~~zahlen~~ in den Funkschlüssel eingesetzt werden sollen und welche Reihenfolge sie von links nach rechts einnehmen sollen.

Die Schlüsselzahl C 58 21 bedeutet z. B., daß die nach der Grundzahl eingestellten Walzen I, III, II in dieser Reihenfolge von links nach rechts in den Funkschlüssel eingesetzt werden, und daß sie zu Beginn des Schlüsselns und Entschlüsselns so gedreht werden sollen, daß die Schlüsselzahl C 58 21 in den Fenstern des Gehäuses sichtbar wird.

23. Schlüsselzahl für den Funkschlüssel C Allgemein.

Diese Schlüsselzahlen sind in einer besonderen Tafel zusammengestellt. Die Tafel enthält mehrere Spalten für Schlüsselzahlen (A—F), wovon jeweils nur eine Spalte in Kraft ist.

Der Kopf dieser Tafel enthält folgende Angaben:

A	B	C	zugehörige Seiten des Kenngruppenbuches	D	E	F
54 AD 09	33 N AG	AF 87 34	1	23 H 77	AL 15 38	K 69 06
43 AJ 04	44 H AN	AC 64 58	2	26 G 61	AY 11 51	R 80 19
31 AE 27	57 P AG	AA 73 50	3	28 M 63	AX 01 42	U 81 12

Abbildung 1.7: Chiffriervorschrift

1.3.2 Marine

1.3.2.1 Funkschlüssel C

Das Chiffrierverfahren der Marine war von Anfang an (1926) wesentlich komplizierter angelegt als das beim Heer (bzw. später der Luftwaffe). Bei dem „Funkschlüssel C“ (S. 3) von 1926 war, anfangs i.a. für mehrere Monate, eine Grundzahl festgelegt, dazu jeweils Schlüsselzahlen für die Verfahren „C Allgemein“, „C Offizier“ und „C Stab“. Eine solche Grundzahl konnte folgendes Aussehen haben: Alpha `B 10 31 65 AZ`. Das hiess: Umkehrwalze in Stellung Alpha, die Ringstellungen der einzelnen Walzen I bis V, identifizierbar an den Ringbezeichnungen, waren mit `B, 10, 31, 65` und `AZ` einzustellen. Wenn nun die Schlüsselzahlen lauteten: `C 58 21`, so hiess dies, dass v.l.n.r. die Walzen I, III und II in die Grundstellungen `C, 58` und `21` gedreht werden mussten. Die Schlüsselzahlen wurden einer Schlüsselzahlentafel entnommen. Diese enthielt in sechs Spalten

(A bis F) jeweils Schlüsselzahlen, in einer weiteren Spalte die zugehörige Seite eines Kenngruppenbuches.

Für einen bestimmten Zeitraum war nur eine Spalte aus A bis F in Kraft. Der Chiffrierer hatte für jeden Spruch eine Seite des Kenngruppenbuches zu wählen, damit waren die Schlüsselzahlen für den Spruch festgelegt. (Abb. 1.7) Aus dem Kenngruppenbuch wurden zwei Kenngruppen gewählt, die dem Empfänger die Seite - und damit den Spruchschlüssel - angaben. Der Klartext selbst wurde vorchiffriert nach einem Codebuch, das aus vierstelligen Buchstabengruppen bestand, einschliesslich der Buchstaben `Ä`, `Ö` und `Ü`. Zur Tastatur bzw. zum Stromweg siehe Kap. 1.1.
Diese Codegruppen wurden nach Uhrzeit, Codegruppe für Empfänger und Anzahl der Vierergruppen durch Eintasten in die ENIGMA chiffriert, der Geheimtext mit der Absenderkennung abgeschlossen.

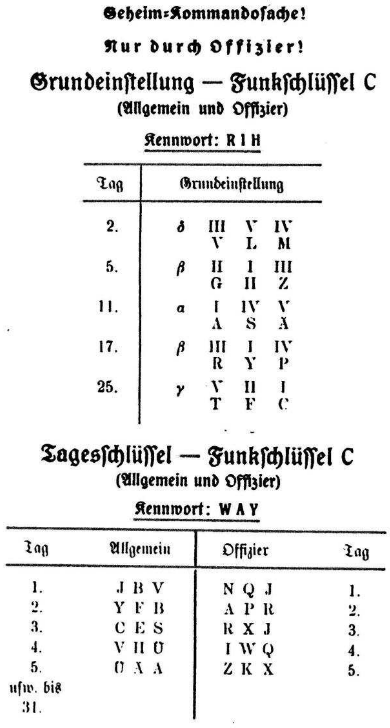
Für die Verfahren „Offizier“ und „Stab“ wurden besondere Schlüsselzahlen zugeteilt.

Anfang 1930 wurde die Sicherheit des Funkschlüssels C in einer Untersuchung durch Oberleutnant z.S. LUCAN verneint[55].

Daher trat mit der Marine-Dienstvorschrift M.Dv.Nr. 21 vom 15.7.1933 der unter 1.1 erwähnte veränderte Funkschlüssel C in Kraft. Die fünf Chiffrierwalzen trugen nun auf den Ringen einheitlich die Buchstaben `A...Z`, `Ä` und `Ü`. Wie vorher - und auch später - bestanden drei Sicherheitsstufen: Allgemein, Offizier und Stab.
Die Schlüsselunterlagen waren

die Grundstellung[56],
der Tagesschlüssel
das F. u. K.- Buch (Geheime Marinefunknamenliste und Kenngruppenbuch)

Grundstellung und Tagesschlüssel wurden für mehrere Monate für die einzelnen Verfahren getrennt nach Monaten in Umschlägen unter Kennwort (jeweils für einen Monat) ausgegeben.



Geheim-Kommandosache!

Nur durch Offizier!

Grundeinstellung — Funkschlüssel C
(Allgemein und Offizier)

Kennwort: R I H

Tag	Grundeinstellung
2.	δ III V IV V L M
5.	β II I III G H Z
11.	α I IV V A S Ä
17.	β III I IV R Y P
25.	γ V II I T F C

Tagesschlüssel — Funkschlüssel C
(Allgemein und Offizier)

Kennwort: W A Y

Tag	Allgemein	Offizier	Tag
1.	J B V	N Q J	1.
2.	Y F B	A P R	2.
3.	C E S	R X J	3.
4.	V H Ü	I W Q	4.
5.	Ü Ä A	Z K X	5.
usw. bis 31.			

Abbildung 1.8: Tagesschlüssel

Die Grundstellung („Innere Einstellung“) bestand aus der Stellung der Umkehrwalze, der Lage der Walzenringe und der Walzenlage. Der Wechsel der Grundstellung erfolgte durchschnittlich in jeder Woche einmal, 1200 Uhr am jeweils befohlenen Tag. Die Liste enthielt in einer Spalte den Tag des Einstellungswechsels, daneben die zugehörige Grundstellung, z.B.

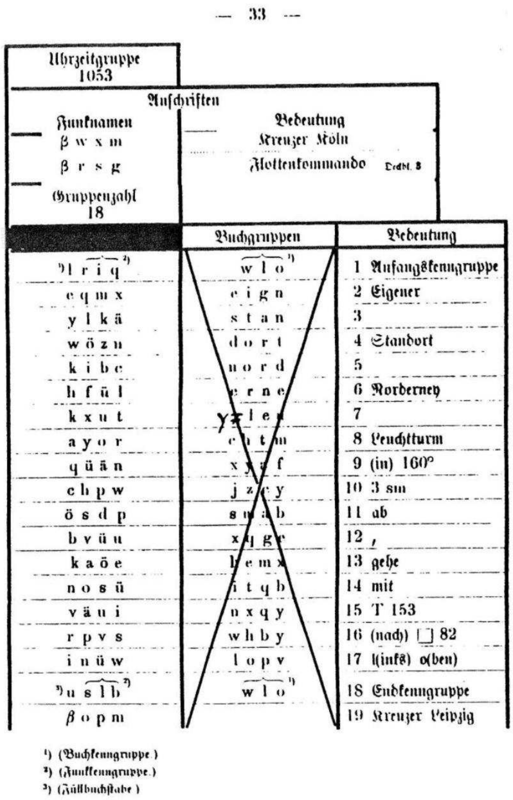
5. β II I III
`G H Z`

Die Grundstellungen waren für „Allgemein“ und für „Offizier“ gleich, für „Stab“ wurde für jeden Monat eine besondere Grundstellung mit einem Tagesschlüssel ausgegeben. (Abb 1.8)
Der Tagesschlüssel war eine dreistellige Buchstabengruppe, die mit Hilfe der Stellräder an den Sichtfenstern einzustellen war („Äussere Einstellung“). Die Tagesschlüssel wurden für einen Monat für jeden Tag in einer Liste ausgegeben.

[55] Arbeitspapier des Chefs der Marineleitung A III h 248/1930 GKdos vom 7.2.1930: „Neue Chiffriermaschine für die Marine“

[56] Die Grundstellung wird verschiedentlich in den Dienstvorschriften Grundeinstellung genannt

Für Auslandsschiffe wurden besondere Schlüssel ausgegeben, Tagesschlüssel auch für einen Monat, die Grundstellungen aber für sechs Monate auf einem Blatt.
Im Gegensatz zum vorhergehenden Schlüssel C wurde nunmehr der Klartext unmittelbar chiffriert. Kenngruppen dienten zur Bezeichnung der Schlüsselart (Allgemein, Offizier oder Stab). Sie wurden aus dem F.u.K.-Buch als Buchgruppen gelesen und mit dem Tagesschlüssel in Funkgruppen umgewandelt. Da sie nur dreistellig waren, musste noch ein vierter Buchstabe davorgesetzt werden, um Vierstelligkeit zu erlangen. Der Buchstabe `x` sollte an beliebiger Stelle in den Text eingestreut werden, seine Häufigkeit sollte die der seltenen Konsonanten nicht überschreiten. Die Ziffern 1 bis 0 wurden durch die in `y...y` eingeschlossenen Buchstaben `a` bis `j` ausgedrückt (oder zwischen `y...y` in Buchstaben ausgeschrieben). Für die Vorbereitung der Übermittlung wurde der Spruch in Vierergruppen in ein Formular eingetragen (Buchgruppen). (Abb 1.9)



— 33 —

Uhrzeitgruppe 1053

Anschriften

Funknamen	Bedeutung
β w x m	Kreuzer Köln
β r s g	Flottenkommando Deckbl. 8
Gruppenzahl 18	

	Buchgruppen	Bedeutung
³) l r i q ²)	w l o ¹)	1 Anfangskenngruppe
e q m x	e i g n	2 Eigener
y l k ä	s t a n	3
w ö z n	d o r t	4 Standort
k i b e	n o r d	5
h f ü l	e r n e	6 Norderney
k x u t	y x l e	7
a y o r	c h t m	8 Leuchtturm
q ü ä n	x y a f	9 (in) 160°
c h p w	j z e y	10 3 sm
ö s d p	s m a b	11 ab
b v ü u	x q g r	12 ,
k a ö e	h e m x	13 gehe
n o s ü	i t q b	14 mit
v ä u i	n x q y	15 T 153
r p v s	w h b y	16 (nach) ☐ 82
i n ü w	l o p v	17 l(inks) o(ben)
³) u s l b ²)	w l o ¹)	18 Endkenngruppe
β o p m		19 Kreuzer Leipzig

¹) (Buchkenngruppe)
²) (Funkkenngruppe)
³) (Füllbuchstabe)

Abbildung 1.9: Chiffrierformular

Die Buchkenngruppe wurde zweimal nacheinander mit dem Tagesschlüssel überchiffriert, die eine Hälfte (+ ein Füllbuchstabe) wurde dem Spruch vorangestellt, die zweite Hälfte (+ ein Füllbuchstabe) ans Ende (Funkkenngruppen). Mit Hilfe der Buchkenngruppe als Grundstellung wurde der eigentliche Text chiffriert und in Vierergruppen (Funkgruppen) in das Formular eingetragen. Allem voran kam der Kopf mit Uhrzeit, Anschrift und Absender (Dreiergruppen aus dem F.u.K-Buch mit vorgeschaltetetem β) und die Gruppenzahl.

Im Verfahren Offizier (Stab) wurde statt des allgemeinen Tagesschlüssels der Tagesschlüssel C-Offizier bzw. C-Stab angewandt. Die Funkkenngruppe wurde jedoch mit dem Tagesschlüssel C-Allgemein ermittelt.

1.3.2.2 Schlüssel M

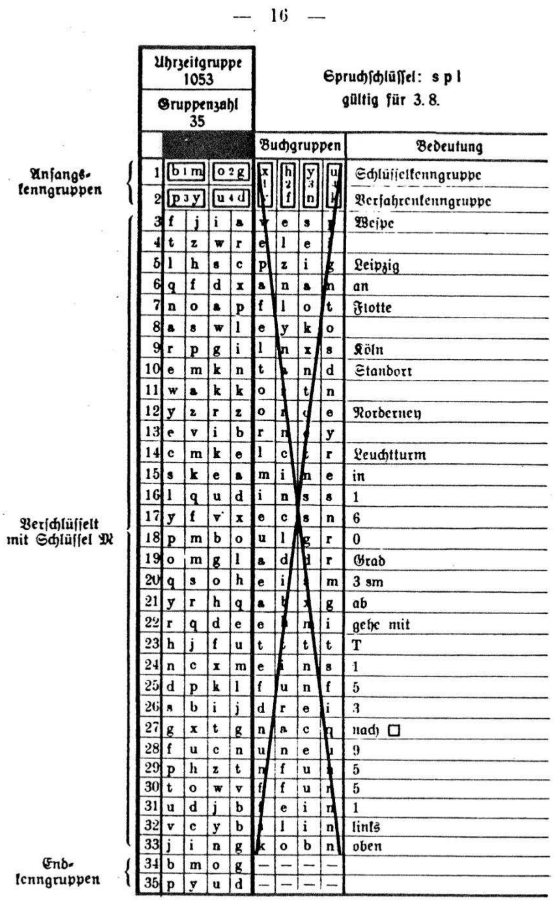
Mit dem 1.Oktober 1934 änderte sich das Chiffrierverfahren insofern, dass jetzt auch bei der Marine als „Funkschlüssel M“ die beim Heer eingeführte Chiffriermaschine ENIGMA I mit Walzen mit je 26 Buchstaben und einem Steckerbrett benutzt wurde[57]. Zum Funkschlüssel M gehörten (mit Sicherheit ab Mitte 1936[58]) die sieben Chiffrierwalzen Walze I bis VII, von denen jedoch die Nrn. IV bis VII noch nicht benutzt werden durften.

Der Schlüssel M war das Hauptchiffriermittel für die Funksprüche der Marine. Beim Verfahren selbst hatte sich zunächst nicht viel geändert, abgesehen von einem neuen F.u.K.-Buch, (da die Umlaute in den Kenngruppen nicht mehr auftauchten) und den zusätzlich für die äussere Einstellung angegebenen sechs Steckerpaaren. Das Deckblatt 11 vom 7.1.1937 zum Funkschlüssel M sagt aus, dass Zahlen

[57]Marine-Dienstvorschrift M.Dv.Nr.32 vom August 1934
[58]Deckblätter N. 1 bis 6 vom 18. Mai 1936

zwischen y...y zu setzen seien. Sie wurden von 1 bis 9 entsprechend der obersten Tastenreihe `Q, W, E, R, T, Z, U, I, O, P ... - 0` bei Taste `P` ausgedrückt. Dies ist ein Hinweis auf Geräte, bei denen die entsprechenden Tasten mit Buchstaben und mit Ziffern gekennzeichnet waren. Die Zahlengruppe musste — mit der Hervorhebung — zweimal nacheinander gegeben werden.

Es gab viele lange Sprüche in mehreren Teilen, die sich durch den Anfang `FORT` mit anschliessender Zeitgruppe des ersten Teils als zusammengehörig zeigten. Vom bekannten Beispiel „`FORT 2330`“ rührte die Bezeichnung „`FORT YWEEPYYWEEPY`“ in der Literatur her. Natürlich lieferten diese fortgesetzten Sprüche über diese allen Teilsprüchen gemeinsame Gruppe dem unbefugten Dechiffrierer vermuteten Klartext bis Mitte 1937. Anfang 1940 sagte der kriegsgefangene Funkmaat Meyer aus, dass ab Mitte 1937 Zahlen voll in Worten ausgedrückt wurden. Ab Oktober 1937 war der jeweils befohlenen Schlüsselwechsel 1200 Uhr, danach wieder 0000 Uhr[59]. In späteren Jahren war er wieder auf 1200 Uhr festgesetzt[60], allerdings galt die Grundeinstellung („Innere Einstellung“) jeweils für zwei Tage, was eine wesentliche Schwäche des Marine-Chiffrier-Systems darstellte. In der Regel sollten Sprüche nicht mehr als 80 Gruppen enthalten. Bei der Aufteilung eines zu langen Spruches musste durch die letzte Gruppe ‚fort‘ auf die Fortsetzung hingewiesen werden, der Folgespruch hatte mit ‚fort‘ und der Uhrzeitgruppe des vorangehenden Teils den Anschluss zu definieren. Am 1.5.1937 trat ein neues Indikatorsystem in Kraft, von dem allerdings keine Spur in alten deutschen Dienstvorschriften zu finden ist. Die einzige Quelle ist TURING[61]. Dieses Verfahren war eine Vorwegnahme des in der M.Dv.Nr. 32/1 angeordneten Vorgehens. Insofern datiert die Verwendung der ENIGMA M 3 bereits ab 1.5.1937.


— 16 —

Uhrzeitgruppe 1053

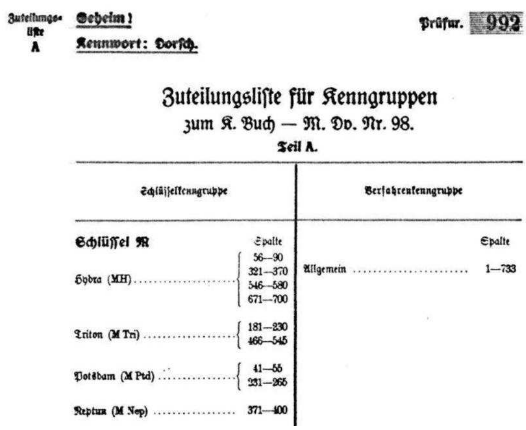
Gruppenzahl 35

Spruchschlüssel: s p l
gültig für 3. 8.

Anfangskenngruppen: 1–2
Verschlüsselt mit Schlüssel M: 3–33
Endkenngruppen: 34–35

					Buchgruppen				Bedeutung
1	b 1 m		o 2 g		x	h	y	u	Schlüsselkenngruppe
2	p 3 y		u 4 d			f	n	k	Verfahrenkenngruppe
3	f	j	i	a	w	e	s	p	Wespe
4	t	z	w	r	e	l	e		
5	l	h	s	c	p	z	i	g	Leipzig
6	q	f	d	x	a	n	a	n	an
7	n	o	a	p	f	l	o	t	Flotte
8	a	s	w	l	e	y	k	o	
9	r	p	g	i	l	n	x	s	Köln
10	e	m	k	n	t	a	n	d	Standort
11	w	a	k	k	o		t	n	
12	y	z	r	z	o	r	d	e	Norderney
13	e	v	i	b	r	n	e	y	
14	c	m	k	e	l	c	t	r	Leuchtturm
15	s	k	e	a	m	i	n	e	in
16	l	q	u	d	i	n	s	s	1
17	y	f	v	x	e	c	s	n	6
18	p	m	b	o	u	l	g	r	0
19	o	m	g	l	a	d	d	r	Grad
20	q	s	o	h	e	i	s	m	3 sm
21	y	r	h	q	a	b	x	g	ab
22	r	q	d	e	e	b	n	i	gehe mit
23	h	j	f	u	t	t	t	t	T
24	n	c	x	m	e	i	n	s	1
25	d	p	k	l	f	u	n	f	5
26	s	b	i	j	d	r	e	i	3
27	g	x	t	g	n	a	c	h	nach □
28	f	u	c	n	u	n	e	u	9
29	p	h	z	t	n	f	u	n	5
30	t	o	w	v	f	f	u	n	5
31	u	d	j	b	f	e	i	n	1
32	v	c	y	b	s	l	i	n	links
33	j	i	n	g	k	o	b	n	oben
34	b	m	o	g	—	—	—	—	
35	p	y	u	d	—	—	—	—	

Abbildung 1.10: Chiffrierformular


Zuteilungsliste A

Geheim!

Kennwort: Dorsch.

Prüfnr. 992

Zuteilungsliste für Kenngruppen
zum K. Buch — M. Dv. Nr. 98.

Teil A.

Schlüsselkenngruppe	Spalte	Verfahrenkenngruppe	Spalte
Schlüssel M		Allgemein	1—733
Hydra (MH)	56—90, 321—370, 546—580, 671—700		
Triton (M Tri)	181—230, 466—545		
Potsdam (M Ptd)	41—55, 231—265		
Neptun (M Nep)	371—400		

Abbildung 1.11: Kenngruppen Teil A

[59]Deckblätter Nr. 17 bis 20 vom 26.8.1937 zum Funkschlüssel M; später handschriftliche Änderungen
[60]M.Dv.Nr. 32/3, Der Schlüssel M, Allgemeine Bestimmungen, 1941
[61]NARA Dokument Box CBCB55, Nr.964 «TURING's Treatise on ENIGMA», Kap. 6

Geheim! Prüfnr. 992

Kennwort: Haifisch.

Zuteilungsliste für Kenngruppen
zum K. Buch — M. Dv. Nr. 98.

Teil B.

Schlüsselkenngruppe	Verfahrenkenngruppe	
	Schlüssel M	R. H. V.
Spalte	Spalte	Spalte
1—100 M Triton (M Tri)	1—733 Allgemein	1—564 Allgemein
101—130 M Neptun (M Nep)		565—733 Offizier
131—180 M Hydra (MH)		
181—200 M Aegir (MA)		
201—225 R. H. V.		
226—275 Schiffssonderschlüssel*) (MS)		
276—305 M Triton (M Tri)		
306—355 M Hydra (MH)		

Abbildung 1.12: Kenngruppen Teil B

Die Folgevorschrift ist bekannt[62]. Sie bestimmte u.a., dass die Umlaute `ä`, `ö`, `ü` durch `a`, `o`, `u` zu ersetzen waren, `ch` durch `c`, Quadrat durch `qu`, Grossquadrat durch `grqu`. Wenn bei Abkürzungen von Dienststellen die Gefahr bestand, dass durch Fehlaufnahme eines Buchstabens Verwechslungen entstehen könnten, wurde der Buchstabe verdreifacht : z.B. B.d.U.: `bduuu`. An- und Unterschriften waren aus der Funknamenliste zu entnehmen und nach einem β (Beta) offen zu senden. Wenn die Unterschrift nötig war, war diese ohne Trennung mittels ‚von von' am Ende des Spruchs mit zu chiffrieren. Zahlen waren in Buchstaben auszuschreiben. Für das Dringlichkeitszeichen `ssd` am Spruchanfang waren Tarnworte wie `bine`, `wespe`, `mucke` oder `muke` zu verwenden. Zur Verlängerung von Sprüchen waren nach drei oder vier beliebigen gleichen Buchstabenpaaren neutrale Wörter anzufügen.

1.3.2.3 Kenngruppen.

	51	52	53	54	55	56
1	WDP	IKZ	QDX	ZBU	OML	DXB
2	PCF	GFG	JVA	UVT	DIJ	IUT
3	UWZ	OUV	YTT	JFQ	FYY	LPQ
4	IGJ	LBQ	XMR	CYY	LUA	XFK
5	NBX	TND	SHC	GNE	RNQ	TQG
6	SYC	YPH	MBJ	OJA	XCK	NKK
7	FEV	RZT	FWW	XZG	JOP	ADX
8	BHD	AWC	PLD	AUO	MXE	FTH
9	KIU	FLS	CZO	MHI	ULW	QGR
10	RTJ	KRX	IQY	EUF	PZI	ZIO

GH A	228	16	GI A	327	2	GJ A	283	24	GK A	447	3	GL A	649	7
B	667	18	B	704	24	B	654	17	B	463	24	B	250	16
C	292	20	C	125	13	C	572	16	C	675	8	C	20	17
D	45	20	D	462	4	D	25	19	D	140	6	D	491	9
E	469	21	E	719	14	E	629	3	E	578	23	E	401	7
F	331	6	F	22	4	F	346	13	F	34	16	F	727	15
G	445	11	G	374	1	G	684	1	G	633	24	G	189	16
H	78	17	H	181	8	H	475	1	H	188	13	H	696	24
I	611	6	I	210	11	I	116	23	I	354	6	I	622	20
J	111	15	J	499	19	J	269	7	J	534	24	J	143	3
K	680	8	K	289	7	K	74	5	K	222	20	K	317	14
L	260	12	L	144	20	L	501	18	L	710	1	L	370	15
M	723	15	M	427	4	M	435	22	M	310	3	M	270	12

Abbildung 1.13: Kenngruppenbuch

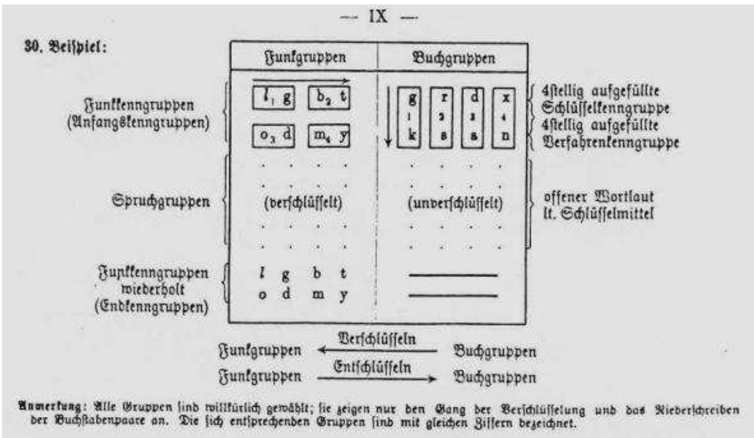
Der Klarspruch war in Vierergruppen zu teilen, und diese waren auf dem Schlüsselzettel als Buchgruppen einzutragen (Abb. 1.10). Aus einer (ab 1943 durch ein Kennwort in Kraft gesetzten) Zuteilungsliste für Kenngruppen wurden für den jeweiligen Schlüsselbereich gültige Spalten zum Auswählen der Schlüsselkenngrupppen und der Verfahrenkenngruppen entnommen. (Abb. 1.11) Für die „Rückübersetzung" der Schlüsselkenngruppe in den Schlüsselbereich diente Teil B der Zuteilungsliste für Kenngruppen (Abb. 1.12) Bei der Zuteilungsliste ist kritisch anzumerken, dass die Zuordnung von jeweils Blöcken von Schlüsselkenngruppen anstelle von zufällig gestreuten Kenngruppenzahlen die Identifizierung der Schlüssel erleichterte. Für die Schlüsselkenngruppe und die Verfahrenskenngruppe waren verschiedene Spalten zu wählen. Die Kenngruppen selbst wurden aus dem Teil A, der Spaltenliste, in der gewählten Spalte ausgesucht. Für jeden Funkspruch mussten andere Kenngruppen verwendet werden. Beide Kenngruppen wurden in die Spalte

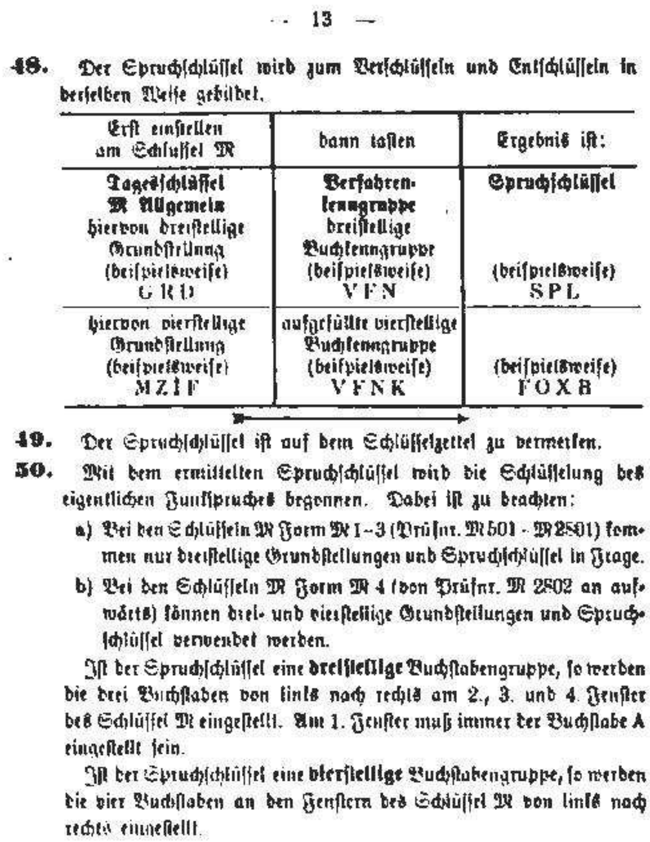
[62] Der Schlüssel M Verfahren M Allgemein, Berlin 1940, M.Dv.Nr. 32/1

Buchgruppen eingetragen und vierstellig ergänzt. An welcher Stelle die Ergänzung an- oder einzufügen war, wurde in der Zuteilungsliste angeordnet.(Abb 1.11) Es scheint nach den vorgefundenen Unterlagen, dass hier überwiegend für die erste Buchgruppe die erste Stelle und für die zweite Buchgruppe die vierte Stelle benutzt worden wäre.

Aus dem Kenngruppenbuch mussten zwei dreistellige Gruppen entnommen werden: Die Schlüsselkenngruppe und die Verfahrenkenngruppe. (Abb. 1.13) Aus dem Tauschtafelplan zu den Bigrammtauschtafeln für Kenngruppen war aus der für den Monat befohlenen Spalte und für den Monatstag der Buchstabe der Tauschtafel zu entnehmen. Bei dreistelliger Grundstellung gewann man den Spruchschlüssel durch Eintasten der dreistelligen Verfahrenkenngruppe mit dem auf den Tagesschlüssel eingestellten Funkschlüssel. Entsprechend erhielt man bei vierstelliger Grundstellung einen vierstelligen Spruchschlüssel durch Eintasten der um einen Buchstaben ergänzten Verfahrenkenngruppe. (Abb. 1.14 unten) Die Umwandlung der Buchkenngruppen in Funkkenngruppen erfolgte mit Hilfe der Tauschtafeln nach dem Schema der Abbildung 1.14 oben. Beide Funkgruppen bildeten Anfang und Ende jedes Spruches. Die im Laufe der Zeit geltenden Zuteilungslisten für Kenngruppen waren (in Klammer Beginn der Gültigkeit):

ohne Namen	(29.11.41)
Forelle	(10.02.43)
Zander	(07.11.43)
Haifisch	(01.02.44)
Dorsch	(21.04.44)
Hering	(20.06.44)
Zander	(10.08.44)
Forelle	(15.10.44)
Haifisch	(30.12.44)
Hering	(04.03.45)





— 13 —

48. Der Spruchschlüssel wird zum Verschlüsseln und Entschlüsseln in derselben Weise gebildet.

Erst einstellen am Schlüssel M	dann tasten	Ergebnis ist:
Tagesschlüssel M Allgemein hiervon dreistellige Grundstellung (beispielsweise) G R D	**Verfahrenkenngruppe** dreistellige Buchkenngruppe (beispielsweise) V F N	**Spruchschlüssel** (beispielsweise) S P L
hiervon vierstellige Grundstellung (beispielsweise) M Z I F	aufgefüllte vierstellige Buchkenngruppe (beispielsweise) V F N K	(beispielsweise) F O X B

49. Der Spruchschlüssel ist auf dem Schlüsselzettel zu vermerken.

50. Mit dem ermittelten Spruchschlüssel wird die Schlüsselung des eigentlichen Funkspruches begonnen. Dabei ist zu beachten:

a) Bei den Schlüsseln M Form M 1–3 (Prüfnr. M 501 - M 2501) kommen nur dreistellige Grundstellungen und Spruchschlüssel in Frage.

b) Bei den Schlüsseln M Form M 4 (von Prüfnr. M 2802 an aufwärts) können drei- und vierstellige Grundstellungen und Spruchschlüssel verwendet werden.

Ist der Spruchschlüssel eine **dreistellige** Buchstabengruppe, so werden die drei Buchstaben von links nach rechts am 2., 3. und 4. Fenster des Schlüssel M eingestellt. Am 1. Fenster muß immer der Buchstabe A eingestellt sein.

Ist der Spruchschlüssel eine **vierstellige** Buchstabengruppe, so werden die vier Buchstaben an den Fenstern des Schlüssel M von links nach rechts eingestellt.

Abbildung 1.14: Tauschvorschrift

Unterschieden von den Funksprüchen wurden, soweit der Schlüssel M verwendet wurde, die Funksignale Flottenfunksignal, Kurzsignal, Ortungsfunksignal und Kurzfunkwetter. Beim Flottenfunksignal, gekennzeichnet durch die Anfangsgruppe Alpha Alpha, wurde die Grundstellung zur

Einstellung des Schlüssels M durch eine Kennzahl des Funksignalschlüssels bestimmt[63]. Die äussere Form eines Funkspruchs nach Schlüssel M war also[64]

1536/16/38	Uhrzeitgruppe,ggf. Datum, Leitnummer
46	Gruppenzahl
`bxda xhbs`	Anfangskenngruppen
`rdyf ...`	Funkgruppen
`bxda xhbs`	Endkenngruppen

Als Beispiel werde ein Original-Flottenfunksignal angegeben:[65]

```
α α
129 IWS 0125/11/773
B O I E F R L D X T P H C T P G U B H I E G O Q B O
P Q G D G E R V L E O F C W N V X H V V O H Z O A R
T J P I B B C F G I R O
```

Der Klartext lautet hier

```
l u c i e d e l t a y g u s t a v g e l b y q u a t
s c h a c h t z w o d r e i s i e b e n p i c a e s
a r z w o n e u n l b s
```

Erklärung: `129`: Indikator für die Walzenstellungen (`OUK`), `IWS`: Indikator für Schlüsselbereich (hier: „Hydra“), `0125/11`: 01.25 Uhr am 11. (April 1944), `773`: Leitnummer.
`G` Gelb: Feindlicher Geleitzug gesichtet, `quatsch „ = Q“` 8237: 71,27ø Nord, 07,10ø Ost. Rest : Unterschrift.

1.3.2.4 Schlüsselbereiche.

1941 bestanden drei wesentliche Schlüsselbereiche, (die Bezeichnungen der Alliierten in «»):
M Heimisch, später „Hydra“, «Dolphin» , M Ausserheimisch, später „Ägir“, «Pike»
M Süd, später „Hermes“, «Porpoise»
Ende 1941 wurde M Heimisch aufgespalten in

M Schnellboote (Ostsee), später „Sleipnir“ ; U-Übungsschlüssel, später „Thetis “
M-„Hydra“ für Ostsee, Norwegen, Kanal
M Süd wurde aufgespalten in

Schiffssonderschlüssel, besonderer Schlüssel für jedes Schiff
Schlüssel für Blockadebrecher Fernost, später „Tibet“, «Sunfish»
Schlüssel für Marine-Attach Berlin-Tokio, „Bertok“, «Seahorse»

November 1942 wurde von „Hydra“ der Schlüssel M 4 „Triton“, «Shark» abgespalten für Atlantik-U-Boote, für die U-Boote im Mittelmeer entstand Mitte 1943 der Schlüssel M „Medusa“, «Turtle» . Weiter kamen 1943/1944 hinzu:[66]

M „Uranus“, «Trumpeter» für die Balkanregion; M „Freya“ als Sonderschlüssel des OKM
M „Poseidon“, «Grampus», für das Schwarze Meer; M „Potsdam“, «Plaice» für die östliche Ostsee
M „Niobe“, «Narwhal», von „Hydra“ abgespalten für U-Boote Norwegen
M „Hydra“ wurde — zumindest zeitweise im August 1944 — aufgespalten in
M „Hydra I“, „Hydra II“, „Hydra I“, von den Alliierten «Sucker» genannt, wurde der Schlüssel für die Festungen am Kanal.
M „Brennessel“, «Sucker» für Westfrankreich, ebenso M „Schachtelhalm“, „Stranddistel“
M „Hermes“ wurde seinerseits aufgespalten in
M „Wotan“, «Bloater» für die Adria und in M „Athena“ , «Catfish» für die Ägäis.
M „Eichendorff“, „Kleist“, «Bonito» Klein-U-Boote, Sabotage-Trupps.

---

[63] Signalschlüssel für den Funksignaldienst (Funksignalschlüssel) (Ausgabe Oktober 1939)
[64] aus: Nachrichtenvorschrift der Kriegsmarine (NV), Heft II, M.Dv.Nr. 922, Berlin 1943, S. 46
[65] Dieser Spruch stammt aus NARA Dokument Box ZEMA20, Nr. 4457 «The German Naval Ciphers», S. 104. Der angegebene Klartext ist ist aber offenbar überarbeitet, denn der 46. Buchstaben `V` liefert bei der Dechiffrierung `g` statt `n`.Der Spruch ist auch im Internet veröffentlicht. Die Walzenlage ist I, VII, V, die Grundstellung `O U K`, die Umkehrwalze ist `B`, die Steckverbindungen sind `(AI), (CF), (DG), (EJ), (OK), (PY), (RM), (SW), (TU), (NQ).`
[66] Schlüssel M, K.T.B.-Beitrag IIc, Anl.Nr. 4 zu I/Skl 33852/44gKdos.,BA/MA RM7/108

Die durch Aufspaltung entstandenen neuen Schlüssel wurden durch zyklisches Verschieben der Walzenlagen erzeugt. Das bedeutete für die alliierten Dienste nur noch das Probieren von jeweils 8 Möglichkeiten anstelle von 336[67].
Im Schlüssel „Hermes“wurden offenbar alle benutzten Walzenlagen aus der Liste aller möglichen (276, weil die 60 Lagen, in denen die Walzen VI, VII bzw. VIII nicht vorkamen, wegfielen) gestrichen, was jeden Monat die Anzahl der verfügbaren und tatsächlich benutzten um 15 verminderte — eine erhebliche Erleichterung für die alliierten Kryptologen[68].

V o r s i c h t ! Wasserlösliche Farbe!

Geheime Kommandosache! Prüfnummer: 1034

S t i c h w o r t b e f e h l

für den Schlüsselbereich " H y d r a "

Anweisung siehe

"Der Schlüssel M Allgemeine Bestimmungen - M.Dv.Nr. 32/3"

Stichwort: S k o r p i o n Kennwort: W o r m s

ab 7.5.12.00 Skorpion II Kennwort - Pirat

OKM 4/Skl IIcc 8060/44 g.Kdos.

Abbildung 1.15: Stichwortbefehl

— 22 —

Änderung der Schlüssel M auf Stichwort.

(Siehe Ziffer 25.)

100. Um bei Gefahr der Bloßstellung der Schlüssel zum Schlüssel M sofort bei allen Dienststellen eine gleichzeitige Änderung der Schlüsseleinstellungen vornehmen zu können, wird durch Befehl des O K M (Skl) ein überall bekanntes Stichwort in Kraft gesetzt, das angibt, wie die Schlüssel geändert werden müssen. Diese Stichwortbefehle sind die einzige Möglichkeit, die Schlüsselsicherheit unverzüglich wieder herzustellen. Sie erfordern größte Sorgfalt bei ihrer Anwendung. (Siehe Ziffer 115).

101. Diese Änderungen beziehen sich nur auf die Schlüssel M Allgemein.

Es werden dadurch geändert: Walzenlage,
Ringstellung und
Steckerverbindungen.

Haben andere Schlüsseltafeln Schlüsselwerte (s. Ziffer 18) mit Schlüssel M Allgemein gemeinsam, so werden diese ebenfalls durch das Stichwort geändert. Die betr. Schlüsseltafeln tragen einen entsprechenden Vermerk.

102. Als Stichwort wird entweder der Name eines Sternes oder eines Sternbildes benutzt. Das Stichwort dient nur zur Bekanntgabe der Gültigkeit, des In- und Außerkrafttretens und zur Benennung im Schriftverkehr.

103. Die einzelnen Werte der vorzunehmenden Änderungen werden durch ein Kennwort ausgedrückt, das im Stichwortbefehl genannt wird und nach folgenden Regeln auszuwerten ist. Es werden nur die ersten fünf Buchstaben des Kennwortes benutzt, die entsprechend ihrem Platz im Abc numeriert werden (s. Ziff. 107). Umlaute und zusammengesetzte Buchstaben werden als zwei Buchstaben gelesen:

ä = ae, ö = oe, ü = ue, ck = c k, ch = c h, ß = s s, qu = q u.

Bei der Auswahl der Kennworte ist auf die eindeutige Auswertung Rücksicht zu nehmen.

Deckbl. 7

17.3.43

Abbildung 1.16: Stichwortbefehl

— 23 —

104. Die gefundenen Zahlenwerte werden dann zu den planmäßigen täglichen Einstellungswerten hinzugezählt, und zwar:

die Zahl für den

1. Buchstaben zu jeder Walzennummer der Schlüsselwalzen,
2. Buchstaben zur Ringstellung der linken Schlüsselwalze,
3. Buchstaben zur Ringstellung der mittleren Schlüsselwalze,
4. Buchstaben zur Ringstellung der rechten Schlüsselwalze,
5. Buchstaben zu jeder Zahl der Steckerverbindungen.

Anmerkung:

a) Die Grundstellungen M Allgemein und die Spruchschlüssel werden durch dieses Stichwort nicht geändert.
b) Die Zusatzwalze bei den Schlüsseln Form M 4 von M 2802 an aufwärts bleibt vorläufig unberücksichtigt.

105. Bei den durch das Hinzuzählen gewonnenen Ergebnissen ist zu beachten:

Liegt das Ergebnis für die	über	so ist abzuziehen	Beispiel:	
a) Walzennummer	8	8 oder ein Vielfaches von 8 d. h. 16 bzw. 24 oder 32	III + 9 = 12, 12 − 8 = IV III + 17 = 20, 20 − 16 = IV	endgültige Walzennummer = IV
b) Ringstellung	26 (Z)	26	20(t) + 12 = 32, 32 − 26 = 6(f)	endgültige Ringstell. = f
c) Steckerverbindung	26	26	21 + 24 = 45, 45 − 26 = 19	endgültige Nummer der Steckerbuchse = 19

106. Für die Berechnung der Walzennummern sind die 8 Walzen I bis VIII zugrunde zu legen.

I = 1 (9) (17) (25) (33)	V = 5 (13) (21) (29)
II = 2 (10) (18) (26) (34)	VI = 6 (14) (22) (30)
III = 3 (11) (19) (27)	VII = 7 (15) (23) (31)
IV = 4 (12) (20) (28)	VIII = 8 (16) (24) (32)

3* Deckbl. 7

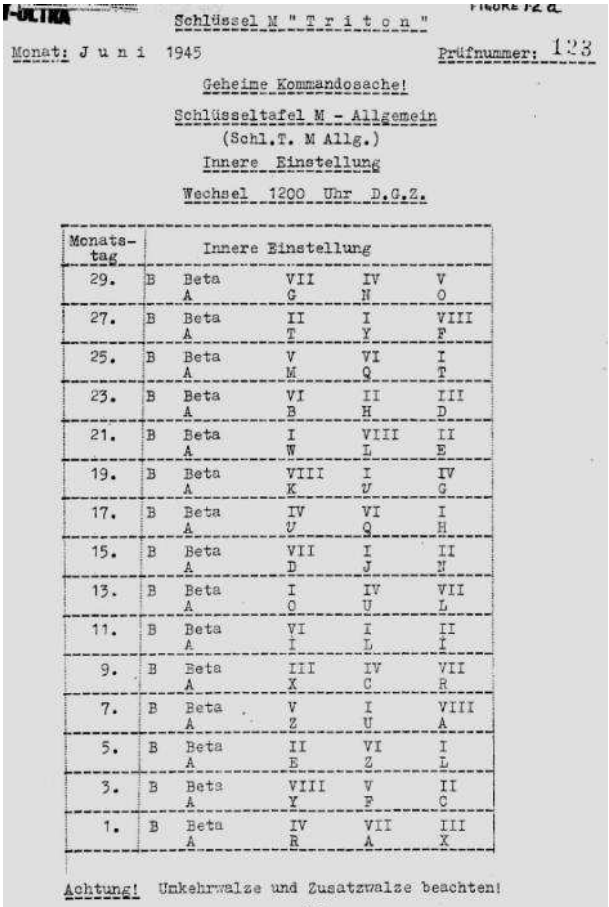
17.3.43

[67]NARA Dokument Box ZEMA20, Nr. 4457 «The German Naval Ciphers»
[68]ALEXANDER, S. 68, Abschnitt 25

1.3.2.5 Schlüssel M Allgemein.

Die Vorschrift „Der Schlüssel M Allgemeine Bestimmungen“ von 1941[69] enthält das Deckblatt 8 vom 17.3.43, in dem ausserdem die Schlüsselbereiche „Neptun“ (für Kernflotte), „Thetis“ (für taktische Übungen der U-Boote), „Sleipnir“, und die Schiffssonderschlüssel definiert wurden. Darüber hinaus wurden für die U-Boote besondere Funkschaltungen eingerichtet (z.B. Küste, Irland, Amerika), in denen jeweils die günstigsten Kurzwellen- bzw. Längswellen bestimmt wurden.

1.3.2.5.1 Stichwortbefehl. Das Deckblatt 7 vom 17.3.1943 zu M.Dv.Nr.32/3 erwähnt den Stichwortbefehl. Im Falle der Blossstellung eines Schlüssels konnte durch ein Stichwort, zu dem noch eine Kennung gehörte, die nicht mitgefunkt wurde, die Schlüssellage verändert werden. Das Stichwort selbst diente nur zur Kennzeichnung von Inkrafttreten oder Ausserkraftsetzung. Die eigentliche Änderung beruhte auf der Kennung. Beim Stichwort Andromeda wurde bei der Aktivierung des Stichwortbefehls eine Zahl kleiner als 24 mitgefunkt, die in Spalte 412 des K-Buches ein Trigramm definierte, das die vorzunehmende Änderung festlegte.



Schlüssel M " T r i t o n "

Monat: J u n i 1945 Prüfnummer: 123

Geheime Kommandosache!

Schlüsseltafel M - Allgemein
(Schl.T. M Allg.)
Innere Einstellung

Wechsel 1200 Uhr D.G.Z.

Monatstag	Innere Einstellung				
29.	B	Beta A	VII G	IV N	V O
27.	B	Beta A	II T	I Y	VIII F
25.	B	Beta A	V M	VI Q	I T
23.	B	Beta A	VI B	II H	III D
21.	B	Beta A	I W	VIII L	II E
19.	B	Beta A	VIII K	I U	IV G
17.	B	Beta A	IV U	VI Q	I H
15.	B	Beta A	VII D	I J	II N
13.	B	Beta A	I O	IV U	VII L
11.	B	Beta A	VI I	I L	II I
9.	B	Beta A	III X	IV C	VII R
7.	B	Beta A	V Z	I U	VIII A
5.	B	Beta A	II E	VI Z	I L
3.	B	Beta A	VIII Y	V F	II C
1.	B	Beta A	IV R	VII A	III X

Achtung! Umkehrwalze und Zusatzwalze beachten!

Abbildung 1.17: Schlüssel M4

Wenn das Stichwort der Name eines Sternes oder eines Sternbildes war und die Kennung eine vierstellige Zahl, dann musste diese Zahl als Grad und Minuten in der Navigationstafel aufgeschlagen werden. Die letzten drei Stellen der log-tan-Tafel wurden zur Bildung des neuen Schlüssels benutzt: die erste wurde (modulo 8) zu den Zahlen der drei Walzen addiert, die zweite zu den Ringzahlen der drei Walzen. Die dritte Zahl wurde schliesslich (modulo 26) zu allen Steckerzahlen addiert. Wenn das Stichwort ein anderes Wort war, wurden die Platznummern der ersten fünf Buchstaben des Wortes im Alphabet verwertet. Die Nummer des ersten Buchstabens wurde zu jeder Walzennummer der Chiffrierwalzen addiert, die der zweiten bis vierten zu jeder Ringstellung, die des fünften zu jeder Zahl der Steckerverbindungen. Im Beispiel der Abbildung 1.15 (Kennwort Worms) musste entsprechend Beispiel in Abb. 1.16 zur Nummer jeder Chiffrierwalze 5 addiert werden, zu den Ringstellungen die Zahlen 5, 3, 1 in dieser Reihenfolge, schliesslich zu jeder Zahl der Steckerverbindungen die Zahl 4. Wesentlich komplizierter waren die Bestimmungen zum Stichwortbefehl „Stier“zu Schlüssel Nixe, einem Sonderschlüssel der Form M Offizier[70].

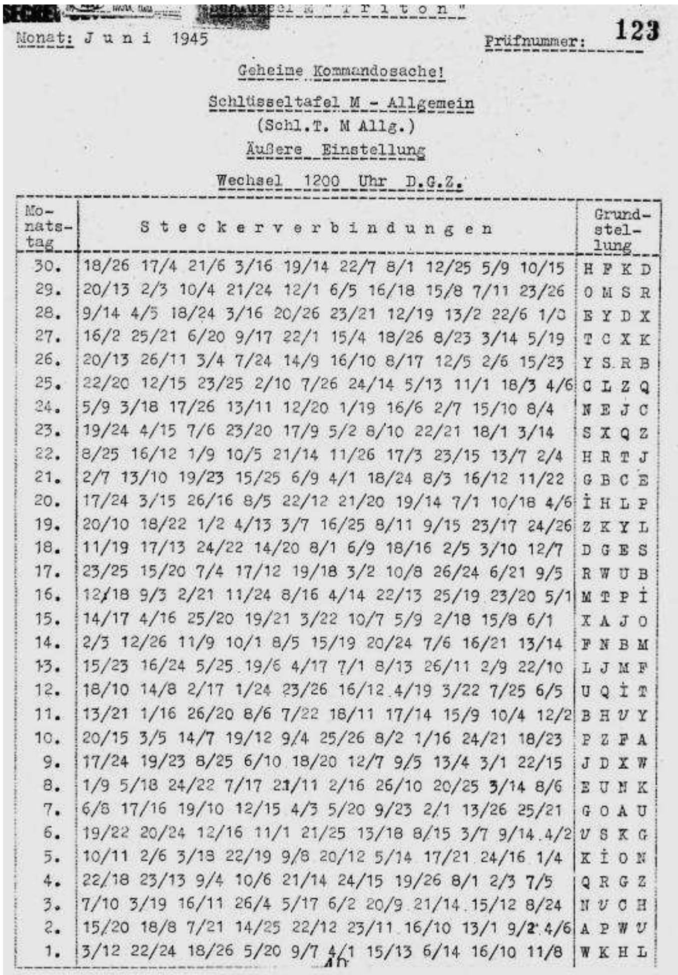
[69] M.Dv.Nr. 32/3, auch im BA/MA, RMD 4/32/3

[70] NARA Dokument Box ZEMA20, Nr.4457,«The German Naval Ciphers», S. 63 und NARA Dokument Box CBKI57, Nr. 1594 «Cipher Enigma M Nixe, Keyword ‹Stier› »

1.3.2.6 Schlüssel M Form M 4

Ab Fabriknummer M 2802 wurde der Schlüssel M als Schlüssel M Form M 4 für eine Grundstellung (und dementsprechend auch für einen Spruchschlüssel) von vier Buchstaben ausgestattet[71]. Die 4. Walzen (Griechenwalzen) konnten nach Ringstellung und Grundstellung variiert eingesetzt werden. (Siehe Kap. 1.1) Wie die Abbildungen 1.17 und 1.18[72] zeigen, sind allerdings unverständliche Ungereimtheiten bei der Ausformung der Schlüsselblätter geschehen, die den alliierten Kryptoanalytikern in die Hände gearbeitet haben: Im Gegensatz zu rein zufallsmässiger Verteilung von einer Periode von zwei Tagen zur nächsten wurde niemals eine volle Walzenanordnung wiederholt.

Die langsame Walze wurde erst wiederholt, wenn alle 8 Walzen einmal benutzt waren. Keine Walze wurde dabei innerhalb eines Monats dreimal eingesetzt. In keiner Position wurde eine Walze zweimal nacheinander benutzt. Unverständlich auch das Festhalten an der Ringstellung A bei der unveränderten Nutzung der Griechenwalze Beta. Dies verhalf bei Kurzsignalen zur Behandlung der Sprüche wie bei ENIGMA M 3. Auch bei den Grundstellungen war ein Abgehen von reiner Zufallsverteilung zu beobachten: In jeder Position trat jeder Buchstabe 22 mal auf, 4 weitere zweimal. Diese Regelmässigkeit half in vielen Fällen in der zweiten Monatshälfte zu schnellerer Ermittlung des Tagesschlüssels. Auch das Festhalten an immer 10 gesteckerten Buchstabenpaaren und somit immer 6 Buchstaben ohne Stecker erleichterte letzten Endes den alliierten Kryptoanalytikern die Arbeit.



[redacted] " T r i t o n "

Monat: J u n i 1945 Prüfnummer: 123

Geheime Kommandosache!

Schlüsseltafel M - Allgemein

(Schl.T. M Allg.)

Äußere Einstellung

Wechsel 1200 Uhr D.G.Z.

Monatstag	S t e c k e r v e r b i n d u n g e n	Grundstellung
30.	18/26 17/4 21/6 3/16 19/14 22/7 8/1 12/25 5/9 10/15	H F K D
29.	20/13 2/3 10/4 21/24 12/1 6/5 16/18 15/8 7/11 23/26	O M S R
28.	9/14 4/5 18/24 3/16 20/26 23/21 12/19 13/2 22/6 1/8	E Y D X
27.	16/2 25/21 6/20 9/17 22/1 15/4 18/26 8/23 3/14 5/19	T C X K
26.	20/13 26/11 3/4 7/24 14/9 16/10 8/17 12/5 2/6 15/23	Y S R B
25.	22/20 12/15 23/25 2/10 7/26 24/14 5/13 11/1 18/3 4/6	C L Z Q
24.	5/9 3/18 17/26 13/11 12/20 1/19 16/6 2/7 15/10 8/4	N E J C
23.	19/24 4/15 7/6 23/20 17/9 5/2 8/10 22/21 18/1 3/14	S X Q Z
22.	8/25 16/12 1/9 10/5 21/14 11/26 17/3 23/15 13/7 2/4	H R T J
21.	2/7 13/10 19/23 15/25 6/9 4/1 18/24 8/3 16/12 11/22	G B C E
20.	17/24 3/15 26/16 8/5 22/12 21/20 19/14 7/1 10/18 4/6	İ H L P
19.	20/10 18/22 1/2 4/13 3/7 16/25 8/11 9/15 23/17 24/26	Z K Y L
18.	11/19 17/13 24/22 14/20 8/1 6/9 18/16 2/5 3/10 12/7	D G E S
17.	23/25 15/20 7/4 17/12 19/18 3/2 10/8 26/24 6/21 9/5	R W U B
16.	12/18 9/3 2/21 11/24 8/16 4/14 22/13 25/19 23/20 5/1	M T P İ
15.	14/17 4/16 25/20 19/21 3/22 10/7 5/9 2/18 15/8 6/1	X A J O
14.	2/3 12/26 11/9 10/1 8/5 15/19 20/24 7/6 16/21 13/14	F N B M
13.	15/23 16/24 5/25 19/6 4/17 7/1 8/13 26/11 2/9 22/10	L J M F
12.	18/10 14/8 2/17 1/24 23/26 16/12 4/19 3/22 7/25 6/5	U Q İ T
11.	13/21 1/16 26/20 8/6 7/22 18/11 17/14 15/9 10/4 12/2	B H V Y
10.	20/15 3/5 14/7 19/12 9/4 25/26 8/2 1/16 24/21 18/23	P Z F A
9.	17/24 19/23 8/25 6/10 18/20 12/7 9/5 13/4 3/1 22/15	J D X W
8.	1/9 5/18 24/22 7/17 21/11 2/16 26/10 20/25 3/14 8/6	E U N K
7.	6/8 17/16 19/10 12/15 4/3 5/20 9/23 2/1 13/26 25/21	G O A U
6.	19/22 20/24 12/16 11/1 21/25 13/18 8/15 3/7 9/14 4/2	V S K G
5.	10/11 2/6 3/18 22/19 9/8 20/12 5/14 17/21 24/16 1/4	K İ O N
4.	22/18 23/13 9/4 10/6 21/14 24/15 19/26 8/1 2/3 7/5	Q R G Z
3.	7/10 3/19 16/11 26/4 5/17 6/2 20/9 21/14 15/12 8/24	N V C H
2.	15/20 18/8 7/21 14/25 22/12 23/11 16/10 13/1 9/2 4/6	A P W V
1.	3/12 22/24 18/26 5/20 9/7 4/1 15/13 6/14 16/10 11/8	W K H L

Abbildung 1.18: Schlüssel M4

Ein Merkblatt zum Schlüssel M Form M 4 datiert schon 1941. Das Begleitbuch für den Schlüssel M, Nr. M 15835 - am 10.5.1944 an U 1057 ausgegeben - weist zwei Zusatzwalzen (Beta bzw. Gamma) und zwei Umkehrwalzen (B und C) aus. Am 27.2.1945 war diese Ausrüstung nachweislich eines handschriftlichen Eintrages in dieses Begleitbuch noch unverändert. Von der Verwendung einer Griechenwalze Alpha oder einer Griechenwalze Delta, wie ROHWER angibt[73], fehlen Belege oder konkrete Hinweise (vgl. S. 6). Die in Abb. 4 gezeigte ENIGMA mit Schreibzusatz war verschiedentlich ab Herbst 1944 in Gebrauch.[74] Erstaunlicherweise ist im Schlüsselbereich Süd mit den Schlüsseln „Poseidon", „Uranus" und „Hermes" seit August 1941 mindestens bis Januar 1944 nicht das Kenngruppenverfahren angewandt worden, sondern das alte Chiffrierverfahren des Heeres aus der Zeit vor dem

[71] Deckblatt Nr. 7 zu Der Schlüssel M Allgemeine Bestimmungen, Berlin 1941, M.Dv.Nr. 32/3 vom 17.3.43

[72] NARA Dokument Box ZEMA20, Nr. 4457«The German Naval Ciphers» S. 39 u. 40

[73] ROHWER b), S. 341

[74] KAHN a), S. 208

15. September 1938, bei dem die Grundstellungen zur Chiffrierung des Spruchschlüssels vorgeschrieben waren. (Siehe Kap. 1.3.1)[75]. Dieses alte Chiffrierverfahren erzeugte Auffälligkeiten («females», siehe Kap. 4.2) und war für die alliierten Dienste ein Fundgrube an Erkenntnissen auch über den Landkrieg im Bereich dieses Schlüssels (bis hin nach Südrussland)[76]. Ab Juni 1944 wurde (M 4) ein 4–stelliger Schlüssel verwendet, was zur Folge hatte, dass bei der doppelten Chiffrierung von `ABCDAB` nur die ersten beiden Buchstaben für die Zyklenbildung in Frage kamen.

1.3.2.7 Offizier.

Für Sprüche, die einer besonderen Geheimhaltung bedurften, gab es das Verfahren „Offizier“[77]. Dabei wurde der Spruch mit der inneren Einstellung wie M Allgemein eingetastet, aber mit Steckerlage für M Offizier und mit einem Spruchschlüssel, der aus 26 möglichen der monatlichen Tagesschlüssel-Liste für M Offizier entnommen war (Kennbuchstaben A bis Z). Dieser chiffrierte Spruch wurde dann vom Funkpersonal um den Kopf, die Anschrift, „von“, die Unterschrift und Offizier, Schlüsselbuchstabe (z.B. Caesar) ergänzt und mit dem normalen Tagesschlüssel Allgemein nochmals chiffriert. Wenn beim Dechiffrieren eines Spruchs die Funkmannschaft auf „Offizier“ und einen Buchstaben traf, musste der Rest an einen Offizier zur weiteren Dechiffrierung abgegeben werden.

Die Tagesschlüssel-Liste galt einen Monat lang, die besonderen Stecker jeweils zwei Tage, nach August 1943 bei den U-Booten 10 Tage (wie Abb. 1.19, ohne „Innere Einstellung“, die Spruchschlüssel gültig für jeweils einen Monat).

Jedes U-Boot bekam gegen Ende des Krieges seinen eigenen Sonderschlüssel. (Abb. 1.19) Beispiele für Zuteilung von Sonderschlüsseln: Schlüssel Nr. 211 bekam U 722 (Reimers), Schlüssel 161 die U-Boot-Basis St. Nazaire, Schlüssel Nr. 282 bekam U 242 (Riedel).

Hier fällt auf, dass die für einen ganzen Monat festgelegten 26 Spruchschlüssel Monat für Monat einfach wiederholt wurden. Dies musste zu immer erneuter Benutzung ein und desselben Schlüssels führen.

Die Wiederholung eines einzigen Buchstabens in den jeweiligen Positionen der Spruchschlüssel führte dazu, dass mit zunehmender Kenntnis einzelner Schlüssel im Laufe eines Monats die mögliche Anzahl der restlichen Schlüssel zunehmend eingeschränkt wurde.

Mit Stichwort-Befehlen wie „Schatten“, „Glocke“ und „Maske“ wurden nach den alliierten Erfolgen bei der Versenkung der Versorgungsboote („Milchkühe“) besondere Schlüsselverfahren befohlen.

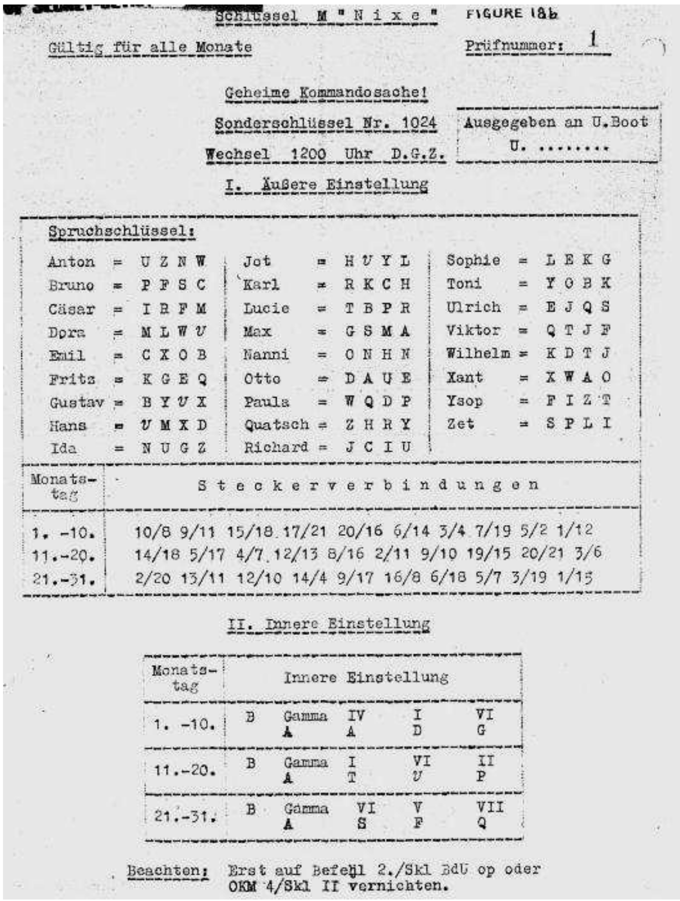
> An: Queck (U 92)
> Entschlüsseln Sie einen folgenden Spruch „Offizier“ mit den Stichwort „Glocke“ mit der folgenden Einstellung:
> 1) Bilden Sie die Einstellung Offizier mit folgenden Einstellungen:
> 3. Buchstabe des Vornamens der Mutter von Oblt. Knof; 2. Buchstabe des Vornamens des 2 WO;[78] 2. Buchstabe des Familiennamens des Arztes; Letzter Buchstabe des Familiennamens des 3 WO.
> 2) Addieren Sie zu den Steckerzahlen Offizier die erste Ziffer der Addresse des Matrosen Scherber.
> 3) Vernichten Sie diesen Befehl nach Kenntnisnahme.[79]

1.3.2.8 Kurzsignale.

Aus der Erkenntnis, dass bei jeglichem Funkverkehr immer eine Peilgefahr durch alliierte Horchstellen bestand, und unter der Annahme, dass der alliierte Peildienst dem deutschen überlegen wäre, seine günstige geografische Aufstellung der Peilstationen eine ideale Basis für Peilauswertung böte[80], wurde das teilweise schon eingeführte Kurzsignalverfahren weiter vervollkommnet.

[75] Beispiele in: Kenngruppenverfahren Süd (M.Dv.Nr. 608), S. 4, Nr. 5 und S. 9 (Spruchschlüsselverfahren Süd)
[76] ERSKINE f)
[77] M.Dv.Nr. 32/2
[78] 2. Wachoffizier
[79] NARA Dokument Box ZEMA20, Nr. 4457 «The German Naval Ciphers», S. 71
[80] Beitrag zum Kriegstagebuch der Seekriegsleitung vom 16.2.40, S. 6 (BA/MA RM 7/103, S. 18)

Angestrebt wurde eine Spruchdauer von etwa 10 Sekunden. Bekannt ist das U-Boot-Kurzsignalheft von 1940 M.Dv.Nr. 299 („FEODOR“) [81]. Für den Verkehr vom Befehlshaber der U-Boote zu den Booten gab es ab der zweiten Hälfte 1944 den Schlüssel „URSULA“.
Die Gebrauchsanweisung dazu lässt erkennen, dass die Kurzsignale i.a. nicht mehr als zwei vierstellige Gruppen enthalten sollten. Deswegen waren die Kurzsignalgruppen so konstruiert, dass sie entstümmelt werden konnten: Der dritte Buchstabe der Gruppe war im Alphabet doppelt so weit vom ersten Buchstaben entfernt wie der zweite. Jede dreistellige Gruppe des Kurzsignalheftes wurde durch Anhängen eines dem U-Boot als Unterschrift zugeteilten Kennbuchstabens vierstellig aufgefüllt. Zahlen wurden in der Reihenfolge 1, 2, 3 ... durch die Buchstaben `q`, `w`, `e`,... des Tastenfeldes ohne Hervorhebungszeichen ersetzt. Zur Erleichterung zeigten die entsprechenden Tasten einiger Chiffriermaschinen Funkschlüssel M unter den Buchstaben Ziffern (siehe Abb. 1.4).



Schlüssel M "N i x e" FIGURE 18b

Gültig für alle Monate Prüfnummer: 1

Geheime Kommandosache!

Sonderschlüssel Nr. 1024

Wechsel 1200 Uhr D.G.Z.

Ausgegeben an U.Boot U. ....

I. Äußere Einstellung

Spruchschlüssel:

Anton	=	U Z N W	Jot	=	H U Y L	Sophie	=	L E K G
Bruno	=	P F S C	Karl	=	R K C H	Toni	=	Y O B K
Cäsar	=	I R F M	Lucie	=	T B P R	Ulrich	=	E J Q S
Dora	=	M L W U	Max	=	G S M A	Viktor	=	Q T J F
Emil	=	C X O B	Nanni	=	O N H N	Wilhelm	=	K D T J
Fritz	=	K G E Q	Otto	=	D A U E	Xant	=	X W A O
Gustav	=	B Y U X	Paula	=	W Q D P	Ysop	=	F I Z T
Hans	=	U M X D	Quatsch	=	Z H R Y	Zet	=	S P L I
Ida	=	N U G Z	Richard	=	J C I U			

Monatstag	Steckerverbindungen
1. -10.	10/8 9/11 15/18 17/21 20/16 6/14 3/4 7/19 5/2 1/12
11.-20.	14/18 5/17 4/7 12/13 8/16 2/11 9/10 19/15 20/21 3/6
21.-31.	2/20 13/11 12/10 14/4 9/17 16/8 6/18 5/7 3/19 1/15

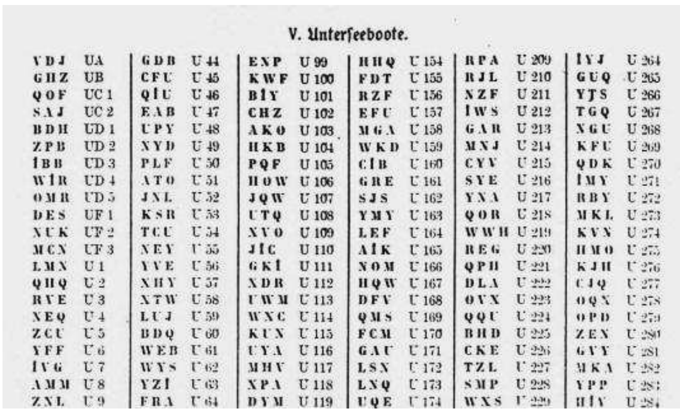
II. Innere Einstellung

Monatstag	Innere Einstellung				
1. -10.	B	Gamma A	IV A	I D	VI G
11.-20.	B	Gamma A	I T	VI U	II P
21.-31.	B	Gamma A	VI S	V F	VII Q

Beachten: Erst auf Befehl 2./Skl BdU op oder OKM 4/Skl II vernichten.

Abbildung 1.19: Sonderschlüssel

Chiffriert wurde mit Schlüssel M Allgemein mit der Tageseinstellung. Aus zwei Tafeln mit Sondergrundstellungen für U-Bootskurzsignale wurde eine von 26 Grundstellungen für gerade bzw. ungerade Monate gewählt. Der Kennbuchstabe der gewählten Grundstellung wurde zweimal offen dem chiffrierten Spruch vorangestellt. Das Kurzsignalheft enthielt etwa 10 Seiten mit den wichtigsten Spruchphrasen für U-Boote als Trigramme. Eingeleitet wurde das Kurzsignal durch zweimaliges Geben von Alpha Alpha.
Bei Standortmeldungen folgte nach der Einleitung Beta Beta der zweimal offen gegebene Kennbuchstabe für die Grundstellung. Zur Verschleierung des Standortes selbst siehe Kap. 1.3.2.10.



V. Unterseeboote.

VDJ	UA	GDB	U 44	EXP	U 99	HHQ	U 154	RPA	U 209	IYJ	U 264
GHZ	UB	CFU	U 45	KWF	U 100	FDT	U 155	RJL	U 210	GUQ	U 265
QOF	UC 1	QIU	U 46	BIY	U 101	RZF	U 156	NZF	U 211	YJS	U 266
SAJ	UC 2	EAB	U 47	CHZ	U 102	EFU	U 157	IWS	U 212	TGQ	U 267
BDH	UD 1	UPY	U 48	AKO	U 103	MGA	U 158	GAR	U 213	NGU	U 268
ZPB	UD 2	NYD	U 49	HKB	U 104	WKD	U 159	MNJ	U 214	KFU	U 269
IBB	UD 3	PLF	U 50	PQF	U 105	CIB	U 160	CYV	U 215	QDK	U 270
WIR	UD 4	ATO	U 51	HOW	U 106	GRE	U 161	SYE	U 216	IMY	U 271
OMR	UD 5	JNL	U 52	JQW	U 107	SJS	U 162	YNA	U 217	RBY	U 272
DES	UF 1	KSR	U 53	UTQ	U 108	YMY	U 163	QOR	U 218	MKL	U 273
NUK	UF 2	TCU	U 54	XVO	U 109	LEF	U 164	WWH	U 219	KVN	U 274
MCN	UF 3	NEY	U 55	JIC	U 110	AIK	U 165	REG	U 220	HMO	U 275
LMN	U 1	YVE	U 56	GKI	U 111	NOM	U 166	QPH	U 221	KJH	U 276
QHQ	U 2	XHY	U 57	XDR	U 112	HQW	U 167	DLA	U 222	CJQ	U 277
RVE	U 3	XTW	U 58	UWM	U 113	DFV	U 168	OVX	U 223	OQX	U 278
NEQ	U 4	LUJ	U 59	WXC	U 114	QMS	U 169	QQU	U 224	OPD	U 279
ZCU	U 5	BDQ	U 60	KUN	U 115	FCM	U 170	BHD	U 225	ZEN	U 280
YFF	U 6	WEB	U 61	UYA	U 116	GAU	U 171	CKE	U 226	GVY	U 281
IVG	U 7	WYS	U 62	MHV	U 117	LSN	U 172	TZL	U 227	MKA	U 282
AMM	U 8	YZI	U 63	XPA	U 118	LNQ	U 173	SMP	U 228	YPP	U 283
ZNL	U 9	FRA	U 64	DYM	U 119	UQE	U 174	WXS	U 229	HIY	U 284

Abbildung 1.20: Funknamenliste

[81] BA/MA, RMD 4/299, nicht zu verwechseln mit der späteren M.Dv.Nr 299 „U-Bootshandbuch der Ostküste Kanadas“ von 1942

— 17 —

Ausgabe X. 43.

Funknamenschlüssel

zur G. F. L. — M. Dv. Nr. 82.

Monate Januar und Juli.					
Uhrzeit					
0000—0159	0200—0359	0400—0559	0600—0759	0800—0959	1000—1159
YSG	AGR	KTX	QLU	OZE	UJC
Uhrzeit					
1200—1359	1400—1559	1600—1759	1800—1959	2000—2159	2200—2359
İPY	MBV	WKA	CRH	SXJ	GNS

Monate Februar und August.					
Uhrzeit					
0000—0159	0200—0359	0400—0559	0600—0759	0800—0959	1000—1159
NTE	BMS	JNC	LAO	DQU	PWL
Uhrzeit					
1200—1359	1400—1559	1600—1759	1800—1959	2000—2159	2200—2359
XKB	RXJ	TZF	VGR	ZİQ	HPV

Monate März und September.					
Uhrzeit					
0000—0159	0200—0359	0400—0559	0600—0759	0800—0959	1000—1159
DQZ	VEM	FYN	LVB	XİT	PWİ
Uhrzeit					
1200—1359	1400—1559	1600—1759	1800—1959	2000—2159	2200—2359
NAF	JDP	BHO	HOW	RFL	ZUD

Abbildung 1.21: Funknamenschlüssel

Im September 1941 trat das Kurzsignalheft M.Dv.Nr. 96 an die Stelle der M.Dv. Nr. 299. Es enthielt eine Liste mit zweistelligen Unterschriftsgruppen, die in das Kurzsignal einzusetzen waren. Nach ERSKINE waren die Bigramme alphabetisch geordnet und den der Grösse nach geordneten U-Boot–Nummern gegenübergestellt. Dieser Fehler, dass eine parallele Ordnung in der Liste bestand,erlaubte den Alliierten Rückschlüsse über Versenkungen, Neubauten usw.

Ab 1.7. 1943 bekamen die U-Boote Funknamen aus drei Buchstaben. Die dreistellige Unterschrift wurde der „Geheimen Funknamenliste der U-Boote“ [82] (Abb. 1.20 und 1.21) entnommen, die dann mit Hilfe des Schlüssels M chiffriert wurde. Im britischen Dechiffrierungszentrum Bletchley Park (BP) soll eine solche Funknamenliste bereits vor Inkrafttreten vorhanden gewesen sein.

Die jeweils zu benutzenden Spruchschlüssel waren einem „Kenngruppenheft zum Kurzsignalheft“ zu entnehmen, in dem jedem Schlüsselkreis Kenngruppen zugewiesen waren, von denen eine auszuwählen war (Abb. 1.22). Jeder Kenngruppe war im Teil A des Kenngruppenheftes auch ein Spruchschlüssel zugeordnet (Abb. 1.23). Im Teil B des Kenngruppenheftes wurde die Kenngruppe in die Kenngruppennummer zurückübersetzt, sodass sowohl der zuständige Schlüsselbereich als auch der Spruchschlüssel festgestellt werden konnten.

Das eigentliche Kurzsignalheft enthielt etwa 100 Seiten mit Spruchphrasen und zugehörigen 4-stelligen Signalgruppen (Buchstaben). Sowohl die Kenngruppen als auch die Signalgruppen waren so aufgebaut, dass sie entstümmelbar waren, d.h. alle Kenngruppen unterschieden sich voneinander um mindestens zwei Buchstaben. Bei sicheren zwei Buchstaben war der dritte aus dem Teil B der Kenngruppentafel zu finden. Bei den Kurzsignalgruppen war der Abstand (im Alphabet) des zweiten Buchstabens von ersten gleich dem Abstand des vierten Buchstabens vom dritten.

Zuteilungsliste zum Kenngruppen

Schlüssel	Monatstag							
	1. u. 2.	3. u. 4.	5. u. 6.	7. u. 8.	9. u. 10.	11. u. 12.	13. u. 14.	15. u. 16
Triton	96—105	46—55	361—370	66—75	51—60	246—255	81—90	31—40
	226—235	336—345	236—245	276—285	126—135	331—340	1—10	271—280
	261—270	311—320	391—400	231—240	241—250	196—205	176—185	221—230
	51—55	246—250	76—80	131—135	106—110	31—35	306—310	111—115
	301—305	296—300	291—295	46—50	326—330	166—170	146—150	331—335
	171—175	126—130	346—350	176—180	211—215	236—240	156—160	201—205
	371—375	376—380	331—335	361—365	386—390	381—385	396—400	391—395
Medusa	131—140	301—310	36—45	51—60	161—170	101—110	91—100	191—200
	391—400	326—335	246—255	321—330	256—265	361—370	186—195	371—380
Niobe	346—355	186—195	106—115	121—130	11—20	66—75	276—285	41—50
	56—65	216—225	351—360	346—355	361—370	256—265	226—235	151—160
Poseidon	216—225	131—140	66—75	181—190	116—125	341—350	71—80	296—305
Thetis	76—95	346—365	371—390	21—40	296—315	146—165	126—145	351—370
	326—345	1—20	166—185	371—390	86—105	271—290	246—265	76—95
	241—250	366—375	26—35	166—175	331—340	76—85	111—120	121—130
	291—300	156—165	321—330	241—250	171—180	121—130	36—45	211—220
	21—30	231—240	256—265	106—115	136—145	176—185	211—220	16—25
	141—150	251—260	126—135	286—295	186—195	206—215	311—320	256—265
	176—180	56—60	336—340	191—195	206—210	326—330	66—70	291—295
	271—275	181—185	186—190	116—120	6—10	96—100	241—245	51—55
	66—70	241—245	61—65	136—140	251—255	376—380	121—125	266—270
	181—185	196—200	266—270	296—300	111—115	191—195	341—345	206—210

Abbildung 1.22: Zuteilungsliste

Ein Kurzsignal bestand aus dem zweimaligen Beta, der offenen Kenngruppe, dem chiffrierten Spruch (einschliesslich Unterschriftsgruppe) und (wiederholt) der offenen Kenngruppe. Bei der

[82] GFL U-Boote M.Dv.Nr. 82/1 - Ausgabe August 1944 - mit zugehörigem Funknamenschlüssel

Chiffrierung blieb die Grundstellung des Tagesschlüssels unberücksichtigt.
Ab 1. 11. 1944 war der Spruchschlüssel durch Verdoppeln des dritten Buchstabens vierstellig zu fassen[83].

Im September 1944 wurde das Kurzsignalheft 1941 abgelöst durch ein neues, das gegliedert war in Teil I (Satzbuch) und Teil II (Buchgruppenheft). Das gesamte Verfahren wurde verfeinert, allerdings ist es mit hoher Wahrscheinlichkeit nicht mehr in Kraft gesetzt worden.

Weitere Einzelheiten zu Kurzsignalen bei ERSKINE.[84] Der Pferdefuss bei den Kurzsignalen war, dass sie von der Zentrale an Land unter Angabe des Inhalts quittiert wurden. Am Anfang des Krieges wurden die Kurzsignale von den U-Booten ohne Rufzeichen und Zeitgruppe abgesetzt. Die Zentrale quittierte jeden Spruch, indem sie ihn dreimal wiederholte und dabei die Zeitgruppe und eine Seriennummer hinzufügte. Später im Kriege enthielt der Spruchkopf der U-Boot-Sprüche eine Zeitgruppe, die Zentrale wiederholte den Spruch mit einer hinzugefügten Seriennummer. Wenn keine Quittung seitens der Zentrale erfolgte, wiederholten die Boote den Spruch innerhalb 30 Minuten. 1944 begannen die Boote ihre Sprüche auf einer jeweils veränderten Frequenz abzusetzen, um Peilungen weiter zu erschweren. Die Quittung wurde von der Zentrale jedoch auf der normalen U-Boot-Frequenz gegeben.

Kenngruppenheft Nr. 6
Teil A

Nr.	Kenngruppe	Spruchschlüssel	Nr.	Kenngruppe	Spruchschlüssel	Nr.	Kenngruppe	Spruchschlüssel	Nr.	Kenngruppe	Spruchschlüssel
1	M F T	*OTL*	51	H C M	*INW*	101	O Y O	*KPA*	151	K M X	*GAV*
2	H Q Z	*OZA*	52	Q E W	*CHZ*	102	N P D	*SYI*	152	B J M	*ZGS*
3	J T D	*WBQ*	53	U M H	*QVB*	103	G E N	*PWE*	153	S Q K	*UZH*
4	R L D	*DFE*	54	J P Z	*FJR*	104	Z O Q	*CJT*	154	O Q F	*MSG*
5	U Q M	*QVU*	55	M S F	*AKG*	105	Q Z R	*IOX*	155	C T X	*RLF*
6	C O S	*UAT*	56	R C V	*OVC*	106	H F P	*UZP*	156	G V D	*WDT*
7	B N Q	*HMD*	57	O W M	*SYO*	107	B A D	*QPM*	157	Q Q H	*AIP*
8	V V S	*MSA*	58	F A H	*YGF*	108	O F V	*YDH*	158	Z U W	*OHV*
9	Q J A	*EJA*	59	D H N	*WDV*	109	V A X	*EJV*	159	F Y F	*MUR*
10	P J Z	*AWM*	60	R T M	*BJG*	110	K J U	*YRT*	160	P E V	*VEQ*
11	X E D	*LQK*	61	N U J	*GOX*	111	E X D	*MSG*	161	W H F	*SYC*
12	S W Q	*CHV*	62	Z S U	*ADJ*	112	W S Q	*ICY*	162	K U F	*DNS*
13	D M R	*OUI*	63	G X F	*CLK*	113	S K D	*TMI*	163	Q U M	*KGZ*
14	K Q B	*YDH*	64	N M A	*GMC*	114	E L R	*BYF*	164	B U X	*OPQ*
15	Q W O	*JNP*	65	X T S	*VZT*	115	H T C	*DQS*	165	N T H	*GLP*
16	O O D	*TYE*	66	P R H	*JDX*	116	C B F	*VEU*	166	R V O	*TAJ*
17	D B G	*IOX*	67	D S X	*OJN*	117	O X N	*HBP*	167	T G B	*SXB*
18	G T B	*FKI*	68	L E R	*IDQ*	118	V R O	*KRX*	168	D X C	*FLS*
19	P C T	*ZEM*	69	Q M D	*KEN*	119	K D F	*AGW*	169	J G R	*BHM*
20	M K X	*WBC*	70	S F Z	*XSC*	120	E R X	*XSA*	170	R N F	*OEQ*

Abbildung 1.23: Kenngruppenheft Teil A

In der „Nachrichtenvorschrift der Kriegsmarine, Heft II, Der Funkdienst" von 1943 (M.Dv.Nr. 922) wurden die Formen der Funksprüche festgelegt.

Ausser dem beschriebenen Kurzsignal wurden auch aufgelistet

das Ortungsfunksignal, eingeleitet durch zweimal Epsilon[85]

das Funksignal für S-Boote, eingeleitet durch zweimal Delta[86]

das Kurzfunkwetter, eingeleitet durch zweimal w[87]

1.3.2.8.1 Kurzfunkwetter. Der Wetterkurzschlüssel diente dazu, Wetterbeobachtungen der U-Boote zu codieren (über Schlüsseltafeln, die die Beobachtungen in Einzelbuchstaben bzw. Buchstabengruppen codierten). Dann folgte die Chiffrierung mit Schlüssel M Allgemein (ohne Grundstellung) nach einem Spruchschlüssel, der am Spruchanfang durch einen offen gesendeten Kennbuchstaben mitgeteilt wurde. Die Länge eines Kurzfunkwetters war im Verlauf des Krieges unterschiedlich, von 12 Buchstaben bis 23 Buchstaben im Jahre 1945.

---

[83] Handschriftliche Ergänzung im Kenngruppenheft Nr.5. zum Kurzignalheft 1941
[84] ERSKINE a), e), g)
[85] M.Dv.Nr. 914, dazu „Ortungsbezugspunkte" , M.Dv.Nr. 914a
[86] Epsilon: —..—, Delta: .— — .
[87] Geheimer Wetter- und Seeschlüssel der Kriegsmarine, Teil 2, Wetterkurzschlüssel, M.Dv. Nr. 443

Ein typisches Beispiel für ein „Kurzwetter“ sah so aus:

```
  w w J
  K Z N
I S F Q
  E F
  L J
```

Mit `J` = Kennbuchstabe für den Spruchschlüssel, `KZN` = Kennung des Seegebietes, `ISFQ, EF` Chiffrierte Wettermeldung, `LJ` = Unterschrift.[88]

Die Dechiffrierung lautet:

> `KZN` = 61 Grad nördliche Breite, 17 Grad West
> `ISFQ` = Luftdruck 1034 oder 982 mb, Temperatur +7øC oder -19øC, Bedeckung 6/10 oder 9/10, Sicht 10 sm
> `EF` = Wind SW 1 bis 2, Dünung leicht SW.
> Unterschrift `LJ` = U 530, Kommandant Kptlt. Kurt Lange

Die zu den einzelnen Beobachtungen gehörigen Schlüsselbuchstaben wurden den Schlüsseltafeln des Wetterkurzschlüssels M.Dv.Nr. 443 entnommen. (Wetterkurzsignalheft 1940, Wetterkurzsignalheft 1942 ?)[89]

In der ersten Ausgabe des Schlüsselbuches wurde unter mehreren Arten von Wettermeldungen unterschieden. In der Praxis gab es aber fast nur die „Kurzfunkobs“, (Allgemeine Wetterdaten). 1940 hatte eine solche Wettermeldung die Form

```
S b l P
T D W V
  U U
```

`S` ist dabei der Indikator für den Spruchschlüssel, `b` die geogr. Breite, `l` die geogr. Länge, `P` der Luftdruck, `T` die Lufttemperatur, Windrichtung und -Stärke, `v` die Sicht, `UU` schliesslich die Unterschrift.[90]

In der 2. Ausgabe des Wetterkurzschlüssel, aktiv ab Januar 1942 kamen noch zwei zusätzliche Daten hinzu, sodass die Spruchlänge nunmehr 12 Zeichen war. Die dazugehörige „Spruchschlüsseltafel für Wetterkurzfunksprüche“ (Kennwort Weimar) enthielt etwa 2600 Spruchschlüssel für verschiedene Perioden von je 6 Stunden. Es wurde gefolgt von dem Kennwort Eisenach, später Naumburg.

In der dritten Ausgabe, die ab März 1943 im Verkehr war, erhielten die Sprüche die Form

```
S R B B
P Z V D
K L T M
U U [U]
```

Hierbei war `S` wieder der Indikator für den Spruchschlüssel, `R, B, B` bestimmten den Standort, `P` den Luftdruck, `Z` die Wetteränderung in den letzten 12 Stunden, `V` die Sicht, `D` den Wind, `K` die Änderung der Windstärke und die Höhe der Dünung, `L` die Länge und Richtung der Dünung, `T` die Temperatur, `M` den Temperaturunterschied zwischen Luft und Wasser und schliesslich `UU` die Unterschriftgruppe, die später dreistellig war.

[88]ERSKINE e), S. 336, Der Spruch stammt vom 3.3. 1943 und wurde 04.13 Uhr aufgefangen. Er war chiffriert gemäss der zweiten Auflage des Wetterkurzschlüssels , M.Dv.Nr.443

[89]Geheimer Wetter- und Seeschlüssel der Kriegsmarine, Teil 2, Wetterkurzschlüssel, 2. Auflage Berlin 1941, 3. Auflage Berlin 1942 (mit eingearbeiteten Deckblättern)

[90]ERSKINE h), S. 75

1.3.2.9 Wetterschlüssel.

Die Marinefunkstation Norddeich (Rufzeichen DAN) funkte jeweils eine Folge von Wettermeldungen aller verfügbaren Quellen, auch der Wettermeldungen aus Spanien, Portugal usw. Die Klarsprüche bestanden aus je fünf 5-ziffrigen Gruppen des Internationalen Meteorologischen Codes.
Die Struktur einer solchen Klarmeldung war:

$$IIIC_lC_m wwVhN_h DDFWNPPPTTUC_h app$$

Dabei waren die ersten drei Zeichen der ersten Gruppe das Kennzeichen der sendenden Station. Die vierte Ziffer zeigte die Form der niedrigen Wolken an, die fünfte die der mittleren Wolken. Die zweite Gruppe gab zunächst in den ersten beiden Ziffern das gegenwärtige Wetter, die dritte die Horizontalsicht, die vierte die Höhe der niedrigen Wolken, die fünfte schliesslich den Bedeckungsgrad. In der dritten Gruppe gaben die ersten beiden Ziffern die Richtung des Bodenwindes an, die dritte die Stärke. Die vierte Ziffer zeigte das Wetter während der vergangenen sechs Stunden an, die fünfte den Bedeckungsgrad in Zehnteln. Die vierte Gruppe gab in den ersten drei Ziffern den Luftdruck in Seehöhe an, die letzten beiden die Temperatur. Die letzte Gruppe schliesslich wurde benutzt, um Höhenwindangaben (durch Ballonaufstiege ermittelt) zu geben.
Sie wurden mit dem Wetterschlüssel der Kriegsmarine chiffriert. Es gab zwei wesentlich verschiedene Schlüssel:
Bis etwa 1942 wurde die gesamte Klarmeldung ohne Rücksicht auf Gruppenstruktur in Dreiergruppen aufgespalten, die dann mit Trigrammtafeln, Bigrammtafeln und Monogrammtafeln chiffriert wurden. Die so entstehenden Geheimgruppen wurden wieder in Fünfergruppen zusammengefasst und gesendet. Ein Satz von 20 Tafeln (10 zum Chiffrieren, 10 zum Dechiffrieren) galt 8 bis 17 Tage. Teilweise wurde diese Tafeln in späteren Zeitabschnitten wiederholt genutzt. Jeder Tag war in 6 Schlüsselperioden aufgeteilt.
Die spätere Chiffrierart (mit Sicherheit ab 1943) sollte durch Veränderung der Klargruppen in einem ersten Substutionsschritt das Erkennen der zugrunde liegenden Gruppenstruktur unmöglich machen.

> Die mittlere Ziffer jeder Gruppe wurde durch zwei Ziffern ersetzt, die als Summe mod 10 die zu ersetztende Ziffer hatten.
> Beispiel: Die Gruppe 90304 konnte (nach Belieben des Chiffrierers) ersetzt werden durch 906704, 905804, 904904, 903004, 902104, 901204, 900304, 909404, 908504, 907604.

Im zweiten Substitutionsschritt wurden die in Dreiergruppen aufgespaltenen Sechsergruppen des ersten Schrittes mit Trigrammtafeln von je 1000 Trigrammen chiffriert. Je 24 Stunden waren in 8 Zeitabschnitte unterschiedlicher Länge aufgeteilt. Die Geltungsdauer für je 12 Tafeln, die in beiden Richtungen verwendbar waren, betrug normalerweise fünf Tage. Keine Tafel wurde in aufeinander folgenden Zeitabschnitten benutzt, wohl aber war es möglich, eine Tafel mehrfach zu gebrauchen. Nach Ablauf der 40 Zeitabschnitte wurden die benutzten Tafeln aus dem Verkehr genommen.[91]

1.3.2.9.1 Zenit. Für die ausführlichen Wetternachrichten von Flugzeugen aus war der Wetterschlüssel „Zenit“ im Einsatz[92], wenngleich Wettermeldungen auch nach der Aufklärungs-und Kampffliegertafel (Au.Ka.-Tafel)abgegeben wurden. Nach chiffrierter Standortangabe (Luftwaffen - Gradnetz - Meldeverfahren) durch Umsetzen in mehrere Gruppen aus je drei Ziffern folgten die eigentlichen Wetterangaben als Ziffern, die aus der „Zenittafel“ entnommen und bis Herbst 1941 offen gesendet wurden. Danach setzte man die einzelnen Ziffern mit einem Chiffrierblatt (Tagesschlüssel) Ziffer um Ziffer um. Ab Sommer 1944 wurden alle Ziffernangaben, auch die der Standortgruppen, mit einem Zenit- (Tages-) Schlüssel in Buchstaben chiffriert.

[91] NARA Dokument Box ZEMA07, Nr. 3776, «Outline of Procedures for the Solution of Main German Six–figure Meteorological Reports»
[92] SCHWERDTFEGER, S. 200

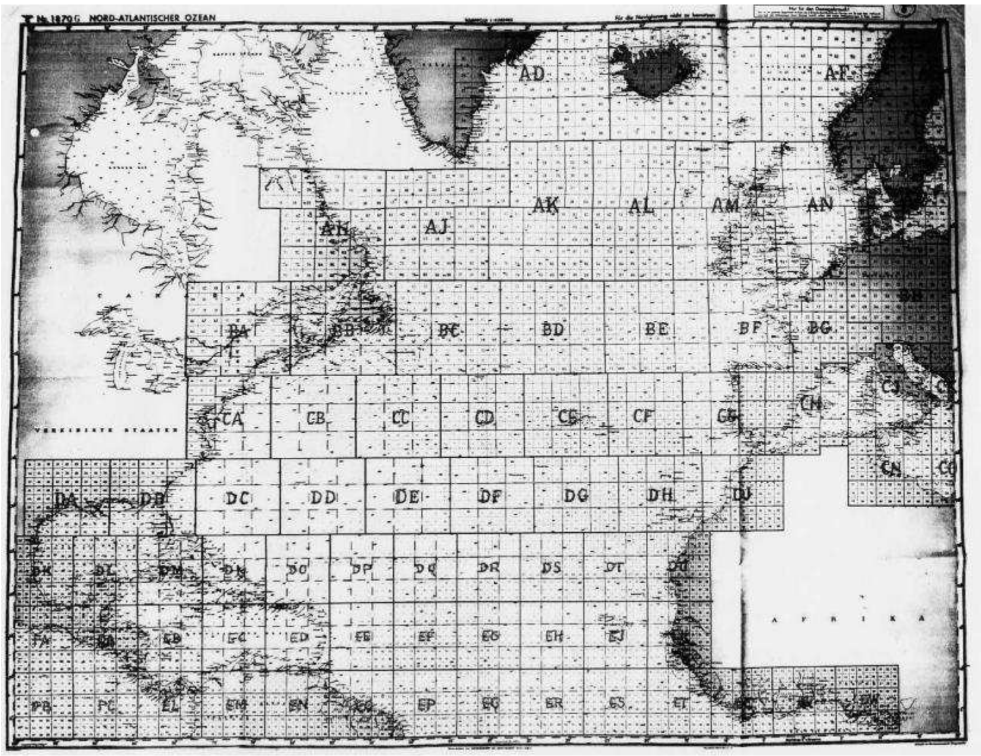


Abbildung 1.24: Grossquadrate

1.3.2.10 Standortverchiffrierung.

Für die gegenseitige Verständigung zwischen U-Booten und der Zentrale war eine Chiffrierung von Standortangaben vonnöten. Die Gesamtheit der in Frage kommenden Meeresgebiete war dazu in Grossquadrate in der Mercator- Projektion eingeteilt (in der Realität eigentlich Rechtecke). Jedes Grossquadrat wurde mit zwei Grossbuchstaben bezeichnet und hatte im Normalfall eine Seitenlänge von 486 sm. (Bild 1.24)
Jedes Grossquadrat war eingeteilt in $9 \cdot 9$ kleinere Quadrate mit je 54 sm Seitenlänge, diese wiederum in je 9 Quadrate mit 18 sm Seitenlänge und schliesslich diese in je 9 Quadrate mit 6 sm Seitenlänge. Die Kennzeichnung dieser Kleinquadrate erfolgte mit 4 Ziffern (je eine für den Unterteilungsschritt). (Abb. 1.25) Diese Darstellung einer Position hatte den grossen Vorteil gegenüber der Angabe in geografischen Koordinaten, dass im Funkverkehr viele Buchstaben gespart weden konnten (Alle Ziffern mussten ja in Buchstaben ausgedrückt werden).[93]
Der Standort selbst wurde nur durch den zweiten Buchstaben des Grossquadratbigramms und die zwei ersten Ziffern (54 sm - Quadrat) angegeben. Wie bei den Alpha-Meldungen wurde die Gruppe durch den Unterschriftsbuchstaben ergänzt und danach zweimal nacheinander chiffriert[94]. Nach ERSKINE[95] wurde aus Furcht vor landgestützter Peilung ab 12.2.1941 die ergänzte Gruppe nur einmal chiffriert gesendet.
Am 16.6.1941 wurde eine Verschleierung der Positionen für U-Boote im Schlüsselberich „Heimisch" befohlen, möglicherweise als Reaktion auf den Verlust der Schiffe „Krebs" (März 1941) und „München" (Mai 1941), wobei Karten mit den Marinequadraten in britische Hände hätten fallen können (was in der Tat der Fall war, dazu noch durch U 110).
Es wurden Referenzpunkte festgelegt(z.B. „Hecht", „Hammer"), auf die sich die Positionen nach Richtung und Entfernung bezogen.

[93] Die Umrechnung in geografische Koordinaten ist bei RECHE zu finden
[94] Alpha: ..—.. ; Beta: —...—
[95] ERSKINE h)

Offenbar hat sich dieses Verfahren nicht bewährt. Es wurde am 11. September 1941 aufgegeben. (Kurzzeitig ist es jedoch für die Rudeltatktik von September 1943 bis Dezember 1943 wieder benutzt worden.) Ab 10. 9. 1941 wurde eine Chiffrierung für die Grossquadrat-Bigramme in Kraft gesetzt, die die auf den Booten vorhandenen Bigramm-Tauschtafeln zu benutzen gestattete. Dazu mussten über die (Doppel-)Spalten der Tauschtafeln 26 Grossquadrat-Bigramme geschrieben werden. Die Chiffrierung bestand darin, dass ein beliebiges Bigramm der rechten Spalte unter dem Klarbigramm als Geheimbigramm benutzt wurde. Daher gab es zu jedem Klarbigramm 26 mögliche Geheimbigramme.

Damit nicht genug, ab 24.11. 1941 wurde das Adressbuchverfahren eingeführt. Es hat mehrere Ausgaben des Adressbuches gegeben. Der erste Name war „Jacob Boettcher“ - ohne weitere Zusätze - vom 24.11. 1941 bis Dezember 1941, dabei wurden nur die Bigramme verändert, die Ziffern der kleineren Quadrate blieben hier unverändert.

Ab 28.12. 1941 bedeutete dann „Gottfried Becker, Blücherplatz 30“, dass von der 4-ziffrigen Angabe des Kleinquadrates 3000 abzuziehen war.

Nach der Einführung des Schlüssels M4 war das Adressbuch nur für U-Boote des Schlüsselbereichs „Hydra“ anzuwenden.

Der Operationsbefehl vom 5.4. 1943 beschreibt das zu diesem Zeitpunkt befohlene Vorgehen: Je zwei Grossquadrat-Bigramme (für geografisch weit auseinender liegende Gebiete) wurden einem Geheimbigamm zugeordnet. Diese Paare wurden in Gruppen zusammengefasst („Grün“, „Blau“). Die Grossquadrat-Paare „Grün“wurden über den Spalten der Tafel eingetragen, die von „Blau“ darunter. Jedes Boot besass nur für diesen Zweck 10 Bigrammtafeln. Welche jeweils zu benutzen war, wurde durch einen Vornamen festgelegt:

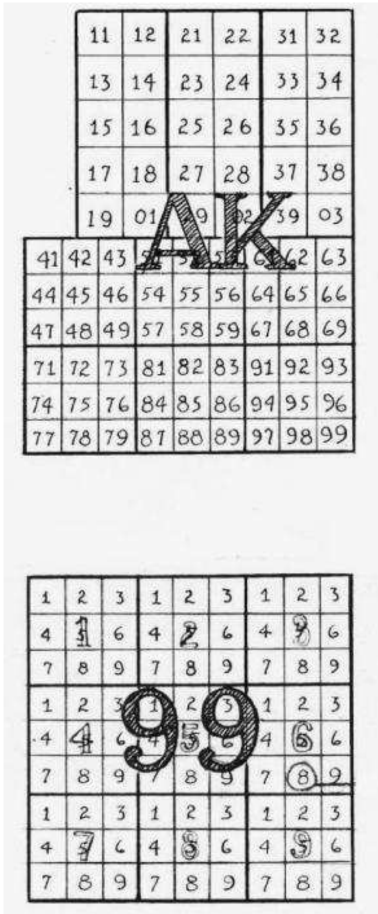


Abbildung 1.25: Kleinquadrate

Tafel 1 = J o h a n n a	Tafel 2 = H i l d e
Tafel 3 = A n n e l i e s e	Tafel 4 = M a r i a n n e
Tafel 5 = I n g e b o r g	Tafel 6 = R e n a t e
Tafel 7 = B a r b a r a	Tafel 8 = I r m g a r d
Tafel 9 = U r s u l a	Tafel 10 = G r e t c h e n

Strasse und Hausnummer bestimmten die Chiffrierung der 54-sm-Quadrate. Die 18-sm-und die 6-sm-Quadrate wurden nicht chiffriert.

Paradeplatz: (Hausnummer nur Schein): Die Zahlen 01 bis 50 wurden ersetzt durch 51 bis 00, die Zahlen 51 bis 00 durch 01 bis 50.
Gneisenaustrasse: (Hausnummer nur Schein): Zahlen wurden nicht chiffriert.
Gartenstrasse: (Hausnummer nur Schein): Beim Chiffrieren wurde 30 addiert, beim Dechiffrieren abgezogen.
Marktstrasse: Beim Chiffrieren wurde die Hausnummer addiert, beim Dechiffrieren abgezogen.
Schillerstrasse: (Hausnummer nur Schein): Der Monatstag der Inkraftsetzung des Schlüsselworte wurde beim Chiffrieren addiert, beim Dechiffrieren abgezogen.
Lessingstrasse: (Hausnummer nur Schein): Die Stunde der Inkraftsetzung des Schlüsselwortes wurde beim Chiffrieren addiert, beim Dechiffrieren abgezogen.[96]

[96] NARA Dokument Box CBKJ21, Nr. 1674 «General Nature of Address Book», dort auch Listen der Zuordnung für Ehrlich, Neumann, Schmitz und Huber zur den Bigrammtafeln

Die alliierten Bemühungen zur Analyse und schliesslich Rekonstruktion der Adressbücher sind in einem (handschriftlichen) Dokument bekannt geworden.[97] Weitere Ausführungen zur Positionsverschleierung bei HINSLEY[98]. Von U505 wurde am 4.6.44 ein Adressbuch erbeutet, eins der wichtigsten eroberten deutschen Dokumente.

1.4 Handschlüssel.

Ausser der Chiffriermaschine ENIGMA müssen deutsche Handschlüssel betrachtet werden. Die Kenntnis der Inhalte von Sprüchen, die mit diesen Schlüsseln verschleiert wurden und den mittleren und unteren militärischen Ebenen zuzuordnen gewesen sein dürften, gestatteten den Alliierten wertvolle Erkenntninsse der militärischen Situation. Oft waren damit auch Hinweise auf mögliche Inhalte von ENIGMA-Sprüchen verbunden.

1.4.1 Heer.

Die Heeresdienstvorschrift H.Dv.g.7 „Allgemeine Schlüsselregeln für die Wehrmacht“, berichtigt durch Deckblätter, kannte neben dem Maschinenverfahren und dem Chiffrierfernschreibverfahren die Handverfahren.

1.4.1.1 Doppelkastenschlüssel.

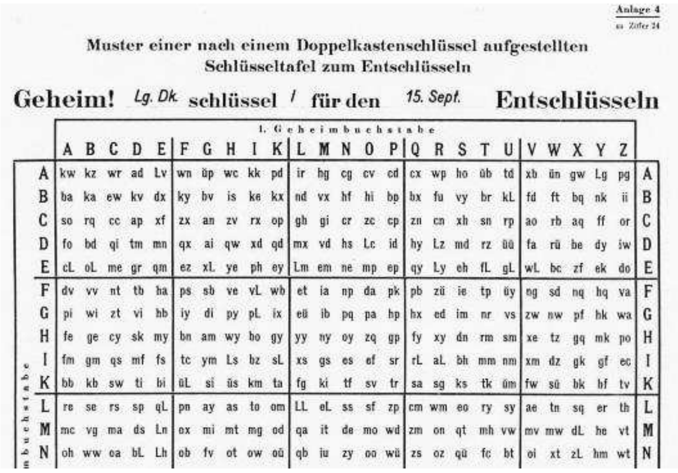
(Bis 1942)[99] Es handelt sich dabei eigentlich um ein Doppelkassettenverfahren. Die Schlüssel wechselten täglich 0 Uhr. Sie bestanden aus zwei Kästen A und B (je 25 Felder), in die das Alphabet (ohne j) permutiert eingetragen war, und den Kenngruppen. Die Zeilenlänge war auf 17 Buchstaben festgelegt, die Höchstlänge eines Spruches war 500 Buchstaben. Zu jedem Tagesschlüssel, der aus zwei vorgegebenen Kästen A und B bestand, gehörten vier Kenngruppen von je drei Buchstaben. Der Spruchkopf enthielt nach der Uhrzeit und der Buchstabenzahl eine der Kenngruppen, offen getastet. Bei mehrteiligen Sprüchen musste jeder Teil die gleiche Kenngruppe enthalten, ansonsten war zu wechseln.
Der Klartext wurde so zeilenweise geschrieben, dass je 34 Buchstaben eine Doppelzeile bildeten. Diese Doppelzeilen waren zwecks besserer Übersicht durch eine Leerzeile getrennt. Ein Rest von weniger als 34 Buchstaben wurde mit der Zeilenlänge (Rest: 2 , aufgerundet) in die letzte Doppelzeile geschrieben, wobei zum Füllen evtl. noch ein Buchstabe (ungleich x) nötig war.

Die untereinander stehenden Buchstabenpaare bildeten für die Chiffrierung eine Einheit. Dabei wurde der obere Klarbuchstabe im Kasten A aufgesucht, der untere im Kasten B. Standen beide Buchstaben in derselben Zeile, wurde der 1. Klarbuchstabe durch den rechts vom 2. Klarbuchstaben im Kasten B stehenden Buchstaben ersetzt, der 2. Klarbuchstabe durch den rechts vom 1. Klarbuchstaben im Kasten A.
Standen die beiden Klarbuchstaben in verschiedenen Zeilen, wurden die Klarbuchstaben durch die dritte und vierte Ecke des durch die Klarbuchstaben definierten Rechtecks ersetzt, die Ecke im Kasten B zuerst.
Das so entstandene Buchstabenpaar wurde als Zwischentext angesehen und sofort erneut wie angegeben chiffriert.

---

[97] NARA - Dokument Box CBKJ21, Nr. 1674,«General Nature of Address Book»
[98] HINSLEY II/1, Appendix 9, S. 681 - 682
[99] M.Dv.Nr. 158, Vorläufige Schlüsselanleitung zum Doppelkastenschlüssel, Ausgabe Dezember 1941

Das Ergebnis dieser zweiten chiffrierung war das Geheimtextpaar. Diese Geheimtextpaare bildeten, nacheinander geschrieben, den ganzen Geheimtext. Beim Dechiffrieren wird in zwei Schritten das Verfahren umgekehrt. Zur Erleichterung des Chiffrierens / Dechiffrierens konnten Schlüsseltafeln wie in Abb. 1.26 erstellt werden. Mit dem Eingang `RV` (Geheimtext) liefert die Tafel unmittelbar den Klartext `fn`. Es ist aber bekannt, dass in einigen Heeresverbänden bei der Anwendung dieses Verfahrens bei Sprüchen innerhalb des Verbandes der zweite Chiffrierschritt weggelassen wurde. Mit dieser „Vereinfachung“ leistete man unabsichtlich den unbefugten Dechiffrierern Vorschub. Dieser Schlüssel wurde auch von der SS und der Polizei benutzt, dort offenbar nur einstufig. Am 1. November 1942 wurde das Doppelkastenschlüssel-Verfahren verändert.[100] Die Schlüssel wechselten nun täglich mehrmals. Für jeden Tag wurden 6 Kästen A bis F vorgeschrieben, dazu, welche Kombinationen von zwei Kästen für welche Zeitspanne des Tages gültig sein sollte. (Abb. 1.27)



Anlage 4
zu Ziffer 24

Muster einer nach einem Doppelkastenschlüssel aufgestellten Schlüsseltafel zum Entschlüsseln

Geheim! Lg. Dk. schlüssel / für den 15. Sept. Entschlüsseln

1. Geheimbuchstabe

	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
A	kw	kz	wr	ad	Lv	wn	üp	wc	kk	pd	ir	hg	cg	cv	cd	cx	wp	ho	üb	td	xb	ün	gw	Lg	pg	A
B	ba	ka	ew	kv	dx	ky	bv	is	ke	kx	nd	vx	hf	hi	bp	bx	fu	vy	br	kL	fd	ft	bq	nk	ii	B
C	so	rq	cc	ap	xf	zx	an	zv	rx	op	gh	gi	cr	zc	cp	zn	cn	xh	sn	rp	ao	rb	aq	ff	or	C
D	fo	bd	qi	tm	mn	qx	ai	qw	xd	qd	mx	vd	hs	Lc	id	hy	Lz	md	rz	üü	fa	rü	be	dy	iw	D
E	cL	oL	me	gr	qm	ez	xL	ye	ph	ey	Lm	em	ne	mp	ep	qy	Ly	eh	fL	gL	wL	bc	zf	ek	do	E
F	dv	vv	nt	tb	ha	ps	sb	ve	vL	wb	et	ia	np	da	pk	pb	zü	ie	tp	üy	ng	sd	nq	hq	va	F
G	pi	wi	zt	vi	hb	iy	di	py	pL	ix	eü	ib	pq	pa	hp	hx	ed	im	nr	vs	zw	nw	pf	hk	wa	G
H	fe	ge	cy	sk	my	bn	am	wy	ho	gy	yy	ny	oy	zq	gp	fy	xy	dn	rm	sm	xe	tz	gq	mk	po	H
I	fm	gm	qs	mf	fs	tc	ym	Ls	bz	sL	xs	gs	es	ef	sr	rL	aL	bh	mm	nm	xm	dz	gk	gf	ec	I
K	bb	kb	sw	ti	bi	üL	si	üs	km	ta	fg	ki	tf	sv	tr	sa	sg	ks	tk	üm	fw	sü	bk	hf	tv	K
L	re	se	rs	sp	qL	pn	ay	as	to	om	LL	eL	ss	sf	zp	cm	wm	eo	ry	sy	ae	tn	sq	er	th	L
M	mc	vg	ma	ds	Ln	ox	mi	mt	mg	od	qa	it	de	mo	wd	zm	on	qt	mh	vw	mv	mw	dL	he	vt	M
N	oh	ww	oa	bL	Lh	ob	fv	ot	ow	oü	qb	iu	zy	oo	wü	zs	oz	qü	fc	bt	oi	xt	zL	hm	wt	N

Abbildung 1.26: Schlüsseltafel

Kasten A

H	*I*	*L*	*Q*	*E*
T	*U*	*A*	*R*	*S*
B	*K*	*X*	*F*	*G*
P	*W*	*C*	*O*	*Z*
D	*V*	*Y*	*M*	*N*

Kasten B

Z	*N*	*O*	*C*	*H*
B	*X*	*A*	*V*	*I*
U	*D*	*T*	*G*	*W*
M	*Y*	*E*	*L*	*S*
K	*P*	*Q*	*R*	*F*

K l a r t e x t

```
f e i n d p a n z e r g r e i f e
n i n g r o s z e r z a h l a n e
    r b i t t e n l u f t u n
    t e r s t u e t z u n g p
```

Im Beispiel wird im ersten Schritt das Buchstabenpaar `fn` zu `DQ`. Im zweiten Schritt wird `DQ` zum endgültigen Geheimtextpaar `RV`. Somit ergibt sich der Geheimtext

```
RVHPS ZVFGR ZHHLT WNYYL TDIPO VMLMF RVMQI YXDLA NVXRL GNEYR WTRBN LPYNF
```

[100] M.Dv.Nr.158, Schlüsselanleitung zum Nachrichtenschlüssel 42, Ausgabe November 1942

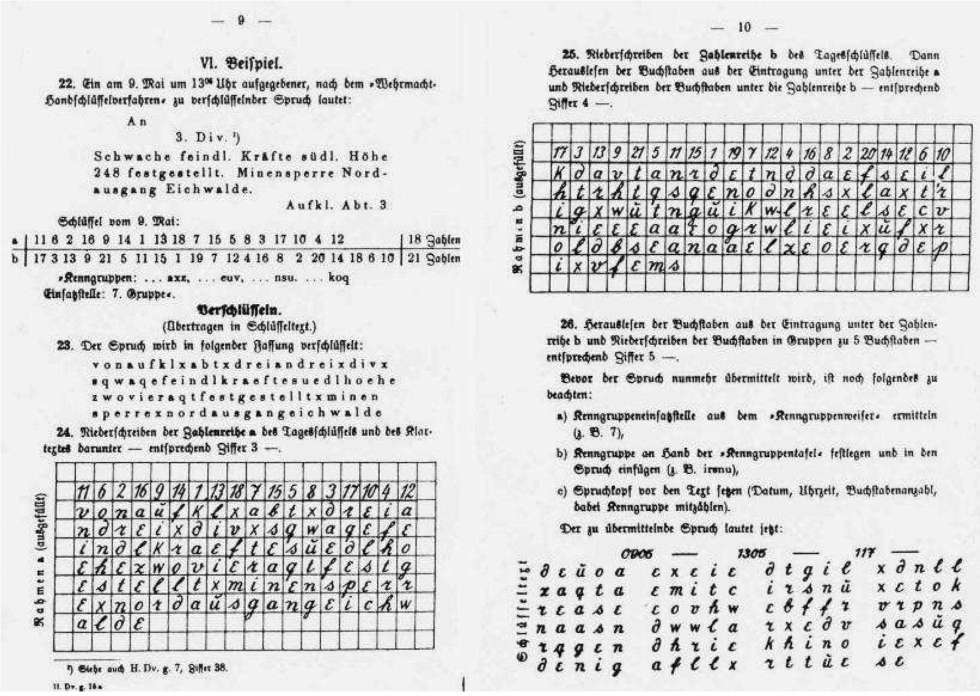


Abbildung 1.27: Handschlüssel

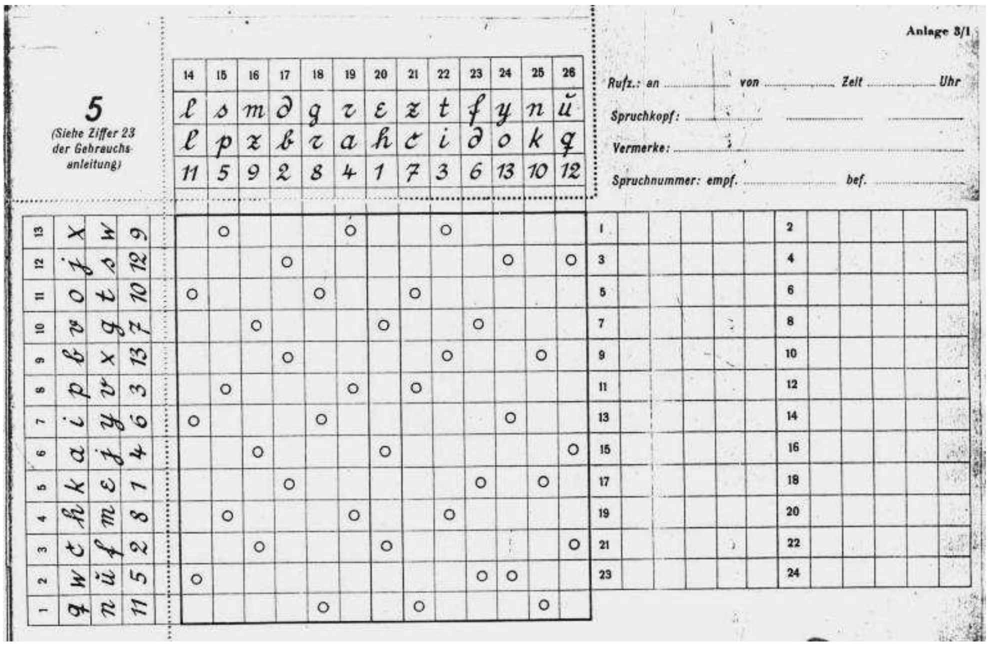


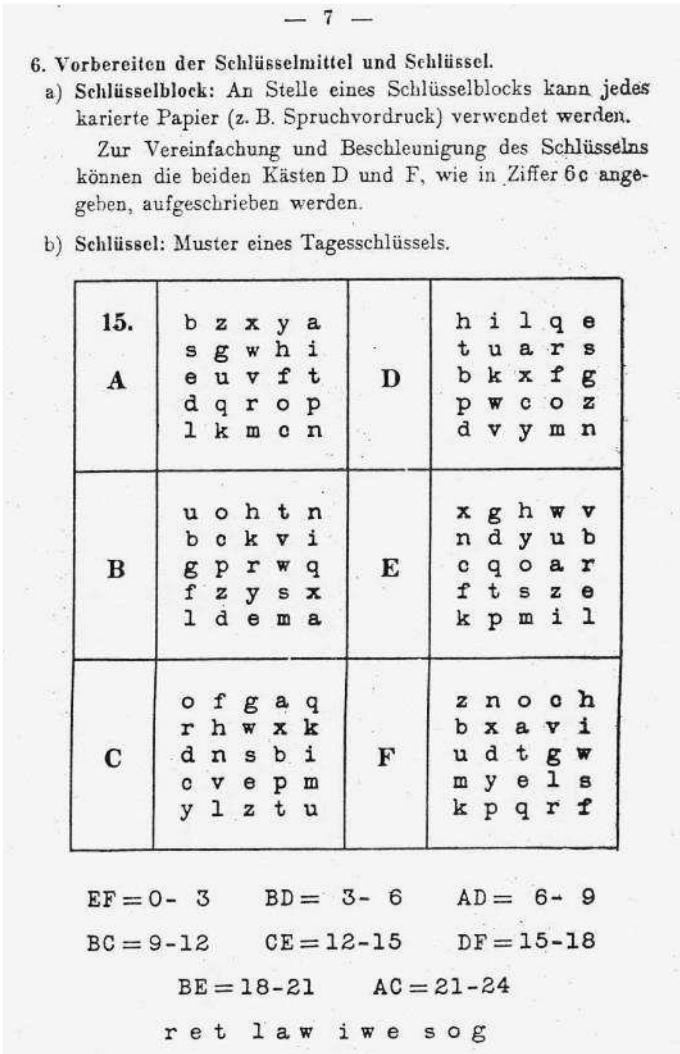
Abbildung 1.28: Heftschlüssel

1.4.1.2 Wehrmacht-Handschlüssel.

Hierbei handelte es sich um eine doppelte Spaltentransposition (auch Doppelwürfel genannt) mit täglich wechselndem Schlüssel.[101] Der Schlüssel bestand aus zwei Zahlenreihen a und b, die wenigstens aus den Zahlen 1 bis 17, höchstens aus 1 bis 29 bestanden.

Der jeweilige Schlüssel wurde durch die letzten drei Buchstaben einer fünfstelligen Kenngruppe über eine Kenngruppentafel festgelegt. Die Kenngruppe musste offen an einer täglich wechselnden Einsatzstelle in den chiffrierten Spruch eingefügt werden.

Die Zahlenreihe a wurde in kariertes Papier eingetragen, darunter der Klartext von links nach rechts zeilenweise. Entsprechend der natürlichen Reihenfolge der im Kopf der Matrix permutiert stehenden Zahlen wurden die Spalten von oben nach unten ausgelesen und von links nach rechts zeilenweise in eine entsprechende Matrix mit der Zahlenreihe b als Kopf eingetragen. Die spaltenweise entsprechend den Zahlen im Matrixkopf ausgelesenen Buchstaben ergaben nacheinander geschrieben den Geheimtext. (Abb. 1.26) Hierzu liefert KOZACZUK eine Lösungsmethode, wie sie in Polen von 1929 bis 1932 angewandt worden war.[102] Diese wird in Kap. 6.2.2.1 gezeigt.



— 7 —

6. Vorbereiten der Schlüsselmittel und Schlüssel.

a) **Schlüsselblock:** An Stelle eines Schlüsselblocks kann jedes karierte Papier (z. B. Spruchvordruck) verwendet werden.

Zur Vereinfachung und Beschleunigung des Schlüsselns können die beiden Kästen D und F, wie in Ziffer 6c angegeben, aufgeschrieben werden.

b) **Schlüssel:** Muster eines Tagesschlüssels.

15. **A**	b z x y a s g w h i e u v f t d q r o p l k m o n	**D**	h i l q e t u a r s b k x f g p w c o z d v y m n
B	u o h t n b c k v i g p r w q f z y s x l d e m a	**E**	x g h w v n d y u b c q o a r f t s z e k p m i l
C	o f g a q r h w x k d n s b i c v e p m y l z t u	**F**	z n o c h b x a v i u d t g w m y e l s k p q r f

EF = 0- 3 BD = 3- 6 AD = 6- 9

BC = 9-12 CE = 12-15 DF = 15-18

BE = 18-21 AC = 21-24

r e t l a w i w e s o g

Abbildung 1.29: Doppelkastenschlüssel

1.4.1.3 Heftschlüssel.

Das Verfahren beruhte auf einem Raster von 13 mal 13 Feldern karierten Papiers mit je 3 Löchern in jeder Spalte, die so angeordnet waren, dass auch in jeder Zeile genau drei Löcher waren.[103] Die Zeilen und Spalten waren durch Bigramme definiert (Abb. 1.29). Die Höchstlänge eines Spruches betrug 115 Buchstaben, die Mindestlänge 45. Aus einer Kenngruppe, die an vorgeschriebener Stelle in den Spruch einzusetzen war, folgte, welches Raster zu benutzen war, an welcher Stelle im Raster die horizontale Eintragung des Klartextes begann und in welcher Reihenfolge der Spalten die Buchstaben senkrecht auszulesen waren. Das Formular konnte auch um 90ø gedreht verwendet werden.

Als Beispiel: Mit der Kenngruppe `GRKPV`[104] wird `strkleinmachnow-zehlendorffeindbesetzt` als Klartext,

---

[101] H.Dv.g. 15a, Nachdruck mit eingearbeitetem Deckblatt Nr. 1, 1940

[102] KOZACZUK b), Anhang B, S. 291 - 298

[103] H.Dv.g. 16, Schlüsselanleitung für das Heftschlüsselverfahren vom 1.11.1937, Nachdruck 1938. Die Deckblätter 1–4 sind eingearbeitet.

[104] MEULEN, van der, a)

beginnend mit dem Feld Spalte 18 (gr), Zeile 8 (pv) zeilenweise eingetragen. Damit ergibt sich beim spaltenweisen Auslesen entsprechend den Spaltenzahlen der Geheimtext

THITA QTROL DCEEN IRKWE GRKPV NHNSZ FZFME ESDRO SITEL NB

die 5. Gruppe ist die Kenngruppe.

1.4.1.4 Rasterschlüssel 44.

Der Rasterschlüssel 44 (RS 44)[105] ist erstmals von SKILLEN beschrieben worden[106]. Es handelte sich um ein Versatzverfahren, bei dem Klartext in eine täglich wechselnde Rasterschablone (ähnlich einem Kreuzworträtsel) an einer bestimmten, von Spruch zu Spruch wechselnden Stelle zeilenweise eingetragen und spaltenweise ausgelesen wurde.

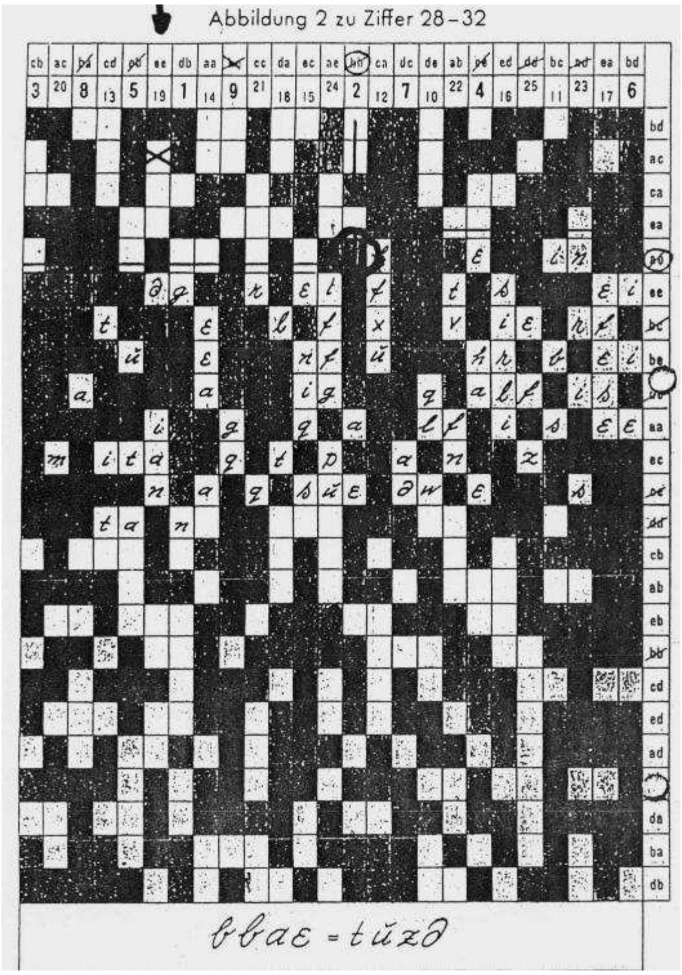


Abbildung 1.30: Rasterschlüssel

Die Rasterschablone enthielt 24 Zeilen mit 25 Spalten. (Abb. 1.30) In jeder Zeile der Schablone waren 10 beschreibbare Felder. Die Lage der Felder wurde durch eine Spaltenlosung (oben) und eine Zeilenlosung (rechts) definiert.
Zu den Chiffriervorgaben gehörte eine täglich wechselnde Buchstabentauschtafel und zwei Ortsnamenalphabete, die jeweils am Monatsersten wechselten. Ortsnamen mussten dabei mit dem Ortsnamenalphabet chiffriert eingetragen werden. Die Spruchlänge war auf zwischen 60 und 200 Buchstaben begrenzt. Der Schlüsselblock enthielt durchsichtige Blätter zum Eintragen der Buchstaben. Nach beliebiger Wahl des Anfangsfeldes (das konnte ein schwarzes Feld sein) wurde der Text eingetragen. Das gewählte Anfangsfeld bestimmte zwei Buchstabenpaare (für die Spalte und für die Zeile), diese wurden als benutzt markiert und über die Buchstabentauschtafel chiffriert. Die Spalte für den Beginn des Herauslesens erhielt der Chiffrierer, indem er die Summe der Ziffern der Minutenzahl der Zeitangabe und der Buchstabenzahl addierte und diese Summe von der für diesen Spruch als Anfangsspalte markierten Spalte nach rechts zählte. Ab Oktober 1944 entfiel diese Rechnung: Der Chiffrierer wählte die Spalte zum Beginn des Herauslesens selbst frei. Herausgelesen wurde der Geheimtext immer von der obersten Zeile beginnend in der Reihenfolge der in der Schablone vorgegebenen Spaltennumerierung.

[105] Schlüsselanleitung Rasterschlüssel 44 (RS 44), Ausgabe 27. März 1944

[106] SKILLEN c), S. 127-132; Inzwischen ist der Rasterschlüssel in einer sehr ausführlichen Arbeit von COWAN behandelt worden, einschliesslich der Ersatzverfahren und Notschlüsel. Er zeigt auch die Methoden die Alliierten zum Brechen des Rasterschlüssels

Abbildung 1.30 zeigt den Chiffriervorgang für einen Spruch mit der Uhrzeit 1203 und 77 Buchstaben Spruchlänge. Das Anfangsfeld ist bbae. Der Geheimtext ist dabei ab Spalte 19 (17 Spalten rechts von der Anfangsspalte) den folgend auszulesen. Abbildung 1.31 gibt ein Blatt eines Tagesschlüssels wieder.
Zu Lösungsansätzen siehe COWAN und ein NARA-Dokument[107].

Der Geheimtext lautet:

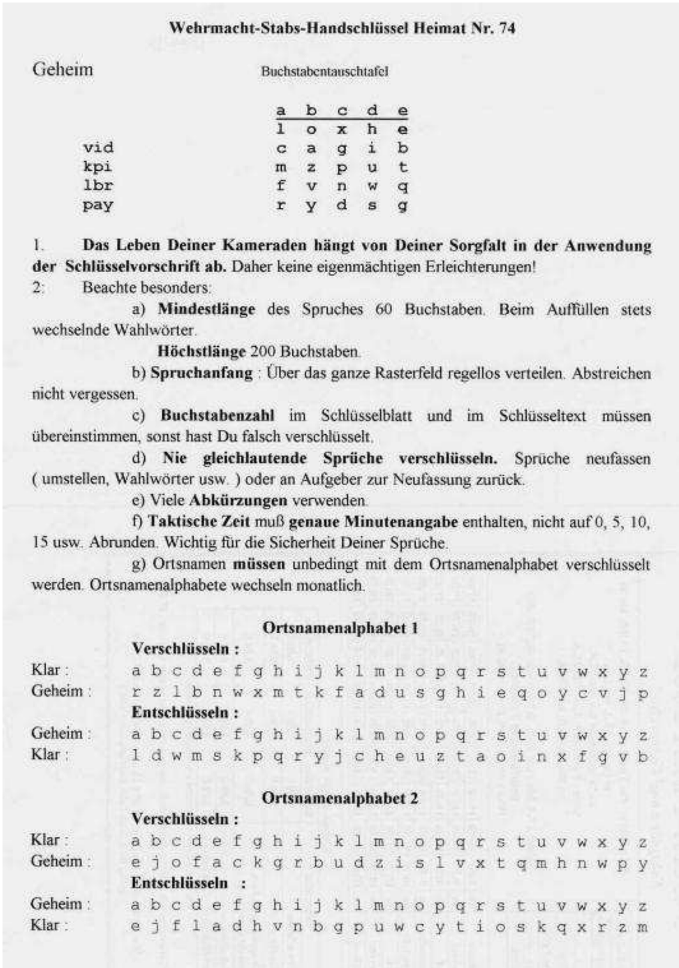
1203 - 77 - tuzd -
```
DIANM RQTVF NNRIS IFFGP UEFZG NAEEH AEUTA IIEAD AGQQL WIBSF FXUTI TEEAA ENIQS
SIRLI EFESE LT
```

Der Rasterschlüssel erschien den Alliierten zunächst praktisch unbrechbar. HINSLEY weist wohl, ohne ihn zu nennen, auf diesen Schlüssel in einer Fussnote hin[108]:

> *The German army in France made much less use of its medium-grade cypher than had been expected, and from February 1943 it adopted a new one which was practically unbreakable; it had been used by the Army in Italy and by the GAF since August 1944 and by the Police since September 1944.*

1.4.1.5 Andere.

Im Bereich des Sicherheitsdienstes war in den letzten Kriegsmonaten ein Tauschtafelschlüssel in Gebrauch. Quersummenbildung aus bestimmten Teilziffern des Spruchkopfes ergab dabei die Stelle im Geheimtext, an der der Kennbuchstabe zum Aufsuchen der benutzten Tauschtafel zu finden war. Die Tauschtafeln waren Bigramm-Tafeln.



Wehrmacht-Stabs-Handschlüssel Heimat Nr. 74

Geheim

Buchstabentauschtafel

	a	b	c	d	e
	l	o	x	h	e
vid	c	a	g	i	b
kpi	m	z	p	u	t
lbr	f	v	n	w	q
pay	r	y	d	s	g

1. **Das Leben Deiner Kameraden hängt von Deiner Sorgfalt in der Anwendung der Schlüsselvorschrift ab.** Daher keine eigenmächtigen Erleichterungen!

2: Beachte besonders:

a) **Mindestlänge** des Spruches 60 Buchstaben. Beim Auffüllen stets wechselnde Wahlwörter.

Höchstlänge 200 Buchstaben.

b) **Spruchanfang** : Über das ganze Rasterfeld regellos verteilen. Abstreichen nicht vergessen.

c) **Buchstabenzahl** im Schlüsselblatt und im Schlüsseltext müssen übereinstimmen, sonst hast Du falsch verschlüsselt.

d) **Nie gleichlautende Sprüche verschlüsseln.** Sprüche neufassen (umstellen, Wahlwörter usw.) oder an Aufgeber zur Neufassung zurück.

e) Viele **Abkürzungen** verwenden.

f) **Taktische Zeit** muß **genaue Minutenangabe** enthalten, nicht auf 0, 5, 10, 15 usw. Abrunden. Wichtig für die Sicherheit Deiner Sprüche.

g) Ortsnamen **müssen** unbedingt mit dem Ortsnamenalphabet verschlüsselt werden. Ortsnamenalphabete wechseln monatlich.

Ortsnamenalphabet 1

Verschlüsseln :

Klar :	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Geheim :	r	z	l	b	n	w	x	m	t	k	f	a	d	u	s	g	h	i	e	q	o	y	c	v	j	p

Entschlüsseln :

Geheim :	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Klar :	l	d	w	m	s	k	p	q	r	y	j	c	h	e	u	z	t	a	o	i	n	x	f	g	v	b

Ortsnamenalphabet 2

Verschlüsseln :

Klar :	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Geheim :	e	j	o	f	a	c	k	g	r	b	u	d	z	i	s	l	v	x	t	q	m	h	n	w	p	y

Entschlüsseln :

Geheim :	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Klar :	e	j	f	l	a	d	h	v	n	b	g	p	u	w	c	y	t	i	o	s	k	q	x	r	z	m

Abbildung 1.31: Schlüsselblatt

1.4.2 Marine.

Bei der Marine gab es ebenfalls mehrere Handverfahren, die unterschiedliche Bedeutung erlangt haben.

[107] NARA Dokument Nr. 3017, Box CBNM57, 6060A «Rasterschluessel (Raster), Series 2, Solution Hints»
[108] HINSLEY II/2, Appendix 15, S. 845

1.4.2.1 Reservehandverfahren.

Als Ersatzschlüssel bei Ausfall des Funkschlüssels M diente das Reservehandverfahren.[109]

Geheim! Vorsicht! Wasserlöslicher Druck! Prüfnr. 3196 b
Ausgabe IV. 44

Tauschtafelweiser
zum R. H. V. Allgemein
M. Dv. Nr. 929/1

Lfde. Nr. der Verfahrenkenngruppe

der Schlüsselkenngruppe	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24				Lfde. Nr. der Schlüsselk
1	7	13	19	2	22	11	6	16	25	1	15	21	5	10	18	4	20	14	9	24	3	17	12	8	23	6	10	1
2	10	20	5	14	23	1	16	9	6	13	25	4	19	8	12	22	2	18	24	7	21	15	3	17	11	14	4	2
3	22	3	10	24	7	14	20	2	16	9	19	11	4	25	6	18	15	5	21	12	17	8	23	13	1	3	19	3
4	8	17	1	20	10	6	24	13	4	19	7	15	22	2	14	25	9	18	11	21	3	23	12	16	5	15	10	4
5	13	6	18	2	21	10	5	22	17	9	20	1	24	14	4	23	11	19	3	16	12	7	25	15	8	18	9	5
6	16	22	4	17	7	20	14	1	24	11	9	19	5	25	12	2	21	8	15	6	23	13	3	18	10	20	11	6
7	9	1	19	13	23	5	21	18	4	25	10	7	17	20	2	16	8	24	11	3	15	12	22	6	14	13	25	7
8	11	4	18	14	10	23	1	21	9	16	5	20	13	8	25	2	19	15	6	22	12	24	7	17	3	23	5	8
9	1	16	6	20	12	4	22	9	19	8	15	2	23	18	10	25	14	5	24	11	17	3	21	7	13	12	22	9
10	20	6	12	23	1	17	8	19	7	24	11	16	2	22	14	5	25	13	3	18	9	21	10	4	15	1	19	10
11	12	16	1	21	13	6	25	10	22	2	18	9	20	5	24	15	3	23	11	8	17	4	19	14	7	16	20	11
12	6	24	10	5	19	14	1	21	9	16	4	25	13	18	7	23	12	2	20	15	8	22	3	17	11	10	21	12
13	2	16	11	24	6	19	15	5	21	9	23	14	1	20	10	17	4	25	7	18	12	3	22	13	8	2	5	13
14	24	7	18	8	14	21	9	16	1	23	6	20	15	2	22	3	17	10	25	11	4	13	5	19	12	18	1	14

Abbildung 1.32: Tauschtafelweiser

Der Funkspruch nach dem R.H.V. hatte die gleiche äussere Form wie ein mit dem Schlüssel M Allgemein chiffrierter Spruch, also nach Uhrzeit (evtl. Datum und Leitnummer) und Gruppenzahl zwei Anfangskenngruppen (aus dem Kenngruppenbuch zu entnehmen und, wie unter 1.3.2.2 beschrieben, chiffriert), dann die den chiffrierten Klartext darstellenden Funkgruppen, am Schluss die Wiederholung der Kenngruppen des Anfangs. Alle Gruppen waren vierstellig. Diese formale Gleichheit mit den Sprüchen des Funkschlüssels M sollte die unbefugte Dechiffrierung erschweren.

Der Klartext wurde zunächst in einem „Kastenwürfel“ , ähnlich dem Verfahren in Abb. 1.27, mit Hilfe einer Zahlenreihe einer Spaltentransposition unterworfen. („Kastenwürfel“). Diese jeweilige Zahlenreihe wurde in einem Tauschtafelweiser durch die dortige Einsatzstelle bestimmt (Abb. 1.32) und der Zahlenreihentafel entnommen (Abb. 1.33). Die Einsatzstelle war festgelegt durch die lfd. Nummer der Verfahrens- und Schlüsselkenngruppen im Kenngruppenbuch.

Zahlenreihentafel
zum R. H. V. Allgemein
M. Dv. Nr. 929/1

Lfde. Nr. (Einsatzstelle)	Zahlenreihe
1	6 10 2 13 7 1 14 5 9 4 12 8 3 11
2	8 1 10 5 2 9 7 4 11 3 6
3	14 4 11 7 3 16 10 12 5 15 2 9 6 13 1 8
4	11 9 3 6 12 1 7 4 10 2 8 5
5	1 13 7 10 2 16 9 17 3 11 6 15 8 5 12 4 14
6	5 7 13 1 9 4 11 2 8 6 12 3 10
7	9 6 1 5 3 8 2 7 4
8	10 4 14 8 13 3 11 9 5 15 7 2 12 6 1
9	3 13 6 9 1 12 8 5 10 2 11 7 4
10	12 4 17 7 13 3 16 9 1 14 8 6 18 11 2 15 10 5
11	4 7 1 10 5 9 2 8 6 3
12	13 4 10 6 14 5 16 1 11 9 3 15 7 2 12 8
13	7 9 5 1 11 8 2 10 6 4 12 3
14	15 5 13 7 2 17 10 1 14 11 4 16 9 3 12 6 8

Abbildung 1.33: Zahlenreihen

Der Klartext wurde entsprechend der Zahlenreihe in verschiedenen Spalten aus dem Kastenschema senkrecht gelesen und so permutiert in Vierergruppen als Buchgruppen untereinander geschrieben. Aus dem Tauschtafelweiser wurden von der Einsatzstelle (1. Zahl) ausgehend vier hintereinander stehende Zahlen entnommen. Diese vier Zahlen definierten die für die vier Spalten anzuwendenden Tauschtafeln. (Abb. 1.34) Jeweils untereinander stehende Paare der Buchgruppen wurden (jede Spalte mit Hilfe der zugeordneten Doppelbuchstaben - Tauschtafel) (Abb. 1.36) paarweise in Funkgruppen chiffriert.

1.4.2.2 Werftschlüssel.

Ab 15.5.1940 datiert der Werftschlüssel (M.Dv.Nr. 103), der im März 1944 überarbeitet wurde. Er wurde angewandt von Werftfahrzeugen, Schiffen und Booten der Luftwaffe, evtl. auch von Küstensicherungs- und Hafenschutzbooten.

[109]M.Dv.Nr. 929/1, Reservehandverfahren, Allgemein, R.H.V. Allg. , 1940

Tafel 1

NA = JT	OA = QN	PA = NS	QA = CS	RA = YZ	SA = KO	TA = DH	UA = LS	VA = PI	WA = HZ	XA = CK	YA = FR	ZA = EQ
B = UQ	B = KG	B = DD	B = RR	B = ST	B = NL	B = OW	B = FV	B = EU	B = OI	B = NY	B = QT	B = OU
C = GO	C = SJ	C = RN	C = EI	C = DF	C = FP	C = IG	C = PW	C = OQ	C = FT	C = BZ	C = JN	C = DP
D = WJ	D = LJ	D = MU	D = PS	D = UM	D = PY	D = SH	D = HJ	D = CI	D = QV	D = WT	D = TL	D = SV
E = IO	E = UU	E = TN	E = JH	E = HD	E = BF	E = AM	E = QX	E = ZL	E = MI	E = GW	E = CU	E = LV
F = YP	F = AS	F = CE	F = TP	F = WL	F = QR	F = UW	F = CO	F = KE	F = TJ	F = UY	F = WZ	F = WV
G = BL	G = YR	G = OS	G = AK	G = KC	G = HN	G = LF	G = VQ	G = SL	G = CM	G = HV	G = KQ	G = MQ
H = OO	H = MC	H = IE	H = VM	H = OY	H = TD	H = NN	H = IQ	H = DJ	H = PU	H = SN	H = PO	H = RP
I = MY	I = WB	I = VA	I = LN	I = CC	I = AU	I = EW	I = RL	I = RX	I = MG	I = AE	I = LD	I = CQ
J = QL	J = GS	J = AY	J = XN	J = YN	J = OC	J = WF	J = BH	J = HP	J = ND	J = OM	J = ZX	J = NW
K = CA	K = VU	K = XL	K = GE	K = IC	K = JL	K = HF	K = SZ	K = NU	K = AO	K = IU	K = BN	K = JP
L = SB	L = JD	L = HX	L = NJ	L = UI	L = VG	L = YD	L = JF	L = AW	L = RF	L = PK	L = SP	L = VE
M = FH	M = XJ	M = ZV	M = BD	M = GA	M = CW	M = BP	M = RD	M = QH	M = LZ	M = FN	M = GC	M = HH
N = TH	N = BB	N = JV	N = OA	N = PC	N = XH	N = PE	N = GK	N = KM	N = VO	N = QJ	N = RJ	N = WX
O = TV	O = NH	O = YH	O = KY	O = AA	O = LT	O = JB	O = WR	O = WN	O = DN	O = KK	O = HR	O = BJ
P = AI	P = HB	P = GI	P = ZT	P = ZH	P = YL	P = QF	P = DV	P = GU	P = SX	P = RV	P = NF	P = TR
Q = RT	Q = VC	Q = US	Q = DX	Q = EY	Q = IY	Q = FJ	Q = NB	Q = UG	Q = IK	Q = DT	Q = EE	Q = IM
R = HT	R = CY	R = BX	R = SF	R = QB	R = QZ	R = ZP	R = GM	R = LB	R = UO	R = TT	R = OG	R = XX
S = PA	S = PG	S = QD	S = MA	S = LH	S = DZ	S = CG	S = PQ	S = TZ	S = BV	S = LP	S = JJ	S = AG
T = DB	T = IW	T = KA	T = YB	T = NQ	T = RB	T = XR	T = AC	T = FF	T = XD	T = VY	T = XV	T = QP
U = VK	U = ZB	U = WH	U = FD	U = BT	U = ME	U = MO	U = OE	U = OK	U = KS	U = EA	U = AQ	U = KI
V = LL	V = EC	V = FX	V = WD	V = XP	V = ZD	V = NO	V = JZ	V = BR	V = ZF	V = YT	V = ZZ	V = PM
W = ZJ	W = TB	W = UC	W = IS	W = JX	W = EO	W = GY	W = TF	W = XZ	W = GG	W = MS	W = IA	W = FL
X = EK	X = DR	X = ES	X = UE	X = VI	X = WP	X = RZ	X = EG	X = II	X = ZN	X = ZR	X = FZ	X = YJ
Y = XB	Y = RH	Y = SD	Y = HL	Y = MW	Y = MM	Y = KU	Y = XF	Y = XT	Y = EM	Y = MK	Y = DL	Y = GQ
Z = KW	Z = FB	Z = LR	Z = SR	Z = TX	Z = UK	Z = VS	Z = LX	Z = JR	Z = YF	Z = VW	Z = RA	Z = YV

Abbildung 1.34: Tauschtafel RHV

Er war, im Unterschied zu den sonstigen Schlüsseln der Marine, in Fünfergruppen gegliedert. Zur Kenntlichmachung wurde er verschiedentlich mit einem „gr“ vor der Gruppenzahl versehen.

Tauschtafelweiser 2 98

zum Werftschlüssel — M. Dv. Nr. 103.

Vierter und fünfter Buchstabe der Kenngruppe

	aa	bj	cm	dc	et	fi	gz	hl	is	jb	kx	ld	mr	np	ow	ph	qy	ra	sv	tk	un	vf	wu	xq	yo	zg					
aq	18	10	2	15	5	20	1	14	9	11	16	8	13	19	4	17	6	12	3	7	10	5	14	19	2	18	8	15	9	13	aq
bf	4	16	12	7	13	3	10	6	18	2	5	20	17	1	11	8	14	19	9	15	1	12	4	16	6	11	3	20	17	7	bf
ck	9	1	4	19	17	8	15	3	6	14	10	7	12	5	16	20	18	2	13	11	6	20	7	13	9	15	18	10	1	16	ck
dy	11	18	9	3	1	19	4	17	12	7	15	13	16	8	6	2	5	10	20	14	17	2	11	4	19	8	12	5	14	3	dy
eg	5	11	16	13	20	14	6	10	3	19	1	18	8	12	17	9	15	7	4	2	19	8	6	15	10	1	14	17	11	9	eg
fv	13	3	14	10	16	11	9	19	7	12	8	15	4	6	2	18	1	20	17	5	3	13	16	7	12	5	20	2	4	18	fv
gi	19	7	18	6	11	5	13	8	15	17	4	9	2	14	10	12	3	16	1	20	15	9	18	1	14	19	7	12	8	10	gi
he	14	5	3	9	6	12	17	2	13	10	20	11	15	4	19	7	16	1	8	18	4	17	20	11	5	3	13	16	6	2	he
ip	2	17	20	11	3	18	12	4	1	16	7	19	6	9	5	14	8	15	10	13	11	1	15	8	16	6	9	18	3	12	ip
jr	19	13	1	16	14	2	7	15	5	8	3	17	11	20	18	10	4	6	12	9	7	14	10	17	4	20	2	13	19	5	jr
kh	12	8	19	14	9	7	16	10	2	4	6	1	3	15	20	13	11	18	5	17	9	16	2	20	8	17	15	4	7	14	kh
lj	6	14	5	2	15	9	3	20	11	13	17	10	7	18	12	1	19	4	16	8	5	3	12	18	1	10	19	11	13	6	lj
mt	8	2	13	17	10	16	5	1	19	3	9	12	20	7	15	11	6	14	18	4	13	10	5	9	11	14	16	1	18	20	mt

Abbildung 1.35: Werftschlüssel

Der Klartext wurde unmittelbar mit Bigrammtauschtafeln chiffriert. Dazu wurde er in Fünfergruppen geschrieben (Buchgruppen), diese untereinander in ein Schlüsselformular, und zwar in die Zeilen 3, 5, 7, .. 11, dann in die Zeilen 4, 6, .. 12, anschliessend ab 13. Zeile fortlaufend. (Vor 1944 offenbar schon ab der 10. Zeile fortlaufend). Da im nächsten Schritt die übereinander stehenden Paare der 3. und 4. Zeile, der 5. und 6. usw. im Bigrammtauschverfahren chiffriert werden sollten, musste der Spruch in chiffrierter Form eine Angabe über die für die einzelnen Spalten geltenden Tauschtafelnummern enthalten. (Abb. 1.36) Dazu dienten zwei Kenngruppen im Kopf des Spruches. In einem Tauschtafelweiser, der die Zahlen 1 bis 30 (vor 1944: 1 bis 20) in willkürlicher Folge in einer rechteckigen Matrix mit Buchstabenpaaren als „Koordinaten“ enthielt, wurde eine Zahl als Einsatzstelle ausgewählt und die Buchstabenpaare links und oben (Mit einem beliebigen Füllbuchstaben in der Mitte) zur Kenngruppe zusammengefasst. Diese (erste) Kenngruppe wurde durch eine zweite, willkürlich gebildete Kenngruppe ergänzt (Abb. 1.35). Abbildung 1.37 zeigt eine spätere Version des Tauschtafelweisers, der dem Chiffrierer auch die Wahl zwischen mehreren Möglichkeiten der Chiffrierung der Einsatzstelle eröffnete. Die gewählte Einsatzstellen-Zahl und die vier waagerecht (oder, je nach Tagesdatum senkrecht) benachbarten Zahlen bildeten die Tauschtafelfolge. Die erste und die zweite Kenngruppe wurden nach dem Tauschtafelplan für den Tag senkrecht paarweise im Bigrammtauschverfahren chiffriert.

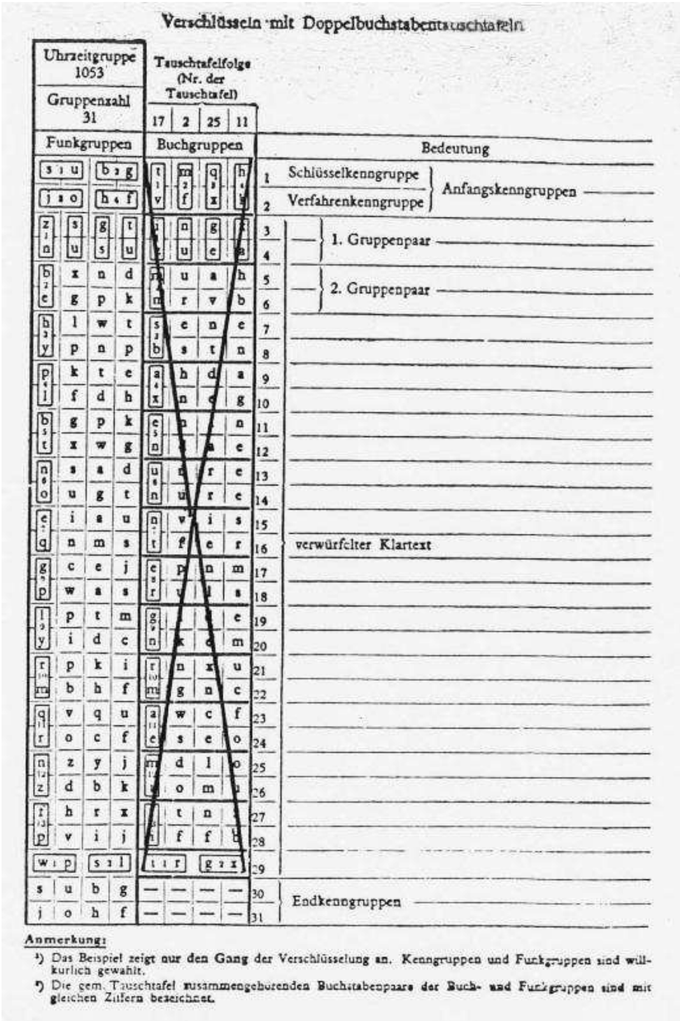


Abbildung 1.36: Schlüsselblatt RHV

Zunächst waren immer 20 Tauschtafeln für zwei Monate gültig, später 30 Tauschtafeln pro Monat[110]. MORRIS schreibt a.a.O., es hätte 38 Schlüsselhefte mit Tauschtafeln zum Werftschlüssel gegeben. Demgegenüber liegt bereits von 1940 ein Schlüsselheft Nr. 42 vor (in Kraft ab 7.12.40), von 1941 ein Schlüsselheft Nr. 47.[111] MORRIS erwähnt als Charakteristikum der Tauschtafeln, dass niemals ein Buchstabe eines Bigramms im zugehörigen Paar des Geheimtextes aufgetreten wäre. Das galt offenbar erst für die späteren Ausgaben. Wie Abbildung 1.38 von 1941 zeigt, gilt in dieser Tauschtafel u.a. `AF`$\mapsto$`QA`. Andere Tauschtafeln lassen die von MORRIS beschriebene Eigenschaft erkennen.
Die M.Dv.Nr. 103 von 1944 ordnete weiter an, dass die einzelnen Sprüche durch Anhängen von Wörtern auf verschiedene Längen gebracht werden sollten. Dabei wurden als Beispiele die Wörter Wassereimer, Fernsprecher und Kleiderschrank genannt. Zu den Folgen siehe Kap. 6.2.2.2.3. Dieses Verfahren hat v.d.MEULEN sehr ausführlich beschrieben.[112]

1.4.2.3 Andere

1.4.2.3.1 Henno. Der Schlüssel Henno:[113] Ähnlich strukturiert wie das R.H.V. war der Schlüssel Henno, der seit Mai 1943 im Mittelmeer benutzt wurde. Das Kenngruppenverfahren unterschied sich allerdings erheblich vom R.H.V.
Der Chiffrierer wählte frei vier Buchstaben, die die erste Funkgruppe bildeten. Aus den im Schlüsselverteilungsplan Süd angegebenen Zahlen wurde eine gewählt und in einer speziellen Kenngruppentafel[114] das zu dieser Zahl und dem ersten Buchstaben der gewählten Vierergruppe gehörige Matrixelement ausgelesen. Dies war der erste Buchstabe der zweiten Funkgruppe. Eine weitere Zahl aus dem Schlüsselverteilungsplan bestimmte in der Zahlenreihentafel die Zahlenfolge, die zur Permutation des Spruchtextes nötig war. Mit dieser Zahl wurde wieder in der Kenngruppentafel unter dem zweiten gewählten Buchstaben der ersten Funkgruppe der zweite Buchstabe der zweiten Funkgruppe ausgelesen. Mit einer dritten Zahl wurde ebenso der dritte Buchstabe der zweiten Funkgruppe bestimmt, sie war auch gleichzeitig die Zeilennummer für den Tauschtafelweiser. Mit einer vierten Zahl schliesslich wurde der vierte Buchstabe der zweiten Funkgruppe ermittelt, sie war auch die Spaltenzahl für den Tauschtafelweiser. Im Schnittpunkt der gefundenen Zeile und

[110] KAHN a), S.118; MORRIS, S. 113
[111] BA/MA, RMD 4/103, Nr. 47
[112] MEULEN, van der, b), c)
[113] M.Dv.Nr. 167
[114] In einer 26 x 26 Matrix waren oben das Alphabet und links von oben nach unten die Zahlen 1 bis 26 aufgetragen. Die Matrixzeilen enthielten voneinander verschiedene permutierte Alphabete.

Spalte fand man die Einsatzstelle mit den drei rechten Nachbarn, die die Zahlen der Tauschtafeln darstellten, mit denen die senkrechten Bigramme der vier Spalten des permutierten Klartextes chiffriert wurden.

Im April 1944 gelangten die Alliierten in den Besitz aller Chiffrierunterlagen. Da deutscherseits die dadurch notwendig gewordenen Änderungen der Tauschtafeln und der Tauschtafelweiser nach und nach und nicht auf einmal erfolgten, wurde die alliierte Dechiffrierungsarbeit kaum behindert.

Nach Aussagen von MORRIS[115] war das Volumen des Verkehrs in diesem Schlüssel zwar gross, aber wegen des offenbar für die Alliierten geringen Nachrichtenwertes wurde die Arbeit an diesem Schlüssel im August 1944 eingestellt.

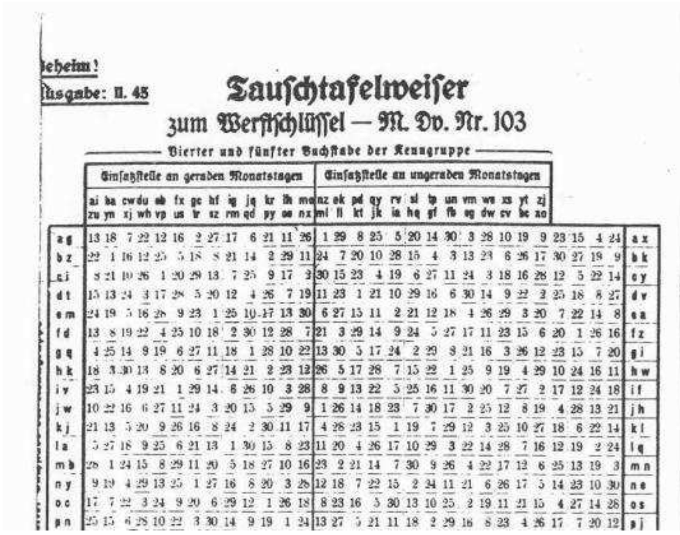
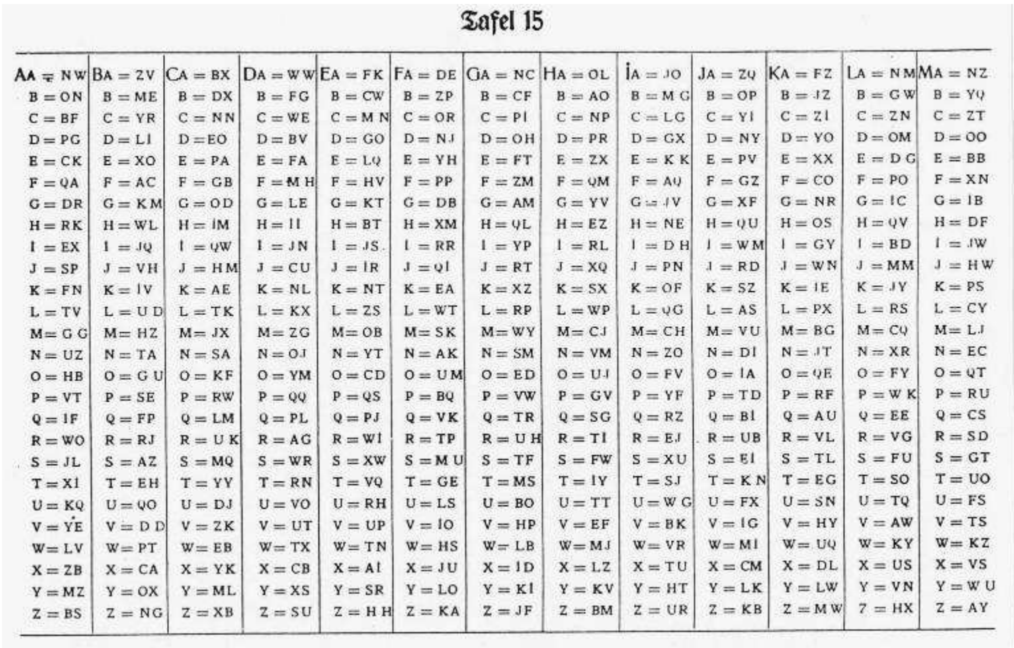


Abbildung 1.37: Werftschlüssel



Tafel 15

AA = NW	BA = ZV	CA = BX	DA = WW	EA = FK	FA = DE	GA = NC	HA = OL	IA = JO	JA = ZQ	KA = FZ	LA = NM	MA = NZ
B = ON	B = ME	B = DX	B = FG	B = CW	B = ZP	B = CF	B = AO	B = MG	B = OP	B = JZ	B = GW	B = YQ
C = BF	C = YR	C = NN	C = WE	C = MN	C = OR	C = PI	C = NP	C = LG	C = YI	C = ZI	C = ZN	C = ZT
D = PG	D = LI	D = EO	D = BV	D = GO	D = NJ	D = OH	D = PR	D = GX	D = NY	D = YO	D = OM	D = OO
E = CK	E = XO	E = PA	E = FA	E = LQ	E = YH	E = FT	E = ZX	E = KK	E = PV	E = XX	E = DG	E = BB
F = QA	F = AC	F = GB	F = MH	F = HV	F = PP	F = ZM	F = QM	F = AQ	F = GZ	F = CO	F = PO	F = XN
G = DR	G = KM	G = OD	G = LE	G = KT	G = DB	G = AM	G = YV	G = JV	G = XF	G = NR	G = IC	G = IB
H = RK	H = WL	H = IM	H = II	H = BT	H = XM	H = QL	H = EZ	H = NE	H = QU	H = OS	H = QV	H = DF
I = EX	I = JQ	I = QW	I = JN	I = JS.	I = RR	I = YP	I = RL	I = DH	I = WM	I = GY	I = BD	I = JW
J = SP	J = VH	J = HM	J = CU	J = IR	J = QI	J = RT	J = XQ	J = PN	J = RD	J = WN	J = MM	J = HW
K = FN	K = IV	K = AE	K = NL	K = NT	K = EA	K = XZ	K = SX	K = OF	K = SZ	K = IE	K = JY	K = PS
L = TV	L = UD	L = TK	L = KX	L = ZS	L = WT	L = RP	L = WP	L = QG	L = AS	L = PX	L = RS	L = CY
M = GG	M = HZ	M = JX	M = ZG	M = OB	M = SK	M = WY	M = CJ	M = CH	M = VU	M = BG	M = CQ	M = LJ
N = UZ	N = TA	N = SA	N = OJ	N = YT	N = AK	N = SM	N = VM	N = ZO	N = DI	N = JT	N = XR	N = EC
O = HB	O = GU	O = KF	O = YM	O = CD	O = UM	O = ED	O = UJ	O = FV	O = IA	O = QE	O = FY	O = QT
P = VT	P = SE	P = RW	P = QQ	P = QS	P = BQ	P = VW	P = GV	P = YF	P = TD	P = RF	P = WK	P = RU
Q = IF	Q = FP	Q = LM	Q = PL	Q = PJ	Q = VK	Q = TR	Q = SG	Q = RZ	Q = BI	Q = AU	Q = EE	Q = CS
R = WO	R = RJ	R = UK	R = AG	R = WI	R = TP	R = UH	R = TI	R = EJ	R = UB	R = VL	R = VG	R = SD
S = JL	S = AZ	S = MQ	S = WR	S = XW	S = MU	S = TF	S = FW	S = XU	S = EI	S = TL	S = FU	S = GT
T = XI	T = EH	T = YY	T = RN	T = VQ	T = GE	T = MS	T = IY	T = SJ	T = KN	T = EG	T = SO	T = UO
U = KQ	U = QO	U = DJ	U = VO	U = RH	U = LS	U = BO	U = TT	U = WG	U = FX	U = SN	U = TQ	U = FS
V = YE	V = DD	V = ZK	V = UT	V = UP	V = IO	V = HP	V = EF	V = BK	V = IG	V = HY	V = AW	V = TS
W = LV	W = PT	W = EB	W = TX	W = TN	W = HS	W = LB	W = MJ	W = VR	W = MI	W = UQ	W = KY	W = KZ
X = ZB	X = CA	X = YK	X = CB	X = AI	X = JU	X = ID	X = LZ	X = TU	X = CM	X = DL	X = US	X = VS
Y = MZ	Y = OX	Y = ML	Y = XS	Y = SR	Y = LO	Y = KI	Y = KV	Y = HT	Y = LK	Y = LW	Y = VN	Y = WU
Z = BS	Z = NG	Z = XB	Z = SU	Z = HH	Z = KA	Z = JF	Z = BM	Z = UR	Z = KB	Z = MW	7 = HX	Z = AY

Abbildung 1.38: Werftschlüssel-Tauschtafel

[115] MORRIS, S. 118

Kapitel 2

Darstellungen.

2.1 Streifen und Matrizen.

2.1.1 Streifenmodell.

Die bekannte Verdrahtung der Chiffrierwalzen kann benutzt werden, um ein Streifenmodell für die ENIGMA zu entwerfen, mit dem Chiffrier- und Dechiffrieraufgaben bewältigt werden können.
Dabei ist es vorteilhaft, die Verdrahtung auf ein raumfestes Koordinatensystem zu beziehen. Dazu dient die feste Eingangswalze, die hinfort Referenzwalze genannt wird. Sie bildet gewissermassen ein raumfestes Koordinatensystem.

Am Beispiel der Chiffrierwalze I der Wehrmacht-ENIGMA soll die Herleitung eines solchen Streifens deutlich gemacht werden. Dabei ist die Lage der Walze so, dass bei einer Ringstellung `A` der Eingangspunkt `A` der Walze bei dem Buchstaben `A` der Eingangswalze liegt, d.h. im Fenster der Maschine ist der Buchstabe `A` zu sehen.
Jeder Eingangspunkt (`A, B, ...`) wird mit seinem durch die Verdrahtung gegebenen Ausgangspunkt verbunden, der die Bezeichnung des Eingangspunktes erhält.
Auf diese Weise entsteht der Streifen

Referenzwalze:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Walzeneingang:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Walzenausgang:	U	W	Y	G	A	D	F	P	V	Z	B	E	C	K	M	T	H	X	S	L	R	I	N	Q	O	J

Wenn im Tastenfeld der Buchstabe `U` gedrückt worden ist wird der Ausgang aus der Walze I bei `A` der Referenzwalze liegen.

2.1.2 Matrix.

Wird die Walze I um eine Position verschoben (bei fortdauernder Ringstellung `A` ist also im Fenster der Buchstabe `B` zu sehen), ergibt das die Streifenlage

Referenzwalze:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Walzeneingang:	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
Walzenausgang:	W	Y	G	A	D	F	P	V	Z	B	E	C	K	M	T	H	X	S	L	R	I	N	Q	O	J	U

Die Eingabe `V` in der Tastatur führt nun wegen der um eine Stelle verdrehten Walze zum Walzeneingang `W`, der Walzenausgang ist nun `B` an der Stelle `A` der Referenzwalze, für die Walzenposition `C` führt die Eingabe `W` der Tastatur (die Walze wiederum eine Stelle weitergedreht) zum Eingang `Y` der Walze und so zum Ausgang `C`, bei der Walzenlage `D` führt die Eingabe `D` (auf dem „Umweg“)

über `G`) zum Ausgang , immer an der Stelle `A` der Referenzwalze . Wenn man das hier begonnene Verfahren für die weiteren Stellungen der Referenzwalze fortsetzt, erhält man eine Matrix aus den obigen Streifen. Die die Spalten definierenden Kopfbuchstaben gehören zu den Walzenstellungen (bei Ringstellung `A`). Die Buchstaben im Matrixfeld sind die, die in der Tastatur eingegeben werden, die linke Spalte gibt den Ausgang aus der Walze für den jewils eingetasteten Buchstaben, bezogen auf die Referenzwalze. (Tabelle A.1 im Anhang, S. 186)
Diese Art der Streifen kann zum Chiffrieren benutzt werden (Walzeneingang rechts im Matrixfeld unter der Walzenstellung, Walzenausgang links: Refenzbuchstabe). Umgekehrt kann der Durchgang durch die Walze von links nach rechts, also beim Dechiffrieren, abgelesen werden (Eingang Referenzbuchstabe, Ausgang im Matrixfeld unter der Walzenstellung).

Wird der obige erste Streifen für den Rotor I der Wehrmacht-ENIGMA umgeordnet, ist ebenfalls eine Matrix erstellbar, die ebenso zum Chifferieren/Dechiffrieren geeignet ist (Tablelle A.2 im Anhang, S. 186).

Eingangswalze:	`A B C D E F G H I J K L M N O P Q R S T U V W X Y Z`
Walzeneingang:	`A B C D E F G H I J K L M N O P Q R S T U V W X Y Z`
Walzenausgang:	`E K M F L G D Q V Z N T O W Y H X U S P A I B R C J`

Aus obigem «rod-square» kann man ablesen, dass z.B. für die Walzenstellung `A` (nach dem Tasten und für Ringstellung `A`) der Klarbuchstabe `A` (Zeilenbezeichnung) zum Ausgang (Geheimbuchstaben) `E` führt, für Walzenstellung `B` zu `J`, für `C` zu `K`. usw. So entsteht eine weitere, für die Walze charakteristische Matrix (Tabelle A.2 im Anhang. Im Anhang sind die Matrizen der ersten drei Walzen der Wehrmacht-ENIGMA angegeben.
Man kann die Matrix[1] (Version A) so verstehen: Ein bei einer durch einen Kopfbuchstaben definierten Walzenstellung im Matrixfeld eingetasteter Buchstabe (Klartext oder Geheimtext) führt zum durch den Referenzausgang (linke Spalte) gegebenen Buchstaben (Geheimtext oder Klartext).

Es fällt auf, dass das Referenzalphabet `A, B, C,` ... in jeder Diagonalen von rechts oben nach links unten auftritt. Dass dies so sein muss, zeigt folgende Überlegung: Angenommen, zur Walzenstellung `F` sei der Buchstabe `Q` getastet worden. Der Ausgang der Walze liegt dann bei `D`. Wenn die Walze um einen Schritt auf `G` rückt, wird der Buchstabe `P`, der um einen Schritt vor `Q` liegt, dieselbe Verdrahtung der Walze benutzen und infolgedessen zum Referenzbuchstaben `C` (einen Schritt vor `D`) führen.

Die entsprechenden charakteristischen Matrizen für die Walze II lauten (Tabellen A.3 und A.4 im Anhang) Für die Walze III sind es die Matrizen der Tabellen A5 und A6 im Anhang.

Mit Hilfe der o.g. Streifen lässt also sich ein Modell der ENIGMA darstellen, mit dem man die Zusammenhänge in der Maschine überblicken und Chiffrier- und Dechiffrieraufgaben lösen kann.[2]

Für ein praktisches Beispiel sei die Umkehrwalze `B` eingesetzt, die Reihenfolge der Walzen sei (v.l.n.r.) II, III, I und die Stellung der Walzen `Q, C` und `Y` (nach dem Tasten des Beispielbuchstabens). Die Walzenstreifen muss man sich nach oben und unten fortgesetzt vorstellen. Die nicht grau unterlegten Streifen stellen das (raumfeste) System der Eingangswalze dar. Die Ringstellungen seien (v.l.n.r.) `R, B` und `K`. Letztere sind durch Unterstreichen markiert. Der Klarbuchstabe sei `R`. Man kann verfolgen, wie die einzelnen Walzen auf dem „Hinweg“ (**Fettdruck**)und auf dem „Rückweg“ (***kursiver Fettdruck***) den Geheimbuchstaben `G` erzeugen. Es sei hier auf eine besondere Eigenschaft der Matrix von Tabelle 2.1 aufmerksam gemacht. Der Klarbuchstabe `R` führt im Beispiel zum Geheimbuchstaben `G`. Wenn die Walze I um eine Stelle weiterrückt und der Klarbuchstabe `A` werde chiffriert, so ist das Ergebnis `H`. Wenn die Walze I wiederum um eine Position weiterrückt und der Buchstabe `F` chiffriert wird, ist der entstehende Geheimbuchstabe `I`.

[1] Im angelsächsischen Sprachgebrauch ist es das rod-square, die Spalten heissen uprights, die Zeilen rods

[2] von KOSS ist im Juli 2004 ein solches Modell «The Paper Enigma Machine» veröffentlicht worden. Bei TURING, Kap. 1, findet sich ein ähnliches Beispiel

Voraussetzung dabei war, dass die übrigen Walzen nicht weiterrückten. Wenn man die Ergebnisse in dem Quadrat von Tabelle A.1 im Anhang betrachtet, sieht man, dass die zu den Klarbuchstaben `R, A, F`, die in den Spalten `O, P, Q` der Walzenstellung in der Zeile `S` stehen, zugehörigen Geheimbuchstaben `G, H, I` in denselben Spalten, aber alle in der Zeile `M` zu finden sind. Es gilt generell:

> Wenn eine Zeile des Quadrates - unter Berücksichtigung der jeweiligen Walzenstellung und ohne Weiterrücken anderer Walzen - chiffriert wird, steht der Geheimtext der Zeile in einer anderen Zeile desselben Quadrates.

U-Walze			Walze II					Walze III					Walze I						
01	A	01	01	A	S	26	Z	01	A	A	02	B	01	A	M	15	O	01	A
02	B	02	02	B	A	01	A	02	B	G	03	C	02	B	T	16	P	02	B
03	C	03	03	C	J	02	B	03	C	B	04	D	03	C	H	17	Q	03	C
04	D	04	04	D	P	03	C	04	D	P	05	E	04	D	X	18	R	04	D
05	E	05	05	E	C	04	D	05	E	C	06	F	05	E	S	19	S	05	E
06	F	06	06	F	Z	05	E	06	F	S	07	G	06	F	L	20	T	06	F
07	G	07	07	G	W	06	F	07	G	D	08	H	07	G	R	21	***U***	07	***G***
08	H	04	08	H	R	07	G	08	H	Q	09	I	08	H	I	22	V	08	H
09	I	**08**	09	I	***L***	08	H	09	I	E	10	J	09	I	N	23	W	09	I
10	J	09	10	J	F	09	I	10	J	U	11	K	10	J	Q	24	X	10	J
11	K	10	11	K	B	10	J	11	K	F	12	L	11	K	O	25	Y	11	K
12	L	07	12	L	D	11	K	12	L	V	13	M	12	L	J	26	Z	12	L
13	M	11	13	M	K	12	***L***	13	M	***N***	14	***N***	13	M	***U***	01	A	13	M
14	N	10	14	N	O	13	M	14	N	Z	15	O	14	N	W	02	B	14	N
15	O	11	15	O	T	14	N	15	O	H	16	P	15	O	Y	03	C	15	O
16	P	**08**	16	P	**Y**	15	O	16	P	Y	17	Q	16	P	G	04	D	16	P
17	Q	05	17	Q	U	16	P	17	Q	I	18	R	17	Q	A	05	E	17	Q
18	R	02	18	R	Q	17	Q	18	R	X	19	S	18	R	D	06	**F**	18	**R**
19	S	06	19	S	G	18	R	19	S	J	20	**T**	19	S	**F**	07	G	19	S
20	T	12	20	T	E	19	S	20	T	W	21	U	20	T	P	08	H	20	T
21	U	03	21	U	N	20	T	21	U	L	22	V	21	U	V	09	I	21	U
22	V	13	22	V	H	21	U	22	V	R	23	W	22	V	Z	10	J	22	V
23	W	13	23	W	X	22	V	23	W	K	24	X	23	W	B	11	K	23	W
24	X	09	24	X	M	23	W	24	X	O	25	Y	24	X	E	12	L	24	X
25	Y	01	25	Y	I	24	X	25	Y	M	26	Z	25	Y	C	13	M	25	Y
26	Z	12	26	Z	V	25	**Y**	26	Z	**T**	01	A	26	Z	K	14	N	26	Z

Tabelle 2.1:

2.2 Klassen

Wenn man die Substitutionen, die die einzelnen Chiffrierwalzen relativ zur Eingangswalze darstellen, als Permutation darstellt[3], erhält man eine für jede Walze charakteristische, eindeutige Form. Im Beispiel für die Walze I

$$\begin{pmatrix} \mathtt{A\,B\,C\,D\,E\,F\,G\,H\,I\,J\,K\,L\,M\,N\,O\,P\,Q\,R\,S\,T\,U\,V\,W\,X\,Y\,Z} \\ \mathtt{E\,K\,M\,F\,L\,G\,D\,Q\,V\,Z\,N\,T\,O\,W\,Y\,H\,X\,U\,S\,P\,A\,I\,B\,R\,C\,J} \end{pmatrix}$$

erhält man die Zyklen

[3] BAUER, S.120

(A E L T P H Q X R U)(B K N W)(C M O Y)(D F G)(I V)(J Z)(S)

Diese Aufteilung ist unabhängig von der Anwendung von Steckern. Mit den Steckern der Verfahrenssimulation zur ENIGMA-Uhr erhält man z.B.

(F E Y Q H P T N V J)(W K X B)(G M O L)(D A C)(I R)(U S)(Z)
Durch Trensformation dieser Zyklen mit der „Verschiebungs-Permutation“ (ABCDEFGHIJKLMNOPQRSTUVWXYZ) erhält man alle Spalten der Tabelle A.2, S. 186.

Die charakteristischen Zyklenlängen betragen für die Chiffrierwalzen der Wehrmacht-ENIGMA

Walzennummer	Zyklen
I	10, 4, 4, 3, 2, ,2 ,1
II	8, 7, 3, 2, 2, 2, 1, 1
III	17, 8, 1
IV	22, 2, 2
V	11, 9, 6
VI	14, 8, 4
VII	26
VIII	17, 3, 3, 3

Klasse Vermutlich auf TURING geht eine andere Methode der Identifizierung jeder Walzenverdrahtung zurück, die ebenfalls von evtl. Steckern unabhängig ist . Dazu dient die Klasse der Transformationen, die eine Spalte einer charakteristischen Matrix in die nächst benachbarte überführen. Unter „Klasse“ sind die Ordnungen der Zyklen der Transformation zu verstehen.

Für die Spalten A und B der Walze I ergeben sich die Zyklen
(U-V-Y-F-O-I-M-S-K-L-Q-N-P)(W-X-R-H)(G-Z-A-C-J-T)(D-E-B)
Die Klasse der Walze I ist demnach 3, 4, 6, 13. Falls bei zwei untersuchten Walzen die Klassen übereinstimmen, kann die Zyklenbildung für zwei nicht benachbarte Spalten des Quadrates die Entscheidung bringen, ob die beiden Walzen identisch sind.

Walzennummer	Zyklen 1. Ordnung	Zyklen 2. Ordnung
I	3, 4, 6, 13	1, 2, 9,14
II	10, 16	5, 7, 7, 7
III	6, 6, 7, 7	1, 1, 6, 18
IV	2, 2, 11, 11	3, 6, 8, 9
V	2, 6, 9, 9	2, 7, 8, 9
VI	2, 24	2, 3, 5, 16
VII	4, 5, 5, 12	2, 24
VIII	2, 24	4, 22
UKW B	1, 7, 8, 10	1, 1, 2, 2, 4, 5, 11
UKW C	2, 2, 9, 13	1, 2, 6, 8, 9
B dünn	1, 4, 5, 16	1, 2, 2, 6, 15
C dünn	1, 25	1, 2, 3, 3, 4, 8
Beta	2, 2, 3, 3, 7, 9	1, 3, 5, 17
Gamma	2, 3, 8, 13	2, 3, 9, 12

Für die Umkehrwalzen versagt das geschilderte Verfahren; es gibt keine charakteristische Matrix. Man kann sich behelfen und die Transformation zwischen der Umkehrwalze und der um eine Position verschobenen Umkehrwalze ersatzweise heranziehen. Besser geeignet für die Identifizierung der Walzen ist jedoch die Untersuchung bzgl. des jeweiligen Eingangs bzw. Ausgangs.

Kapitel 3

Steckerlose ENIGMA

3.1 Ermittlung der Walzenverdrahtungen

3.1.1 Saga

Die Chiffriermaschine ENIGMA ohne Stecker ist schon frühzeitig als nicht „einbruchsicher“ erkannt worden. Als Beispiele seien genannt:

Solution of the Commercial ENIGMA Machine[1]
Analysis of the Cipher Machine „ENIGMA“Type K[2]
TURING's Treatise on the ENIGMA[3]

Die folgende Darstellung beruht auf Kap. 3 des Treatise von TURING. Als Arbeitsmaterial werden vollständige chiffrierte Alphabete zugrunde gelegt. Natürlich lässt sich einwenden, dass, wenn man solche vollständigen Alphabete erstellt, eine Maschine zur Verfügung stehen müsste, deren Walzenverdrahtung sich durch einfache Durchgangsprüfung an den Walzen ermitteln liesse. Andererseits lassen sich aber mit sehr viel chiffriertem Material diese Alphabete auch - wenn auch u.U. lückenhaft - fortlaufend kombinieren. Vorausgesetzt werden: Walzenlage III, II, I der Wehrmacht-ENIGMA I, Umkehrwalze A, Ringstellung A, A, A. (Verwendung der Zweierzyklen von Tabelle 3.1)

Boxing Wenn man diese Alphabete „über Kreuz“ miteinander verknüpft (was TURING «Boxing» nennt), erhält man nach geeigneter Umstellung die folgende Darstellung, z.B:

```
(AAA):   (AO)(ZM)(SI)(VW)(HB)(EC)(LD)(KR)(YG)(NT)(FP)   | (JU)(QX)
(ABA):    A)(OZ)(MS)(IV)(WH)(BE)(CL)(DK)(RY)(GN)(TF)(P  | J)(UQ)(X
```

(AAA)(ABA) = (AOZ*M*SIVWHBECL*D*KRYGNTFP)(JUQX)

Entsprechende Verknüpfung für (AAB) und (ABB):

```
(AAB):   (AS)(BJ)(CI)(DW)(EQ)(FZ)(GP)(HL)(KM)(NR)(OU)(TV)(XY)
(ABB):   (AI)(BD)(CU)(EL)(FH)(GO)(JQ)(KS)(MY)(NV)(PZ)(RT)(WX)
```

das Ergebnis in Zyklenform geschrieben und geordnet:

(AAB)(ABB) = (CIA*S*KMYXWDBJQ*E*LHFZPGOU)(TVNR)

[1] NARA Dokument Box ZEMA155, Nr. 4083
[2] NARA Dokument Box CBQM 33, Nr. 3448, dabei handelt es sich um eine deutsche Quelle im Originaltext.
[3] NARA Dokument, Box CBCB55, Nr. 964, Teile dieser Abhandlung aus den Jahren 1939 bis 1942 sind von Ralph Erskine, Philip Marks und Frode Weierud als Herausgeber in lesbarer Form und von erkennbaren Schreibfehlern gereinigt im Internet veröffentlicht worden.

Grundstellung	
AAA	(AO),(BH),(CE),(DL),(FP),(GY),(IS),(JU),(KR),(MZ),(NT),(QX),(VW)
AAB	(AS),(BJ),(CI),(DW),(EQ),(FZ),(GP),(HL),(KM),(NR),(OU),(TV),(XY)
AAC	(AQ),(BY),(CF),(DS),(EZ),(GN),(HJ),(IK),(LR),(MV),(OP),(TX),(UW)
AAD	(AC),(BX),(DV),(EN),(FL),(GP),(HI),(JQ),(KS),(MT),(OR),(UZ),(WY)
AAE	(AX),(BL),(CW),(DP),(ES),(FJ),(GO),(HQ),(IN),(KT),(MV),(RU),(YZ)
ABA	(AP),(BE),(CL),(DK),(FT),(GN),(HW),(IV),(JX),(MS),(OZ),(QU),(RY)
ABB	(AI),(BD),(CU),(EL),(FH),(GO),(JQ),(KS),(MY),(NV),(PZ),(RT),(WX)
ABC	(AI),(BM),(CS),(DX),(EQ),(FP),(GK),(HW),(JU),(LY),(NR),(OZ),(TV)
ABD	(AN),(BL),(CG),(DR),(ES),(FU),(HJ),(IX),(KQ),(MY),(OV),(PW),(TZ)
ABE	(AR),(BK),(CE),(DM),(FY),(GU),(HX),(IP),(JO),(LQ),(NZ),(SW),(TV)
ACA	(AI),(BE),(CR),*(DM)*,(FG),(HV),(JL),(KT),(NU),(OP),(QZ),(SW),(XY)
ACB	(AN),(BD),(CM),*(ES)*,(FR),(GL),(HJ),(IU),(KX),(OZ),(PV),(QT),(WY)
ACC	(AI),(BT),(CH),(DO),(EP),(FN),(GU),(JY),(KL),(MW),(QZ),(RV),(SX)
ACD	(AO),(BI),(CW),(DG),(EP),(FX),(HJ),(KV),(LM),(NQ),(RZ),(SU),(TY)
ACE	(AU),(BE),(CM),(DK),(FR),(GS),(HT),(IP),(JZ),(LX),(NY),(OV),(QW)
ADA	(AD),(BI),(CF),(EQ),(GR),(HM),(JV),(KP),(LY),(NX),(OS),(TU),(WZ)
ADB	(AX),(BN),(CE),(DM),(FQ),(GV),(HZ),(IK),(JO),(LU),(PR),(SW),(TY)
ADC	(AO),(BL),(CE),(DN),(FQ),(GY),(HI),(JM),(KT),(PS),(RX),(UZ),(VW)
ADD	(AK),(BV),(CN),(DP),(EY),(FT),(GO),(HL),(IU),(JR),(MS),(QW),(XZ)
ADE	(AT),(BM),(CY),(DX),(EQ),(FI),(GZ),(HW),(JU),(KL),(NO),(PS),(RV)

Tabelle 3.1:

Die Substitution, die das erste Produkt in das zweite überführt, muss auch ACA in ACB überführen. Es sind also Paare in diesen beiden Mengen zu suchen, deren Entsprechungen in den Zyklen mit den gleichen Abständen zu finden sind. Im Beispiel sind das die Paare DM bzw. MD und SE (kursiv dargestellt). Aus MD $\mapsto$ SE, genauer M $\mapsto$ S folgt D $\mapsto$ E. Im nächsten Schritt folgen die Zuordnungen Z $\mapsto$ A, sowie L $\mapsto$ Q, Q $\mapsto$ N, X $\mapsto$ R usw. Das Ergebnis ist dann die Substitution

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
C D J E B O Z W M T L Q S P I U N H K G V Y X R F A

in Zyklenform geschrieben:

(F O I M S K L Q N P U V Y)(A C J T G Z)(H W X R)(B D E)

Für die Zuordnung ACB $\mapsto$ ACC erhält man

(E N H L R J K P M O T U X)(B I S F Y Z)(G V W Q)(A C D)

für ACC $\mapsto$ ACD:

(D M G K Q I J O L N S T W)(A H R E X Y)(F U V P)(B C Z)

und für ACD $\mapsto$ ACE

(C L F J P H I N K M R S V)(D W X Z G Q)(E T U O)(A B Y)

Wenn man diese Transformationen günstig geordnet untereinander schreibt, erhält man diejenige Substitution, die jeweils die eine Stufe in die nächste überführt. Das Ergebnis ist:

(Z Y X W V U T S R Q P O N M L K J I H G F E D C B A)

das ist gerade das Alphabet (die Ordnung der Eingangswalze) der ENIGMA I.
Wenn man, beginnend bei `A`, die fortschreitenden Transformationen schreibt, erhält man zunächst die Zeile:

`A C D M R`

Die Zyklenprodukte anders geschrieben, in der Reihung, die zur gemeinsamen Transformation führt (senkrecht angeordnet):
Ausgehend von der ersten Zeile, können die Zeilen in eine Reihenfolge gebracht werden, die die Ordnung der Eingangswalze, das Alphabet, von rechts oben nach links unten erscheinen lässt. Der Vergleich mit Tabelle A1 im Anhang zeigt, dass es sich um die Quadrattafel der Walze I handelt, ab Zeile 5.

A	C	D	M	R	A	A	C	D	M	R
O	I	S	T	U	B	D	E	N	S	V
Z	A	C	Z	G	C	F	O	T	W	X
M	S	F	U	O	D	P	U	X	Y	A
S	K	P	S	J	E	V	Y	Z	B	Y
I	M	O	L	F	F	Z	A	C	Z	G
V	Y	Z	B	Y	G	B	D	A	H	I
W	X	E	X	Z	H	E	B	I	J	P
H	W	Q	I	N	I	C	J	K	Q	D
B	D	A	H	I	J	K	L	R	E	T
E	B	I	J	P	K	M	S	F	U	O
C	J	K	Q	D	L	T	G	V	P	H
L	Q	G	K	M	M	H	W	Q	I	N
D	E	N	S	V	N	X	R	J	O	E
K	L	R	E	T	O	S	K	P	F	J
R	H	L	N	K	P	L	Q	G	K	M
Y	F	Y	A	B	Q	R	H	L	N	K
G	Z	B	C	L	R	I	M	O	L	F
N	P	M	G	Q	S	N	P	M	G	Q
T	G	V	P	H	T	Q	N	H	R	S
F	O	T	W	X	U	O	I	S	T	U
P	U	X	Y	A	V	J	T	U	V	C
J	T	U	V	C	W	U	V	W	D	W
U	V	W	D	W	X	W	X	E	X	Z
Q	N	H	R	S	Y	Y	F	Y	A	B
X	R	J	O	E	Z	G	Z	B	C	L

Tabelle 3.2:

Wenn man nun dieses Verfahren, das bisher bezogen war auf die Eingangsbuchstaben in die Eingangswalze, bezieht auf den Übergang zur mittleren Walze, muss man die Glieder in `AAA`, `ABB`, `ACC` bzw. `ADD` ausdrücken durch die jeweiligen Zeilenbuchstaben aus der letzten Tabelle. So umgesetzt und von oben nach unten geschrieben:

Grundstellung	
<u>AAA</u>	(AU),(BP),(CD),(EX),(FK),(GM),(HI),(JQ),(LS),(NT),(OR),(VW),(YZ)
<u>ABB</u>	(AD),(BJ),(CL),(ER),(FU),(GH),(IP),(KO),(MX),(NV),(QY),(SZ),(TW)
<u>ACC</u>	(AR),(BK),(CZ),(DU),(EM),(FT),(GH),(IQ),(JL),(NY),(OX),(PV),(SW)
<u>ADD</u>	(AB),(CI),(DJ),(EV),(FX),(GR),(HT),(KM),(LW),(NS),(OU),(PY),(QZ)

Um die Weiterbewegung der ersten Walze auszugleichen, müssen diese Glieder noch um 1 bei `AAA`, 2 bei `ABB`, 3 bei `ACC` und 4 bei `ADD` durch Verschiebung längs der „Diagonalen“ (Alphabet) verschoben werden. Damit erhält man

Grundstellung	
AAA	(BV),(CQ),(DE),(FY),(GL),(HN),(IJ),(KR),(MT),(OU),(PS),(WX),(ZA)
ABB	(CF),(DL),(EN),(GT),(HW),(IJ),(KR),(MQ),(OZ),(PX),(SA),(UB),(VY)
ACC	(DU),(EN),(FC),(GX),(HP),(IW),(JK),(LT),(MO),(QB),(RA),(SY),(VZ)
ADD	(EF),(GM),(HN),(IZ),(JB),(KV),(LX),(OQ),(PA),(RW),(SY),(TC),(UD)

Entsprechend dem weiter oben geschilderten Vorgehen wird nun die Transformation gesucht, die das Produkt (AAA)(ABB) in das Produkt (ABB)(ACC) überführt und gleichzeitig auch (ACC) in (ADD).

(AAA)(ABB):	(BV),(YF),(CQ),(M*T*),(G*L*),(DE),(NH),(WX),(PS),(AZ),(OU),(IJ),(KR)
(ABB)(ACC):	(DL),(TG),(XP),(HW),(IJ),(KR),(AS),(YV),(Z*O*),(M*Q*),(BU),(CF),(EN)

Das Glied LT in ACC bietet sich an, überführt in OQ in ADD, denn in (AAA)(ABB) und in (ABB)(ACC) haben die Buchstaben dieser Paare gleiche Abstände (Kursiv). Hier erhält man die gesuchte Transformation zu

(A H L Q V R N D B K E U J F S P X G M Z W T O I C Y)

Das ist aber die Spalte D der Matrix der Walze II, A ab Zeile H.

3.1.2 Polnische Arbeiten bis 1939.

3.1.2.1 Einstieg in das Problem.

Beginnend vereinzelt ab 1926, ab 1928 in voller Breite, hatte der polnische militärische Nachrichtendienst festgestellt, dass die deutschen Funksprüche offenbar mit einem Maschinenschlüssel chiffriert wurden. Einen Hinweis darauf könnte z.B. eine fast vollkommen flache Häufigkeitsverteilung der Buchstaben dargestellt haben. Bei Transpositionen und bei polyalphabetischen Substitutionen mit geringer Periode retten sich Häufigkeiiten, wenn nicht der einzelnen Buchstaben, so doch bei längeren Sprüchen die der Bigramme in die Geheimtexte. Die ersten Ansätze zur Entzifferung (die sogar mit Hilfe des Hellsehers Stefan Ossowiecki versucht worden waren !) wurden bald aufgegeben, wenngleich die Möglichkeit der Verwendung einer ENIGMA–artigen Maschine nicht ausgeschlossen worden war. Die Verwendung eines modifizierten Modells der ENIGMA bei den deutschen Streitkräften wurde den Polen dann auch durch ihren Geheimdienst bestätigt. So kann man mit Sicherheit davon ausgehen, dass ihnen eine kommerzielle Maschine zur Verfügung stand, wobei es über den Erwerb die verschiedensten Versionen in der Literatur gibt.[4] Sie wussten später auch von der Existenz einer Art von Steckerbrett, allerdings reichte das alles nicht zu weiteren Erkenntnissen, sodass die Untersuchungen eingestellt worden waren.

Am 1. 9. 1932 wurden bei der deutschen Sektion der Chiffrierabteilung des polnischen Generalstabes drei junge Mathematiker angestellt (REJEWSKI, RÓŻICKI und ZYGALSKI). Sie sollten an der Lösung des deutschen Marine-Codes arbeiten. Als dieses Ziel weitgehend erreicht war, wurde REJEWSKI Mitte Oktober 1932 allein und unter grösster Geheimhaltung an das ENIGMA - Problem gesetzt. Bis Mitte November standen ihm zur Verfügung:

a) die Gebrauchsanleitung
b) die Schlüsselanleitung
c) eine neue kommerzielle ENIGMA
d) viele aus dem Funkverkehr der deutschen Reichswehr aufgefangenen Sprüche

(Zur Herkunft von a) und b) S. 65)

Bei der Beobachtung der aufgefangenen deutschen Funksprüche des Heeres war aufgefallen, dass offenbar die ersten sechs Buchstaben jedes Spruchs eine besondere Rolle spielten.

[4]BLOCH a), S. 145; GARLINSKI, S. 213; HINSLEY I, App. 1, S. 489; KAHN b), S. 78; KASPAREK, S. 292; LEWIN, S. 30; REJEWSKI b), S. 246; REJEWSKI f), S. 75; WELCHMAN a), S. 83; WINTERBOTHAM, S. 22.

> Die Auffälligkeit bestand darin, dass für alle Sprüche eines Tages galt: Die 1. und 4. Buchstaben, die 2. und 5. , sowie die 3. und 6. bildeten jeweils charakteristische Paare.

Ausserdem: Wenn zwei Funksprüche mit gleichen sechs Buchstaben als Anfang untereinander geschrieben werden, kamen gleiche Buchstaben untereinander zweimal so oft vor wie bei Sprüchen mit Unterschieden in den Anfängen.[5] REJEWSKI fand als Erklärung hierfür. dass die Funksprüche mit gleichem Tagesschlüssel chiffriert waren.

1. AUQ AMN	14. IND JHU	27. PVJ FEG	40. SJM SPO	53. WTM RAO
2. BNH CHL	15. JWF MIC	28. QGA LYB	41. SJM SPO	54. WTM RAO
3. BCT CGJ	16. JWF MIC	29. QGA LYB	42. SJM SPO	55. WTM RAO
4. CIK BZT	17. KHB XJV	30. RJL WPX	43. SUG SMF	56. WKI RKK
5. DDB VDV	18. KHB XJV	31. RJL WPX	44. SUG SMF	57. XRS GNM
6. EJP IPS	19. LDR HDE	32. RJL WPX	45. TMN EBY	58. XRS GNM
7. FBR KLE	20. LDR HDE	33. RJL WPX	46. TMN EBY	59. XOI GUK
8. GPB ZSV	21. MAW UXP	34. RFC WQQ	47. TAA EXB	60. XYW GCP
9. HNO THD	22. MAW UXP	35. SYX SCW	48. USE NWH	61. YPC OSQ
10.HNO THD	23. NXD QTU	36. SYX SCW	49. VII PZK	62. YPC OSQ
11.HXV TTI	24. NXD QTU	37. SYX SCW	50. VII PZK	63. ZZY YRA
12.IKG JKF	25. NLU QFZ	38. SYX SCW	51. VQZ PVR	64. ZEF YOC
13.IKG JKF	26. OBU DLZ	39. SYX SCW	52. VQZ PVR	65. ZSJ YWG

Tabelle 3.3: Indikatoren

3.1.2.1.1 Indikator. Als Grundlage für die weitere Arbeit waren die Abweichungen der militärischen ENIGMA von der kommerziellen Version bekannt, ebenso die Tatsache, dass am Anfang jedes Spruches der verdoppelte Spruchschlüssel, chiffriert mit dem Tagesschlüssel, zu finden war. Die 1. und 4. Buchstaben waren also die Chiffrate ein und desselben Klarbuchstabens – des ersten Buchstabens des Spruchschlüssels – , entsprechendes galt für die Buchstabenpaare 2.-5. und 3.-6. Diese Gruppe der ersten sechs Buchstaben wurde Indikator genannt.

Hier setzte nun die Arbeit von REJEWSKI ein. Bei ungefähr 80 Sprüchen eines Tages konnte man erwarten, dass alle Buchstaben auf allen Plätzen 1 bis 6 der Indikatoren auftraten. Auf jedem Platz sind sie das Resultat einer Permutation des Alphabets , d.h. einer eineindeutigen Abbildung des Alphabets auf sich. Diese Permutationen bezeichnete REJEWSKI mit den Buchstaben A bis F. Sie waren natürlich zunächst unbekannt. Die Übergänge vom 1. Geheimbuchstaben zum 4. , vom 2. zum 5. und vom 3. zum 6. bilden ebenfalls Permutationen, und zwar die Produkte AD , BE und CF.

> Angenommen, an der Stelle 1 werde der Klarbuchstabe `X` eingetastet, und als Geheimtext ergebe sich der Buchstabe `t`. Dann gilt auch das Umgekehrte: Zum Klarbuchstaben `T` an der Stelle 1 gehört der Geheimtext `x`. Beim Eintippen des Buchstaben `X` an der Stelle 4 ergebe sich der Buchstabe `m`. D.h. `t` an der Stelle 1 würde auf `x` und `X` an der Stelle 4 auf `m` abgebildet werden: Die Abbildung $\mathtt{T} \mapsto \mathtt{m}$ ist demnach das Produkt der beiden Einzelabbildungen A und D.

Die Produkte AD , BE und CF konnten als Produkte von disjunkten Zyklen dargestellt werden, die charakteristische Längen aufwiesen. Da sie, abhängig von der Einstellung der Chiffriermaschine i.a. von Tag zu Tag verschieden ausfielen, wurde der Satz der drei Zyklenprodukte die Tagescharakteristik genannt. In Tabelle 3.3 sind die in der Literatur als Beispiel angegebenen Indikatoren

[5] KOZACZUK -deutsch, S. 39

geordnet aufgelistet und hierunter durch die zugehörige Tagescharakteristik ergänzt. (Dabei war zu berücksichtigen, dass in den Veröffentlichungen sinnwidrige Druckfehler zu finden waren[6]; diese sind hier korrigiert.)

Tagescharakteristik zu Tabelle 3.3

```
AD = (A)(S)(BC)(RW)(DVPFKXGZYO)(IJMUNQLHTE)
BE = (D)(K)(AXT)(YGC)(BLFQVEOUM)(JPSWIZRNH)
CF = (ABVIKTJGFCQNY)(WPSMODUZREHLX)
```

Zur Herleitung: `(A)` aus Indikator 1; `(S)` aus Nr. 35 bis 44; `(BC)` aus Nr. 2 u. 3 usw.
Das von REJEWSKI zur Erläuterung seines Verfahrens angegebene Material kann nicht original sein, denn das Originalmaterial ging beim Zusammenbruch Polens im Herbst 1939 verloren.

Die Schlussfolgerungen aus dem Material, wie sie im folgenden dargestellt werden, lassen zunächst unberücksichtigt, dass jeweils sechs Buchstabenpaare durch Stecker verändert waren. Aus der Fülle der vorliegenden Sprüche jedes Tages liess sich jedoch ein System von Indikatoren, wie dem der Tabelle 3.3, konstruieren.
In dieser Situation bestand das Problem, aus den Produkten AD , BE und CF die einzelnen Permutationen A bis F selbst zu gewinnen. In den Produkten traten Zyklen gleicher Länge jeweils paarweise auf. Das liegt an dem Satz:[7]

> Wenn zwei Permutationen X und Y vom selben Grad ausschliesslich ein Produkt von Zweierzyklen (disjunkten Transpositionen) sind, dann besteht ihr Produkt XY aus disjunkten Zyklen gleicher Länge in jeweils gerader Anzahl. [8]

Beweis:

> Der Grad der Zyklen sei 2n. Wenn in X ebenso wie in Y eine Transposition (ab) existiert, dann enthält das Produkt XY die Zyklen (a) und (b). Für diesen Fall gilt der Satz also. Ohne Einschränkung der Allgemeinheit gelte nun
> Es treten auf

in der Permutation X	in der Permutation Y
(a_1a_2)	(a_2a_3)
(a_3a_4)	(a_4a_5)
$\dots$	$\dots$
$(a_{2k-3}a_{2k-2})$	$(a_{2k-2}a_{2k-1})$
$(a_{2k-1}a_{2k})$	$(a_{2k}a_1)$

mit $k \leq n$.

Nun multipliziert:

$$XY = (a_1a_3a_5 \dots a_{2k-3}a_{2k-1})(a_{2k}a_{2k-2} \dots a_4a_2).$$

Daraus folgt:

> Buchstaben, die zu ein und demselben Zweierzyklus der Permutation X oder Y gehören, finden sich immer in zwei verschiedenen Zyklen gleicher Länge des Produktes XY.

Weiter:

[6] GARLINSKI (App.), S. 199/200; LISICKI, S. 72-74; WELCHMAN a), S.85
[7] BIRKHOFF, SAUNDERS, MC LANE, A Survey of Modern Algebra, NesYork, 1965.
[8] Unter Grad ist die Anzahl der in den Permutationen vorhandenen voneinander verschiedener Elemente zu verstehen - im Falle der ENIGMA 26 (Buchstaben)

> Wenn zwei Buchstaben, die sich in verschiedenen Zyklen gleicher Länge des Produktes XY befinden, zur selben Transposition der Permutation X oder Y gehören, dann gehören auch die ihnen in XY benachbarten Buchstaben (einer rechts, der andere links) zu ein und derselben Transposition.

Im Folgenden erweist sich die Umkehrung als besonders wichtig:

> Wenn in einer Permutation von geradem Grade verschiedene Zyklen gleicher Länge paarweise auftreten, dann kann die Permutation als Produkt zweier Permutationen aufgefasst werden, die jede nur aus disjunkten Transpositionen besteht.

Hinweise zu den Beweisen der Sätze bei REJEWSKI.[9]

Im folgenden soll von der Voraussetzung ausgegangen werden, dass sich nur die erste Walze bewegt, die Mitnahme der zweiten Walze also nicht stattfindet. Diese Voraussetzung ist in rd. 81 % (21/26) der Fälle erfüllt. Die Permutation durch das Steckerbrett sei mit S bezeichnet, diejenigen durch die drei Walzen mit (beginnend bei der der Eingangswalze benachbarten) mit R_1, R_2 und R_3, schliesslich die der Umkehrwalze mit K. Die Eingangswalze bleibt unberücksichtigt, weil ihre 'Permutation' die identische Abbildung darstellt. Die Permutation

$$P = \begin{pmatrix} \mathsf{a\ b\ c\ d\ e\ f\ g\ h\ i\ j\ k\ l\ m\ n\ o\ p\ q\ r\ s\ t\ u\ v\ w\ x\ y\ z} \\ \mathsf{a\ b\ c\ d\ e\ f\ g\ h\ i\ j\ k\ l\ m\ n\ o\ p\ q\ r\ s\ t\ u\ v\ w\ x\ y\ z} \end{pmatrix}$$

lässt diesen Sachverhalt darstellen. (Die Veränderung der Eingangswalze von der der kommerziellen ENIGMA zu der der militärischen ENIGMA hat REJEWSKI lange genarrt, bis er zufällig den Einfall hatte, hier könne einfach die identische Abbildung vorliegen. KNOX, der die Deutschen überschätzte, konnte sich dies bis 1939 nicht vorstellen.)[10] Weiter muss berücksichtigt werden, dass die erste Walze R_1 vor Stromfluss um 1/26 ihres Umfangs weiterbewegt wird.

Nun liessen sich die einzelnen Chiffrierungs-Permutationen aufschreiben:

$$\begin{array}{rcl} A & = & SPR_1P^{-1}R_2R_3KR_3^{-1}R_2^{-1}PR_1^{-1}P^{-1}S^{-1} \\ B & = & SP^2R_1P^{-2}R_2R_3KR_3^{-1}R_2^{-1}P^2R_1^{-1}P^{-2}S^{-1} \\ C & = & SP^3R_1P^{-3}R_2R_3KR_3^{-1}R_2^{-1}P^3R_1^{-1}P^{-3}S^{-1} \\ D & = & SP^4R_1P^{-4}R_2R_3KR_3^{-1}R_2^{-1}P^4R_1^{-1}P^{-4}S^{-1} \\ E & = & SP^5R_1P^{-5}R_2R_3KR_3^{-1}R_2^{-1}P^5R_1^{-1}P^{-5}S^{-1} \\ F & = & SP^6R_1P^{-6}R_2R_3KR_3^{-1}R_2^{-1}P^6R_1^{-1}P^{-6}S^{-1} \end{array}$$

Damit ergaben sich die bekannten Produkte AD bis CF zu:

$$\begin{array}{rcl} AD & = & SPR_1P^{-1}R_2R_3KR_3^{-1}R_2^{-1}PR_1^{-1}P^3R_1P^{-4}R_2R_3KR_3^{-1}R_2^{-1}P^4R_1^{-1}P^{-4}S^{-1} \\ BE & = & SP^2R_1P^{-2}R_2R_3KR_3^{-1}R_2^{-1}P^2R_1^{-1}P^3R_1P^{-5}R_2R_3KR_3^{-1}R_2^{-1}P^5R_1^{-1}P^{-5}S^{-1} \\ CF & = & SP^3R_1P^{-3}R_2R_3KR_3^{-1}R_2^{-1}P^3R_1^{-1}P^3R_1P^{-6}R_2R_3KR_3^{-1}R_2^{-1}P^6R_1^{-1}P^{-6}S^{-1} \end{array}$$

In diesem zu lösenden System waren die linken Seiten bekannt, sowie die Permutation P mit ihren Potenzen auf den rechten Seiten. Alle anderen Permutationen (S, R_1, R_2, R_3 und K) waren unbekannt, weshalb das System in dieser Form kaum lösbar sein dürfte. Die oben erwähnte Voraussetzung, dass sich nur der erste Rotor bewegen sollte, ermöglichte allerdings eine Vereinfachung. Für das Produkt

[9] REJEWSKI b), d), e)

[10] BLOCH a), S.150; KAHN b), S. 85; REJEWSKI a), S. 221; REJEWSKI b), S. 256; WELCHMAN a), S.86.

$$Q = R_2 R_3 K R_3^{-1} R_2^{-1}$$

wird die Abkürzung Q eingeführt, wobei Q als eine Art von modifizierter Umkehrwalze gedeutet werden kann. Damit ergab sich ein System:

$$\begin{aligned} AD &= SPR_1P^{-1}QPR_1^{-1}P^3R_1P^{-4}QP^4R_1^{-1}P^{-4}S^{-1} \\ BE &= SP^2R_1P^{-2}QP^2R_1^{-1}P^3R_1P^{-5}QP^5R_1^{-1}P^{-5}S^{-1} \\ CF &= SP^3R_1P^{-3}QP^3R_1^{-1}P^3R_1P^{-6}QP^6R_1^{-1}P^{-6}S^{-1} \end{aligned}$$

Mit Hilfe der oben genannten Sätze konnte man nun versuchen, Lösungen zu finden; wegen der Grösse der Lösungsmannigfaltigkeit war aber das Herausfiltern der einzigen richtigen Lösung für das Dechiffrierungsproblem zunächst zu schwierig. REJEWSKI war aufgefallen, dass in der Menge der Indikatoren der jeweils an einem Tage aufgefangenen Sprüche verschiedentlich Häufungen auftraten, und zwar die gleichen bei verschiedenen Absendern. Er schloss daraus, dass es gewisse Buchstabentrigramme geben müsste, die als Spruchschlüssel bevorzugt verwendet worden waren.
Zunächst bemerkte REJEWSKI am Beispiel der Tages-Charakteristik zu Tabelle 3.3, dass wegen der Zyklen `(a)` `(s)` in AD und der Eigenschaft der Reziprozität der Klarbuchstabe a an den Stellen 1 und 4 in den Geheimbuchstaben `S` umgewandelt wurde und umgekehrt. Sowohl A als auch D mussten also den Zweierzyklus `(a s)` enthalten. Der Spruchschlüssel zu den Indikatoren 35 - 39 musste also mit `a` beginnen.

A	($\underline{a}$)
	($\underline{s}$)
D	($\underline{a}$)
	($\underline{s}$)

Die Häufigkeit des Indikators `SYX SCW` liess REJEWSKI vermuten, dass der Spruchschlüssel aaa oder abc lauten könnte. Letztere Möglichkeit scheidet aus, weil die evtl. zugeordneten Buchstaben `Y` und `C` nicht in einem Zyklus gleicher Länge liegen wie der, in dem sich b befindet. Bei der Vermutung aaa ergeben sich keine Widersprüche (Unterstrichene Buchstaben).

A	($\underline{a}$)	(*b* c)		(d v p f k x g z y o)
	($\underline{s}$)	(*r* w)		(i e t h l q n u m j)
D	($\underline{a}$)	(*b* c)		(d v p f k x g z y o)
	($\underline{s}$)	(*w* r)		(j i e t h l q n u m)
B	(d)		($\underline{a}$ x t)	(*b* l f q v e o u m)
	(k)		($\underline{y}$ g c)	(*j* h n r z i w s p)
E	(d)		($\underline{a}$ x t)	(*b* l f q v e o u m)
	(k)		($\underline{c}$ y g)	(*p* j h n r z i w s)
C				($\underline{a}$ *b* v i k t j g f c q n y)
				($\underline{x}$ *l* h e r z u d o m s p w)
F				($\underline{a}$ *b* v i k t j g f c q n y)
				($\underline{w}$ x l h e r z u d o m s p)

Im Schema sind die Zyklen der Tagescharakteristik von Tabelle 3.3 auf Grund der Sätze weiter oben so angeordnet, dass übereinander Beziehungen wie Klarbuchstabe $\Longleftrightarrow$ Geheimbuchstabe bestehen.
Der ebenfalls sehr häufige Indikator `RJL WPX` - auch durch Vergleich mit der Lage der Buchstaben a, `X` und `W` in den Zyklen von CF - zur weiteren widerspruchsfreien Deutung

bbb (Kursive Buchstaben). liessen sich einfacher darstellen, wenn man einen der beiden zusammengehörigen Zyklen, wie im Schema, umgekehrt schrieb. Wegen der schon ablesbaren Zuordnung W und R $\mapsto$ c war die Vermutung berechtigt, die Indikatoren 53 - 55 seien die Chiffrierungen von ccc . Dabei muss in BE nach oben gelesen werden, wobei diesmal die Geheimbuchstaben in der ersten Zeile abgelesen werden. Dabei ergab sich sofort 40 - 42 zu abc . Dieses Verfahren des Anschreibens und Lesens der Zyklen ist im Grunde nichts anderes als die Anwendung der obigen Sätze über Permutationen. Daraus konnten sämtliche Spruchschlüssel des Beispiels von Tabelle 3.3 abgelesen werden (Tabelle 3.4)

1. sss	14. dfg	27. tzu	40. abc	53. ccc
2. rfv	15. ooo	28. xxx	41. abc	54. ccc
3. rtz	16. ooo	29. xxx	42. abc	55. ccc
4. wer	17. lll	30. bbb	43. asd	56. cde
5. ikl	18. lll	31. bbb	44. asd	57. qqq
6. vbn	19. kkk	32. bbb	45. ppp	58. qqq
7. hjk	20. kkk	33. bbb	46. ppp	59. qwe
8. nml	21. yyy	34. bnm	47. pyx	60. qay
9. fff	22. yyy	35. aaa	48. zui	61. mmm
10. fff	23. ggg	36. aaa	49. eee	62. mmm
11. fgh	24. ggg	37. aaa	50. eee	63. uvw
12. ddd	25. ghj	38. aaa	51. ert	64. uio
13. ddd	26. jjj	39. aaa	52. ert	65. uuu

Tabelle 3.4: Spruchschlüssel

Es zeigte sich schon hier, dass auch die Folge benachbarter Tasten auf der Schreibmaschine zu den bevorzugten Spruchschlüsseln gehörte, was sich auch noch viele Jahre später auswirken sollte.
Es war nun möglich, die Permutationen A $\cdots$ F geschlossen aufzulisten:

A = (AS)(BR)(CW)(DI)(EV)(FH)(GN)(JO)(KL)(MY)(PT)(QX)(UZ)
B = (AY)(BJ)(CT)(DK)(EI)(FN)(GX)(HL)(MP)(OW)(QR)(SU)(VZ)
C = (AX)(BL)(CM)(DG)(EI)(FO)(HV)(JU)(KR)(NP)(QS)(TZ)(WY)
D = (AS)(BW)(CR)(DJ)(EP)(FT)(GQ)(HK)(IV)(LX)(MO)(NZ)(UY)
E = (AC)(BP)(DK)(EZ)(FH)(GT)(IO)(JL)(MS)(NQ)(RV)(UW)(XY)
F = (AW)(BX)(CO)(DF)(EK)(GU)(HI)(JZ)(LV)(MQ)(NS)(PY)(RT)

Diese Auflistung war auch zu erhalten,wenn man die Zyklen der Tagescharakteristik, auf grund von Vermutungen der Vorlieben der Chiffrierer oder ihrer Unarten bzgl. der Wahl von Textschlüsseln, geeignet untereinander schreiben konnte. Im Beispiel:

a x t
$\downarrow\nearrow\downarrow\nearrow\downarrow$
y g c

für die Permutationen B ($\downarrow$) und E ($\nearrow$).
Entsprechendes gilt für die übrigen paarigen Zyklen der Tagescharakteristik.

GAJ[11] zeigt ebenfalls, wie durch Versuch und Irrtum die Hypothesen bzgl. angenommener Klarbuchstaben unter ständiger Kontrolle mit Hilfe der Sätze über Permutationen,

[11] GAJ, S. 86 - 92.

angewandt auf die Tagescharakteristik, durchgemustert werden konnten, bis entweder Eindeutigkeit erreicht oder die Zahl der möglichen Varianten handhabbar klein geworden war.
Aus Gründen, die zwar in der Literatur nicht genannt werden, die aber später erkennbar werden, wird dieses Beispiel hier abgebrochen.
In Tabelle 3.5 sind 100 mit der angegebenen ENIGMA-Einstellung zufällig erzeugte Indikatoren aufgelistet. Das Arbeitsblatt zeigt die Auswertung dieser Indikatoren.

ENIGMA SIMULATION
Eingangswalze: II; Mittelwalze: I; Endwalze: Nr. III; Umkehrwalze: `B`
Ringstellung : `V, I, M` ; Grundstellung : `J, W, S`
Steckverbindungen: `(EZ) (PR) (XT) (YV) (GL) (AS)`
100 Indikatoren

AAXNSR	AFONGE	AIBNXQ	AKFNEV	AKVNEC	AMGNTK
BGQGQN	BMEGTZ	BXJGCS	CBLVNP	CFTVGG	CUYVAL
DBYSNL	DLQSIN	DURSAD	ECDIOU	EOPIRJ	ERHIPI
FHKTZO	FMDTTU	GFWLGF	GGTLQG	GGTLQG	GPKLHO
GQKLBO	GUQLAN	HHZDZM	HMBDTQ	HQDDBU	HTPDJJ
HVRDFD	IEGJWK	IJBJYQ	IOFJRV	IVTJFG	IZWJMF
JFJOGS	JHWOZF	JHYOZL	JMSOTX	JMSOTX	JTGOJK
KDXWUR	KJXWYR	KJXWYR	KLUWIW	KXWWCF	KYUWLW
LNIQDA	LRQQPN	LRQQPN	LRQQPN	LXEQCZ	NAQCSN
NASCSX	NMNCTH	NQHCBI	OBPXNJ	ORMXPB	OWBXVQ
OZBXMQ	OZGXMK	PTREJD	QFDZGU	QGUZQW	QIGZXK
QLOZIE	RPRRHD	RYARLT	SFXHGR	SLOHIE	SOCHRY
SVMHFB	TMOUTE	TSNUKH	TSPUKJ	TZBUMQ	UPRFHD
UUJFAS	UUJFAS	VCWBOF	VCWBOF	VCWBOF	VKXBER
VSYBKL	WFAYGT	WFAYGT	WTLYJP	XAQKSN	XVGKFK
YFTPGG	YHKPZO	YUAPAT	YYCPLY	YYCPLY	ZFDAGU
ZFDAGU	ZGUAQW	ZUMAAB	ZZJAMS		

Tabelle 3.5: Indikatoren

Die Permutationszyklen lauten:

```
AD (VBGLQZANC)(EIJOXKWYP)(DSH)(TUF)(M)(R)
BE (WVFGQBNDUASKE)(RPHZMTJYLIXCO)
CF (XRDUWFVCYLPJS)(NHIATGKOEZMBQ)
```

Arbeitsblatt

Auffällig ist das mehrfache Auftreten der Indikatoren
`LRQQPN, VCWBOF` (je 3mal),
`GGTLQG, JMSOTX, KJXWYR, UUJFAS, WFAYGT, YYCPLY, ZFDAGU` (je 2mal)
Zusammen mit der Vorerfahrung über Gewohnheiten einzelner Funker könnte angenommen werden, dass `LRQQPN` oder `VWCBOF` zum Textschlüssel eee gehören. (`aaa, bbb, ccc` scheiden aus, weil diese Buchstaben mit `L` bzw. `V` in einem Zyklus stehen.) Wegen des Ausschlusses von `Q, N` für `e` in Stufe 3 - 6 bleibt vorläufig als Annahme die Zuordnung `VCWBOF` $\mapsto$ `eee`.

AD	:	(r)	(dsh)	(vbglqzanc)
		(m)	(tfu)	(epywkxoji)
BE	:			(wvfgqbnduaske)
				(xilyjtmzhproc)
CF	:			(xrduwfvcylpjs)
				(qbmzeokgtaihn)

Die Zyklen dahingehend geordnet geschrieben führt zu den Folgerungen:

1) `LRQQPN` $\mapsto$ `wsx` (Plausible Tastenfolge)
2) `GGTLQG` $\mapsto$ `yyy` (Plausibel)
3) `JMSOTX` $\mapsto$ `nnn` (Plausibel)
4) `KJXWYR` $\mapsto$ `qqq` (Plausibel)
5) `UUJFAS` $\mapsto$ `?hh` (Mit der plausiblen Annahme, dass der Textschlüssel `hhh` lautet, ist auch die Zuordnung in 1 - 4 eindeutig.)
6) `WFAYGT` $\mapsto$ `lll` (Plausibel)
7) `YYCPLY` $\mapsto$ `ggg` (Plausibel)
8) `ZFDAGU` $\mapsto$ `xlm`

Insgesamt erscheinen diese Zuordnungen überzeugend, sodass mit ihnen weiter gearbeitet werden kann.

Durch genaue Beobachtung und einfühlsame Vermutung gelang es REJEWSKI also — allein aus den Tagescharakteristiken heraus — , für viele Tage die Spruchschlüssel zu ermitteln. Zwar schien er damit dem Ziel, die Sprüche selbst zu lesen, noch nicht nähergekommen zu sein, aber er hatte nun Klartext/Geheimtext-Paare, wenn auch nur jeweils sechs Buchstaben lang. In den Chiffrierungsgleichungen waren somit für viele einzelne Tage auf den linken Seiten die Permutationen A bis F bekannt. Dies waren schon erhebliche Fortschritte, jedoch ein weiterer Schluss auf die Verdrahtung der Walzen war noch nicht möglich. Die Verwendung dreifacher gleicher Buchstaben als Spruchschlüssel wurde zwar in der Folge verboten, aber dieses Verbot kam zu spät.[12]

An dieser Stelle erhielt REJEWSKI Hilfe:

3.1.2.1.2 H.-T. SCHMIDT. Dem französischen Geheimdienst war von einem Bediensteten der Chiffrierstelle des Reichswehrministeriums, Hans - Thilo SCHMIDT, Material über die ENIGMA übergeben worden. Die Zeitangaben und verschiedene Einzelheiten über diese Vorgänge differieren in den einzelnen Veröffentlichungen, die ausschliesslich auf Erinnerungen beruhen. (Die französischen Akten dazu bleiben - soweit sie nicht im Kriege verlorengegangen sind - für 60 Jahre unter Verschluss.) Hier soll der zeitliche Ablauf in Anlehnung an BLOCH[13] beschrieben werden, der die verschiedenen Quellen am sorgfältigsten auf ihre Plausibilität hin überprüft hat. ASCHÉ, wie der Deckname von H. - T. SCHMIDT lautete, bot den Franzosen erstmals im Oktober 1931 Geheimmaterial an, das ihnen dann am 8.11.1931 zum Abfotografieren vorgelegt wurde.

Die Franzosen selbst wussten mit dem Material nicht viel anzufangen, gaben es aber an befreundete Dienste (Briten, Polen) weiter. Erstere hefteten es sorgfältig ab. Zwischen dem 7. und dem 11. Dezember 1931 übergab BERTRAND das Material dem Chef des polnischen Chiffrierbüros, Major LANGER. Daraufhin wurde in Polen die Arbeit am Problem ENIGMA wieder aufgenommen.

BERTRAND übergab dem polnischen Chiffrierbüro im Mai 1932 weiteres Material, das er von ASCHÉ erhalten hatte, am 17. September Schlüsseltafeln mit den Tagesschlüsseln für September und Oktober 1932, sowie ein vollständiges Chiffrierungsbeispiel.[14]

Mitte November 1932 erhielt REJEWSKI (er meint allerdings, es hätte sich um den 9. oder 10. Dezember 1932 gehandelt) von seinem Vorgesetzten, Major CIEZKI, zwei weitere Unterlagen, nämlich vollständige Schlüsseltafeln mit allen Tagesschlüsseln für die Monate September 1932 und Oktober 1932 (also zweier Monate aus verschiedenen Quartalen), allerdings nicht das Chiffrierungsbeispiel aus Klartext und Geheimtext[15]

[12] DEAVOURS/KRUH a), S. 109/110; GARLINSKI, S. 201; KOZACZUK, S. 42/43; REJEWSKI a), S. 241; REJEWSKI b), S. 253; REJEWSKI e), S. 218; WELCHMAN a), S. 87; WOYTAK, S. 56.

[13] BLOCH a)

[14] PAILLOLE, S. 57 und SEBAG-MONTEFIORE, S. 294

[15] KOZACZUK, engl. , Bemerkung 9, S. 23

Er wurde nicht darüber informiert, dass es sich um Material handelte, das BERTRAND am 17.9.1932 in Warschau übergeben hatte. Damit gelang ihm bis Jahresende 1932 die vollständige Rekonstruktion der ENIGMA auf dem Papier. Das Material war entscheidend für den weiteren Erfolg von REJEWSKI (und nicht nur förderlich, wie verschiedentlich behauptet wurde).[16] Das Material enthielt allerdings keine Angaben zur inneren Verdrahtung der Walzen.

Nach den vorliegenden Berichten lieferte ASCHÉ bis 1934 weitere Geheimunterlagen an BERTRAND, u.a. auch solche über die ENIGMA. BERTRAND leitete sie auch an LANGER weiter, der sie jedoch REJEWSKI nicht zugänglich machte. REJEWSKI bekam nicht einmal zu erfahren, dass die ihm 1932 übergebenen Unterlagen vom französischen Geheimdienst stammten. GOUAZÉ[17] schreibt von insgesamt 303 Chiffrierdokumenten, die von ASCHÉ an BERTRAND übergeben worden seien, dabei wären aber nur wenige gewesen, die sich auf die ENIGMA bezogen hätten. Da die französischen Archive erst weit nach dem Jahr 2000 geöffnet werden, handelt es sich nur um Vermutungen auf Grund vager persönlicher Erinnerungen der damals Beteiligten. REJEWSKI widerspricht sich selbst, ob er ausser Gebrauchsanleitung, Chiffrieranleitung und zwei Schlüsseltafeln (Sept./Okt. 1932) weitere Dokumente erhalten hätte, insbesondere Beispiele mit Klartext/Geheimtext.[18] Sie hätten ihm sowieso keinen Nutzen gebracht. Er gab zwar Dezember 1932 als Übergabetermin für die Schlüsseltafeln an[19], das dürfte aber nicht ganz stimmen, da dann die Zeit zur endgültigen Rekonstruktion der Maschine zu kurz gewesen sein dürfte. Die Möglichkeit der Ermittlung der Spruchschlüssel (Tabelle 3.4) ohne jede Kenntnis von Steckerstellung, Ringstellung oder Grundstellung offenbart eine erhebliche Schwäche des Systems der Chiffrierung des verdoppelten Spruchschlüssels und zeigt ausserdem die verheerende Wirkung von leichtfertig ausgewählten Schlüsseln (offenbar eine Folge von mangelhafter Ausbildung des damit befassten Chiffrierpersonals).

3.1.2.2 Walzenverdrahtung.

3.1.2.2.1 Schlüsseltafeln. Mit den Schlüsseltafeln war für die Monate September und Oktober 1932 auch für jeden Tag die Steckerstellung bekannt. Daher konnte im Gleichungssystem A bis F die Permutation S auf die linke Seite übertragen werden. Für die Entwicklung eines Produktes $L = M^{-1}NM$ ist es nur nötig, auf die Elemente von N die durch die Permutation M vorgegebenen Ersetzungen vorzunehmen.
Die Regel dazu: Falls N gesucht ist, ergibt die Gleichung nur Lösungen, wenn L und N konjugiert sind; d.h. dieselbe Zyklenstruktur aufweisen. Die Lösungsanzahl ist dann gleich der Anzahl der Möglichkeiten, L unter N zu schreiben, ohne L zu ändern.
Da beim hier vorliegenden Problem die Permutationen A bis F aus je 13 Zweierzyklen bestanden, war die Lösungsmannigfaltigkeit zu gross, als dass das Problem auf direktem Wege hätte angegangen werden können. REJEWSKI transformierte die Gleichungen von Seite 59 zunächst mit wachsenden Potenzen von P.

$$\begin{aligned}
U &= P^{-1}S^{-1}ASP \\
V &= P^{-2}S^{-1}BSP^2 \\
W &= P^{-3}S^{-1}CSP^3 \\
&\dots \\
Z &= P^{-6}S^{-1}FSP^6
\end{aligned}$$

[16] BLOCH a), S. 143, S. 151
[17] GOUAZE, S. 90.
[18] REJEWSKI gibt in a), S. 109/110 an, dass die den Schlüsseltafeln für September und Oktober 1932 beiliegenden Klartext/Geheimtext - Beispiele seine Arbeit erleichtert hätten. In REJEWSKI f), S. 77 leugnet er, solche Beispiele erhalten zu haben. Es gibt in den Daten zu seiner Arbeit in den verschiedenen Veröffentlichungen weitere Unstimmigkeiten (Erinnerungslücken).
[19] REJEWSKI c), S. 279; WOYTAK, S. 54

Mit $Q = R_2R_3KR_3^{-1}R_2^{-1}$ (vgl. S. 62) erhielt er

$$\begin{array}{rcl} U & = & R_1P^{-1}QPR_1{}^{-1} \\ V & = & R_1P^{-2}QP^2R_1{}^{-1} \\ W & = & R_1P^{-3}QP^3R_1{}^{-1} \\ & \cdots & \\ Z & = & R_1P^{-6}QP^6R_1{}^{-1} \end{array}$$

Dann multiplizierte er jeweils zwei aufeinander folgende Zeilen miteinander:

$$\begin{array}{rcl} UV & = & R_1P^{-1}(QP^{-1}QP)PR_1{}^{-1} \\ VW & = & R_1P^{-2}(QP^{-1}QP)P^2R_1{}^{-1} \\ & \cdots & \\ YZ & = & R_1P^{-5}(QP^{-1}QP)P^5R_1{}^{-1} \end{array}$$

oder, aufgelöst nach der Klammer und eingesetzt:

$$\begin{array}{rcl} VW & = & R_1P^{-1}R_1{}^{-1}(UV)R_1PR_1{}^{-1} \\ & \cdots & \\ YZ & = & R_1P^{-1}R_1{}^{-1}(XY)R_1PR_1{}^{-1} \end{array}$$

Diese Ausdrücke mussten alle die gleiche Form (bzgl. ihrer Zyklen) aufweisen. Wenn nicht, lag — abgesehen von evtl. Rechenfehlern — der Fall vor, dass sich entweder, entgegen der Annahme, nicht nur die erste Walze bewegt hatte, oder dass Stecker das Ergebnis verfälschen.

Im Beispiel (S.64 oben) sorgten in der Tat die nicht berücksichtigten Stecker für den Abbruch. Wenn man es fortführen wollte bis zur Ermittlung der UV bis WX, erhielte man

$$\begin{array}{rcl} UV & = & \mathtt{(AENIKHRQWMDBS)(CTXLFUYOPGZJV)} \\ VW & = & \mathtt{(AWNGYSVOIBMPL)(CDHFXZRETQKJU)} \\ WX & = & \mathtt{(ARTGXZP)(BMJVIDF)(CELNK)(HOWYU)(Q)(S)} \end{array}$$

Die Zyklenstruktur zeigt keine Übereinstimmung.
REJEWSKI führt aber selbst ein Beispiel an, beginnend mit der Tagescharakeristik, ohne jedoch zu schreiben, dass es das abgebrochene Beispiel ist, nachdem die Stecker herausgerechnet wurden. KOZACZUK erwähnt die Stecker.[20]
Dieses führt zu

$$\begin{array}{rcl} UV & = & \mathtt{(AEPFTYBSNIKOD)(RHCGZMUVQWLJX)} \\ VW & = & \mathtt{(AKJCEVZYDLWNU)(SMTFHQIBXOPQR)} \\ WX & = & \mathtt{(AQVLOIKGNWBMC)(PUZFTJRYEHXDS)} \end{array}$$

[20] Die Stecker waren hier: (AP)(BL)(CZ)(FH)(JK)(QU), nach HAMER et al. S. 219

Weitere Untersuchung führt im Vorgriff auf das Verfahren von S. 69 zu

$$H = R_1 P R_1^{-1} = \texttt{AYURICXQMGOVSKEDZPLFWTNJHB}$$

Ein Vergleich mit den Klassentabellen der Zyklen bei TURING zeigt, dass es sich um die Walze II einer von TURING untersuchten ENIGMA K handelt.[21]

In den Tabellen 3.6 bis 3.9 sind im oberen Teil weitere Beispiele für die Tagescharakteristiken, bereits geordnet geschrieben, dargestellt. Sie sind durch Simulation fiktiver (zufälliger) Spruchschlüssel entstanden. Dabei ist allerdings auf die Auflistung der Klartext/Geheimtext-Paare verzichtet worden. Sie zeigen die Entwicklung für verschiedene Tagescharakteristiken eines Monats, also — noch vermutlich — gleicher Walzenlage. Zur Vereinfachung sind für die folgende Rechnung die Steckerstellungen herausgerechnet und die Ringstellungen auf AAA reduziert. Die Angabe der Anfangsstellungen in den Tabellen 3.6 bis 3.9 dient hier nur zur Orientierung des Lesers und Zuordnung der Anlagen zueinander.

Walzenlage: 321 , Ringstellung: AAA , Grundstellung: AAA

AD		AKPLXJQTOEWGH
AD		FNCISRUZDVBYM
AD		MFNCISRUZDVBY
BE		ALZQSUNYDFPKX
BE		TOVIRBWCMEHJG
BE		GTOVIRBWCMEHJ
CF	Q	DVGKZILPWRUT
CF	O	SCMYAJNBHFXE
CF	O	ESCMYAJNBHFX

A: (AF)(KN)(PC)(LI)(XS)(JR)(QU)(TZ)(OD)(EV)(WB)(GY)(HM)
B: (AT)(LO)(ZV)(QI)(SR)(UB)(NW)(YC)(DM)(FE)(PH)(KJ)(XG)
C: (QO)(DS)(VC)(GM)(KY)(ZA)(IJ)(LN)(PB)(WH)(RF)(UX)(TE)
D: (AM)(KF)(PN)(LC)(XI)(JS)(QR)(TU)(OZ)(ED)(WV)(GB)(HY)
E: (AG)(LT)(ZO)(QV)(SI)(UR)(NB)(YW)(DC)(FM)(PE)(KH)(XJ)
F: (QO)(DE)(VS)(GC)(KM)(ZY)(IA)(LJ)(PN)(WB)(RH)(UF)(TX)

U: (BG)(LO)(QD)(MJ)(YT)(KS)(RV)(UA)(PE)(FW)(XC)(HZ)(IN)
V: (CV)(NQ)(BX)(SK)(UT)(WD)(PY)(AE)(FO)(HG)(RJ)(ML)(ZI)
W: (TR)(GV)(YF)(JP)(NB)(CD)(LM)(OQ)(SE)(ZK)(UI)(XA)(WH)
X: (EQ)(OJ)(TR)(PG)(BM)(NW)(UV)(XY)(SD)(IH)(AZ)(KF)(LC)

UV : (BHIQWOMRC)(DNZGXVJLF)(ATP)(EYU)(K)(S)
VW : (ASZURPFQB)(EXNOYJTIK)(CGW)(DHV)(L)(M)
WX : (BWIVPOEDL)(CSQJGUHNM)(AYK)(FXZ)(R)(T)

Tabelle 3.6:

[21] TURING, S. 64

Walzenlage: 321 , Ringstellung: AAA , Grundstellung: AAC

AD	Q	AYMCSEXFHBNJ
AD	O	ZKGVDTURWPLI
AD	O	IZKGVDTURWPL
BE		BMSLTYEPQFWIZ
BE		GAJCUHDRNKVXO
BE		OGAJCUHDRNKVX
CF	KWQMRSZLP	BCGX
CF	HYVFUIOTE	NDAJ
CF	EHYVFUIOT	JNDA

A: (QO)(AZ)(YK)(MG)(CV)(SD)(ET)(XU)(FR)(HW)(BP)(NL)(JI)
B: (BG)(MA)(SJ)(LC)(TU)(YH)(ED)(QR)(PN)(FK)(WV)(IX)(ZO)
C: (KH)(WY)(QV)(MF)(RU)(SI)(ZO)(LT)(PE)(BN)(CD)(GA)(XJ)
D: (QO)(AI)(YZ)(MK)(CG)(SV)(ED)(XT)(FU)(HR)(BW)(NP)(JL)
E: (BO)(MG)(SA)(LJ)(TC)(YU)(EH)(QD)(PR)(FN)(WK)(IV)(ZX)
F: (KE)(WH)(QY)(MV)(RF)(SU)(ZI)(LO)(PT)(BJ)(CN)(GD)(XA)

U: (RP)(BA)(ZL)(NH)(DW)(TE)(FU)(YV)(GS)(IX)(CQ)(OM)(KJ)
V: (DI)(OC)(UL)(NE)(VW)(AJ)(GF)(ST)(RP)(HM)(YX)(KZ)(BQ)
W: (NK)(ZB)(TY)(PI)(UX)(VL)(CR)(OW)(SH)(EQ)(FG)(JD)(AM)
X: (US)(EM)(CD)(QO)(GK)(WZ)(IH)(BX)(JY)(LV)(FA)(RT)(NP)

UV : (AQOHESFLK)(BJZUGTNMC)(DVX)(IYW)(P)(R)
VW : (ADPCWLXTH)(IJMSYUVOR)(BEK)(NQZ)(F)(G)
WX : (AEOZXSING)(BWQMFKPHU)(CTJ)(DYR)(L)(V)

Tabelle 3.7:

Walzenlage: 321 , Ringstellung: AAA , Grundstellung: AAE

AD	ETOIUFVYH	ADNJ
AD	PLZSRMQWK	GCBX
AD	KPLZSRMQW	XGCB
BE	I	DGKTRSJZPWUO
BE	A	ECMXHVLYNBFQ
BE	A	QECMXHVLYNBF
CF		ABFWYEXICQMLR
CF		SONKUHZVTDGJP
CF		PSONKUHZVTDGJ

A: (EP)(TL)(OZ)(IS)(UR)(FM)(VQ)(YW)(HK)(AG)(DC)(NB)(JX)
B: (IA)(DE)(GC)(KM)(TX)(RH)(SV)(JL)(ZY)(PN)(WB)(UF)(OQ)
C: (AS)(BO)(FN)(WK)(YU)(EH)(XZ)(IV)(CT)(QD)(MG)(LJ)(RP)
D: (EK)(TP)(OL)(IZ)(US)(FR)(VM)(YQ)(HW)(AX)(DG)(NC)(JB)
E: (IA)(DQ)(GE)(KC)(TM)(RX)(SH)(JV)(ZL)(PY)(WN)(UB)(OF)
F: (AP)(BS)(FO)(WN)(YK)(EU)(XH)(IZ)(CV)(QT)(MD)(LG)(RJ)

U: (FQ)(UM)(PA)(JT)(VS)(GN)(WR)(ZX)(IL)(BH)(ED)(OC)(KY)
V: (KC)(FG)(IE)(MO)(VZ)(TJ)(UX)(LN)(BA)(RP)(YD)(WH)(QS)
W: (DV)(ER)(IQ)(ZN)(BX)(HK)(AC)(LY)(FW)(TG)(PJ)(OM)(US)
X: (IO)(XT)(SP)(MD)(YW)(JV)(ZQ)(CU)(LA)(EB)(HK)(RG)(NF)

UV : (CMXVQGLEY)(DINFSZUOK)(ARH)(BWP)(J)(T)
VW : (AXSIRJGWK)(BCHFTPEQU)(DLZ)(NYV)(M)(O)
WX : (AUPVMIZFY)(CLWNQODJS)(BTR)(EGX)(H)(K)

Tabelle 3.8:

Walzenlage: 321 , Ringstellung: AAA , Grundstellung: AAS

AD	Y	DJLZFQMIXRGS
AD	W	CBOUPNEKATHV
AD	W	VCBOUPNEKATH
BE	AFLDMBZJRUY	CX
BE	GEKITOSHWNV	QP
BE	VGEKITOSHWN	PQ
CF	AIOXGEYHNFDW	J
CF	QBCPLSMUZVRT	K
CF	TQBCPLSMUZVR	K

A: (YW)(DC)(JB)(LO)(ZU)(FP)(QN)(ME)(IK)(XA)(RT)(GH)(SV)
B: (AG)(FE)(LK)(DI)(MT)(BO)(ZS)(JH)(RW)(UN)(YV)(CQ)(XP)
C: (AQ)(IB)(OC)(XP)(GL)(ES)(YM)(HU)(NZ)(FV)(DR)(WT)(JK)
D: (YW)(DV)(JC)(LB)(ZO)(FU)(QP)(MN)(IE)(XK)(RA)(GT)(SH)
E: (AV)(FG)(LE)(DK)(MI)(BT)(ZO)(JS)(RH)(UW)(YN)(CP)(XQ)
F: (AT)(IQ)(OB)(XC)(GP)(EL)(YS)(HM)(NU)(FZ)(DV)(WR)(JK)

U: (ZX)(ED)(KC)(MP)(AV)(GQ)(RO)(NF)(JL)(YB)(SU)(HI)(TW)
V: (CI)(HG)(NM)(FK)(OV)(DQ)(BU)(LJ)(TY)(WP)(AX)(ES)(ZR)
W: (DT)(LE)(RF)(AS)(JO)(HV)(BP)(KX)(QC)(IY)(GU)(ZW)(MN)
X: (CA)(HZ)(NG)(PF)(DS)(JY)(UT)(QR)(MI)(BO)(VE)(KX)(WL)

UV : (BTPNKIGDS)(CFMWYUEQH)(AOZ)(RVX)(J)(L)
VW : (AKRWBGVJE)(FXSLOHUPZ)(CYD)(IQT)(M)(N)
WX : (ADUNIJBFQ)(CRPOYMGTS)(EWH)(LVZ)(K)(X)

Tabelle 3.9:

Die Gleichungen auf Seite 66 hatten die Form $L = M^{-1}NM$. Ihre Lösungsmannigfaltigkeit konnte also auf die oben angegebene Weise ermittelt werden. Aus den ersten beiden Gleichungen war also das beiden Mannigfaltigkeiten gemeinsame Element zu ermitteln. Im Beispiel von Tabelle 3.6 hiess das:
Gesucht war diejenige Permutation $H = R_1 P {R_1}^{-1}$, die sowohl UV in VW überführte als auch VW in WX. Durch geschicktes Untereinanderschreiben wurde diese Folge von Transformationen deutlich:

$$\begin{array}{lcl} UV & = & \texttt{(GXVJLFDNZ)(BHIQWOMRC)(EYU)(ATP)(K)(S)} \\ VW & = & \texttt{(ASZURPFQB)(EXNOYJTIK)(CGW)(DHV)(M)(L)} \\ WX & = & \texttt{(DLBWIVPOE)(CSQJGUHNM)(KAY)(FXZ)(T)(R)} \end{array}$$

$\texttt{A}$ im Zyklus $(UV) \mapsto \texttt{D}$ im Zyklus (VW) und
$\texttt{A}$ im Zyklus $(VW) \mapsto \texttt{D}$ im Zyklus (WX)
$\texttt{D}$ im Zyklus $(UV) \mapsto \texttt{F}$ im Zyklus (VW) und
$\texttt{D}$ im Zyklus $(VW) \mapsto \texttt{F}$ im Zyklus (WX)
$\texttt{F}$ im Zyklus $(UV) \mapsto \texttt{P}$ im Zyklus (VW) und
$\texttt{F}$ im Zyklus $(UV) \mapsto \texttt{P}$ im Zyklus (WX)
$\ldots$

So erhielt man die Permutation $H = R_1 P {R_1}^{-1}$ in Zyklenschreibweise zu:

$$H = \texttt{(A D F P V Z B E C K M T H X S L R I N Q O J U W Y G)}$$

Aus den Ausdrücken für H erhielt man nach den Regeln von S. 65 je 26 äquivalente mögliche Lösungen für R_1

$$\begin{array}{l} H = \texttt{(A D F P V Z B E C K M T H X S L R I N Q O J U W Y G)} \\ \quad\;\;\; \texttt{(A B C D E F G H I J K L M N O P Q R S T U V W X Y Z)} \end{array}$$

1. Zeile nach dem Alphabet umgeordnet:

$$R_1 = \begin{pmatrix} \mathtt{A} & \mathtt{B} & \mathtt{C} & \mathtt{D} & \mathtt{E} & \mathtt{F} & \mathtt{G} & \mathtt{H} & \mathtt{I} & \mathtt{J} & \mathtt{K} & \mathtt{L} & \mathtt{M} & \mathtt{N} & \mathtt{O} & \mathtt{P} & \mathtt{Q} & \mathtt{R} & \mathtt{S} & \mathtt{T} & \mathtt{U} & \mathtt{V} & \mathtt{W} & \mathtt{X} & \mathtt{Y} & \mathtt{Z} \\ \mathtt{A} & \mathtt{G} & \mathtt{I} & \mathtt{B} & \mathtt{H} & \mathtt{C} & \mathtt{Z} & \mathtt{M} & \mathtt{R} & \mathtt{V} & \mathtt{J} & \mathtt{P} & \mathtt{K} & \mathtt{S} & \mathtt{U} & \mathtt{D} & \mathtt{T} & \mathtt{Q} & \mathtt{O} & \mathtt{L} & \mathtt{W} & \mathtt{E} & \mathtt{X} & \mathtt{N} & \mathtt{Y} & \mathtt{F} \end{pmatrix}$$

Weiter, erneut verschoben:

$$\begin{aligned} H = &(\mathtt{A\ D\ F\ P\ V\ Z\ B\ E\ C\ K\ M\ T\ H\ X\ S\ L\ R\ I\ N\ Q\ O\ J\ U\ W\ Y\ G}) \\ &(\mathtt{B\ C\ D\ E\ F\ G\ H\ I\ J\ K\ L\ M\ N\ O\ P\ Q\ R\ S\ T\ U\ V\ W\ X\ Y\ Z\ A}) \end{aligned}$$

umgeordnet:

$$R_2 = \begin{pmatrix} \mathtt{A} & \mathtt{B} & \mathtt{C} & \mathtt{D} & \mathtt{E} & \mathtt{F} & \mathtt{G} & \mathtt{H} & \mathtt{I} & \mathtt{J} & \mathtt{K} & \mathtt{L} & \mathtt{M} & \mathtt{N} & \mathtt{O} & \mathtt{P} & \mathtt{Q} & \mathtt{R} & \mathtt{S} & \mathtt{T} & \mathtt{U} & \mathtt{V} & \mathtt{W} & \mathtt{X} & \mathtt{Y} & \mathtt{Z} \\ \mathtt{B} & \mathtt{H} & \mathtt{J} & \mathtt{C} & \mathtt{I} & \mathtt{D} & \mathtt{A} & \mathtt{N} & \mathtt{S} & \mathtt{W} & \mathtt{K} & \mathtt{Q} & \mathtt{L} & \mathtt{T} & \mathtt{V} & \mathtt{E} & \mathtt{U} & \mathtt{R} & \mathtt{P} & \mathtt{M} & \mathtt{X} & \mathtt{F} & \mathtt{Y} & \mathtt{O} & \mathtt{Z} & \mathtt{G} \end{pmatrix}$$

usw.

In den Tabellen A.7 bis A.10 im Anhang sind diese äquivalenten Lösungen R_i für die verschiedenen Schreibungen der Permutation H aufgelistet.

Wenn man sich bei der Lösung Nr. 1 vorstellt, dass von der Eingangsseite (Basis) der Walze her Drähte gezogen seien zur Ausgangsseite (`AGIB...`), die Ausgangsseite dann von diesen Drähten löst, um eine Position weiterdreht und wieder an die Drähte „ankoppelt", dann ist dies die Lösung Nr. 2 usw. Die verschiedenen zu einem H gehörigen Lösungen für R_1 unterscheiden sich also nur durch verschieden grosse relative Verdrehungen der beiden Walzenseiten gegeneinander. An verschiedenen Tagen erhielt REJEWSKI i.a. auch verschiedene Permutationen H. Die dazugehörigen Mannigfaltigkeiten für R_1 zeigten zunächst keine gesetzmässigen Zusammenhänge. Die Schlüsseltafeln, die REJEWSKI im Herbst 1932 übergeben worden waren, enthielten die Anfangsstellungen der Walzen, sodass er nunmehr die bisher ermittelten verschieden erscheinenden Permutationen H bewerten konnte. Da von REJEWSKI zu den folgenden Schritten keine Angaben gemacht worden sind, wird hier eine Rekonstruktion seines möglichen Vorgehens versucht.

Die für die Chiffrierung wirksame Anfangsstellung `A` der Walze, also die Stellung des Walzenkörpers, war (natürlich) aus der Grundstellung `G`, wie sie bei der Einstellung sichtbar war, und der Ringstellung `R` zu gewinnen:

$$\mathtt{A} = \mathtt{G} - \mathtt{R}$$

Es musste allerdings berücksichtigt werden, dass das Weiterrücken der jeweils folgenden Walze nur durch den Ring gesteuert wurde.

Die wirksame Anfangsstellung der ersten Walze bestimmte allein die Entwicklung von H, sodass es erlaubt ist, in den folgenden Schritten vorauszusetzen, dass die Ringstellung `A A A` lautet, d.h. dass die wirksame Anfangsstellung mit der tatsächlichen Stellung des Walzenkörpers identisch ist. In den Beispielen der Tabellen A.7 bis A.10 im Anhang Seiten bedeutet dies, dass nunmehr durch die Schlüsseltafeln als bekannt vorausgesetzt werden kann, dass die Permutationen H zu den Anfangsstellungen der ersten Walze

`A` (Tabelle A.7)
`C` (Tabelle A.8)
`E` (Tabelle A.9)
`S` (Tabelle A1.0)

gehören. (Hierbei sind, wie oben begründet, zur Vereinfachung evtl. Steckerstellungen herausgerechnet und die Anfangsstellungen auf die Ringstellung `A A A` reduziert.) Wie die folgenden Beispiele zeigen, hängt das Verfahren zur Ermittlung der Verdrahtung der ersten Walze allein von der Grundstellung dieser Walze ab. Die Grundstellung (z.B.) `L G S` liefert die gleichen Ausdrücke wie (z.B.) `A A S`, wie der Vergleich der Tabellen A10 und A11 im Anhang zeigt. Diese Durchläufe für die Grundstellungen

`A A A , A A C , A A E` und `A A S` bei gleicher Walzenanordnung - also im selben Quartal - zeigen auf den ersten Blick keine Zusammenhänge.

Wenn man jedoch berücksichtigt, dass eine geänderte Anfangsstellung einer Verdrehung der Walze entspricht, um deren Verdrahtung es hier geht, kommt man zu einer Art ‚Normierung'. Der Ausdruck für H für die Grundstellung `A A A` lautet

`(A D F P V Z B E C K M T H X S L R I N Q O J U W Y G)`

Für Stellung `B` der Walze steht die Stelle `A` der Walze bei `Z` der Eingangswalze, also muss der Ausdruck für H mit `Z` beginnen, wegen der ungeänderten Abstände innerhalb des Zyklus hiesse also dieses H

`(Z C E O U Y A D B J L S G W R K Q H M P N I T V X F)`

Ebenso fortgesetzt:

```
(AA)C: (Y B D N T X Z C A I K R F V Q J P G L O M H S U W E)
(AA)D: (X A C M S W Y B Z H J Q E U P I O F K N L G R T V D)
(AA)E: (W Z B L R V X A Y G I P D T O H N E J M K F Q S U C)
                              ...
(AA)L: (P S U E K O Q T R Z B I W M H A G X C F D Y J L N V)
                              ...
(AA)S: (I L N X D H J M K S U B P F A T Z Q V Y W R C E G O)
                              ...
```

Dass dieses Verfahren tatsächlich keine Veränderung der Zyklen selbst hervorruft, sieht man beim Vergleich mit dem direkt abgelesenen H für `A A S`:

`(A T Z Q V Y W R C E G O I L N X D H J M K S U B P F)`

Der Übergang von der Anfangsstellung `A` der Walze zur Anfangsstellung `C` führte dazu, dass alle Elemente in H um zwei Stellen (entspricht dem Abstand der Buchstaben `A` und `C` voneinander) im Alphabet rückwärts verschoben werden müssen. Daher heisst nun die entsprechend „normierte" Permutation W für die Anfangsstellung `C`

$W =$ `(Y B D N T X Z C A I K R F V Q J P G L O M H S U W E)`

Entsprechend dem weiter oben gewonnenen Ergebnis gilt für die Anfangsstellung `E`

$W =$ `(W Z B L R V X A Y G I P D T O H N E J M K F Q S U C)`

Mit diesen normierten Permutationen werden erneut die Verdrahtungsvarianten ermittelt. Bei der Entwicklung der Verdrahtungsvarianten selbst muss noch der letzte Transformationsschritt ausgeführt werden, nämlich die Verschiebung um die entsprechende Stellenzahl (2 bei `C` usw.) nach rechts. Wie man in den Tabellen A.12 bis A.15 im Anhang sieht, führt die Normierung auf ein und dieselben Varianten zurück, sodass also die noch ausstehenden Untersuchungen von 26 Verdrahtungsvarianten ausgehen können (soweit eine Normierung möglich war).
Von einer zweiten Walze liegen, wegen des Glücksfalles, dass das SCHMIDTsche Material sich auf zwei verschiedene Quartale bezog, die entsprechenden Ergebnisse vor (Hier sei angenommen, es handele sich um die Walze Nr. III). Von der dritten Walze (Nr. II) weiss man zunächst nur, dass sie in einem oder mehreren zurückliegenden Quartalen als Eingangswalze eingesetzt gewesen sein muss.
Mit der normierten Grundstellung

$W =$ `(U W Y G A D F P V Z B E C K M T H X S L R I N Q O J)`

(vgl. mit der 1. Spalte der Tabelle A.1 im Anhang) erhält man letzten Endes die Tabelle A.2.

3.2 Der spanische Bürgerkrieg.

Im spanischen Bürgerkrieg von 1936 bis 1939 ergab sich die erste Gelegenheit, mit der ENIGMA unter Kriegsbedingungen chiffrierte Sprüche zu bearbeiten. Die nationalspanischen und die italienischen Verbände benutzten eine leicht veränderte Version der kommerziellen ENIGMA ohne Steckerbrett.[22]

3.2.1 KNOX.

Auf der Eingangswalze waren die Buchstaben wie auf der Tastatur angeordnet, ein Umstand, der den britischen Kryptologen Dillwyn KNOX lange auf eine falsche Fährte bei dem Versuch, die Wehrmacht-ENIGMA zu brechen, führen sollte[23].

Ende 1937 war in diese Version der Chiffriermaschine bei GC&CS ein Einbruch gelungen, nicht aber in den Verkehr der deutschen Verbände.[24]

Dieser Einbruch wurde erleichtert, weil alle Sprüche eines Tages - zumindest anfangs - jeweils von derselben Anfangsposition der Walzen ausgingen. Das weist darauf hin, dass es sich bei dem von ROHRBACH beschriebenen Verfahren [25] offenbar um das bei den italienischen und den national-spanischen Truppen mit der ENIGMA verwendeten gehandelt hat. Dabei könnte es sich um das Modell D gehandelt haben, wohl aber ohne die DAMM'schen„Influenzbuchstaben“, denn bei diesem Modell hatte die Umkehrwalze 26 verschiedene mögliche Stellungen. (Bei Modell C waren es nur zwei, sodass die Benutzung der ersten bzw. letzten vier Buchstaben der jeweiligen Wochentagsnamen als äussere Einstellung möglich erscheint.) Da zudem die innere Einstellung der Maschine über längere Zeit konstant blieb, hatten alle Sprüche eines Tages (mit etwa 100 konnte man sicher rechnen) dieselbe Anfangsstellung. Somit erhielt man ein (fast) vollständiges polyalphabetisches System, das bereits in Kolonnen geordnet war. Mit linguistischen Methoden (Häufigkeitsanalyse, für Einzelbuchstaben, Bigramme bzw. Trigramme) konnten die jeweils zugehörigen Klartexte gefunden werden. So erhielt man für einen Tag eine vollständige Entsprechung von Tauschalphabeten für die jeweiligen Walzenstellungen. Da die Umkehrwalze nie ihren Platz verliess und zudem die innere Verdrahtung der Lieferfirma behalten hatte, konnte mit Hilfe der Substitution

$$S_u = (T^r R_1 T^{-r})(T^s R_2 T^{-s})(T^t R_3 T^{-t}) K (T^t R_3^{-1} T^{-t})(T^s R_2^{-1} T^{-s})(T^r R_1^{-1} T^{-r})$$

die innere Schaltung der Walzen ermittelt werden. (In der Gleichung bedeuten T den Zyklus der Schreibmaschinentastatur, R_i die Walzen in ihrer Reihenfolge, der negative Exponent soll den Rückweg durch die Walze symbolisieren). (Vgl. Kap. 3.1.2.1)

Nachdem die Verdrahtung der Walzen bekannt war, konnte die jeweilige Tageseinstellung herausgefunden werden, wobei die Ringe allerdings die tatsächliche Lage verfälschten.

3.2.2 crib.

Hierbei war es nicht mehr nötig, die vorher unabdingbare Häufigkeitsanalyse anzuwenden. Es genügte ein vermuteter Klartext (Im Englischen: «crib») , um die Walzenanordung und die Startpositionen zu finden. Die Eigenschaft der ENIGMA, dass Klarbuchstabe und zugehöriger Geheimbuchstabe niemals gleich sein können, half, bei richtig angenommenem Klartext, einen Teil der falschen Positionen des Klartextes im

[22] FUENSANA: Es wurden Versionen mit K-Nummern verwendet und auch solche mit A-Nummern.
[23] HINSLEY I, S. 210; Peter TWINN in HINSLEY-STRIPP, S. 127
[24] ALLASON, S. 127; BLOCH d), D 11; HINSLEY I, App.1, S. 491
[25] ROHRBACH, S. 253

Geheimtext auszuschliessen. Wenn nämlich der Klartext über dem Geheimtext entlanggeführt wird, sind alle Positionen falsch, bei denen irgendein Buchstabe des angenommenen Klartextes mit dem darunterstehenden des Geheimtextes übereinstimmt.

BAUER[26] gibt an, wie hoch die Wahrscheinlichkeit für mögliche Lagen eines Klartextes im Geheimtext ist, abhängig von der Länge des vermuteten Klartexts. (Bei einem Klartextfragment der Länge 10 kann man rd. 68% erlaubte Positionen erwarten.)
Im folgenden werde bereits vorausgesetzt, dass die Walzenanordnung und die Anfangsstellung richtig seien. Die Länge des angenommenen Klartextes sei t. Solange bei der Chiffrierung aufeinander folgender Klarbuchstaben die mittlere Walze nicht weitergerückt wird, gilt demnach:

$$c_\mu = p_\mu R_1^{i+\mu} R_2^j R_3^k K R_3^{-k} R_2^{-j} R_1^{-i-\mu} \qquad \mu = 1 \ldots t$$

Dabei ist R_n^m die Walze n in der Schlüssellage m, wobei negative Exponenten den Durchgang durch die Walzen auf dem „Rückweg“ symbolisieren sollen. U stellt die Umkehrwalze dar. c_μ ist der μ-te Geheimbuchstabe, p_μ der μ-te Klarbuchstabe. Wegen der Konstanz kann man zusammenfassen:

$$M = R_2^j R_3^k K R_3^{-k} R_2^{-j}$$

Aus der ersten Gleichung entstehen so

$$c_\mu = p_\mu R_1^{i+\mu} M R_1^{-i-\mu}$$
$$c_\mu R_1^{i+\mu} = p_\mu R_1^{i+\mu} M$$

Die letzte Gleichung zeigt, dass unter den genannten Voraussetzungen die Substitutionen von Klartext und Geheimtext schon durch die erste Walze allein Ergebnisse liefert, die sich jeweils nur durch eine einfache monoalphabetische Substitution unterscheiden. Es lassen sich daher sowohl die erste Walze als auch deren Anfangsstellung identifizieren. (Die Voraussetzung, dass die mittlere Walze nicht bewegt werden soll, ist bei genügend langem angenommenen Klartextteil mit Sicherheit bei einer Teilung dieses Textes in zwei Abschnitte in einem der beiden Abschnitte erfüllt.)

3.2.2.1 bâtons, rods.

Praktiziert wurde dieses Verfahren mit Kartonstreifen, bzw. Holzstäbchen, auf denen zu jeweils einem Klartextbuchstaben die für die verschiedenen Stellungen der ersten Walze allein entstehenden Geheimtextbuchstaben untereinandergeschrieben waren («bâtons», «rods»).

Beispiele für solche Streifen siehe Tabellen 2.2, 2.3 und 2.5.
Die Bewegung der ersten Walze konnte durch die Auswahl der Streifen, die zu den Buchstaben p_μ und c_μ gehörten und ihre relative Lage zueinander charakterisiert werden. (Notwendig waren auf den Streifen zwei volle Durchgänge der ersten Walze.)
Die jeweils den einzelnen Buchstaben des angenommenen Klartextes und des dazugehörigen Geheimtextes zugeordneten Streifen wurden nebeneinandergelegt, mit der dem Weiterrücken der ersten Walze entsprechenden vertikalen Versetzung. Sodann wurde nach derjenigen Zeile gesucht, in der die Bedingungen der einfachen Substitution erfüllt waren.
Als Beispiel diene:

```
Klartext   : a b e n d m e l d u n g
Geheimtext : Q R I W Q J M R N J J C
```

Die Tabelle 3.10 zeigt das Verfahren.

[26] BAUER, S. 190 u. 311

	Klartext :	Geheimtext :
	`abendmeldung`	QRIWQJMRNJJC
Stäbeschema		
0	ELBUMPHLLWHJ	XRLGWTMVAJFL
	JDNQQMMHFBRG	TNQADBIBSFPM
	KIRNTIGRMVXC	QXKFVQSVHPWU
	CCUJGSNYNRRM	MERGKMZARWOJ
	HYHTLZOQVDWT	WWSYUJRBXODF
	BKMAFRWFKHXL	DLADAFGTRDNC
	XOGSMGLPGKPA	VVPXUPQYWNTY
	JRNHNQHVDXUK	KBLTZWWSXTNI
	NEORVWEPZCOQ	UVIFAOQOPNSP
	QJWXKQAUJWKK	AAEJSDVAUSTH
	DDLRGVKVQDWP	UBOMXNWEOTLW
	IKHWDWRNIEAQ	ZTVZRTOHKLQG
	CLEXZOJSXMDI	AYNENNTUWQKM
	JTAPJTYMHBQN	SSCYZSNZAKGG
	KIKUQNIINXVH	XOMFDTJTDGSL
	SEROIJOUHUPD	RASGGLVAQSWM
	HBJKXVIYMQWP	NEMOTQZBVWZE
	DXYWHZNBNAXT	ZHRDYKCJPZMJ
	AHIANCOOFHFW	DUSZSGPYWMRD
	WOODHPGTKZUJ	GZKWZSUUXRLZ
20	*GGIQMULNEOQO*	*TTPSAWORFLSL*
	NVNVNOFUAYNI	YAJCIZVNUSTP
	FFOPFVBVMEJP	SBFJXMWXQTBS
	ULGWKWNDQYTQ	ZJRBTREENBQF
	EFLXEERSTDAY	AYVQQLTWJQMK
25	KKFFATUOGESN	IUYAMSPLTMJE

Tabelle 3.10:

Der Vergleich mit Tabelle A.2 im Anhang zeigt, dass die zum Klartextbuchstaben der Tabelle 3.10 gehörenden Zeilen der Matrix transponiert als Spalten benutzt werden. Diese sind entsprechend den Klartextbuchstaben `b, e, n` usw. jeweils um eine Position nach oben verschoben rechts neben die Spalte für `a` (Anfangsbuchstabe des Klartextes) gelegt. (Entsprechend beim Geheimtext). In der herausgehobenen Zeile 20 zeigen die Zyklen `(QS)`, `(OL)` und `(GT` den Erfolg an. Die Wiederholung des Verfahrens für die Walze II bzw. III bringt keine Lösungen. Mit einem Katalog aller möglichen Kombinationen für die zweite und die dritte Walze (+ Umkehrwalze) kommt man auch zu weiteren Aussagen über die zweite bzw. dritte Walze.

```
G G I Q M U L N E O Q O
T T P S A W O R F L S L
```

Diese gesuchte Permutation ergibt sich bei Stellung 20 der Walze I ohne Widerspüche. Die Anfangsstellung vor Chiffrierung des ersten Buchstabens liegt einen Buchstaben zurück.

Zum Bestimmen der zweiten Walze konnte man ein Klartextstück und das vorgestellte Schema dann benutzen, wenn während dessen Chiffrierung die zweite Walze weitergerückt wird. Ein Beispiel soll das Verfahren zeigen: Vorgegeben seien Klartext und Geheimtext[27]

[27] erzeugt mit der Walzenlage III, I, II, der Ringstellung `A,A,A` und der Grundstellung `B,T,X`

```
a n d a s o b e r k o m m a n d o d e r
H D Q Y F H F A H N Q D Q N K O V Y F H
```

Werden beide Zeilen der Substitution mit einer der Walzen unterworfen, dann findet man nur mit der Walze II (Tabelle A.4) in der Zeile 24 ein entsprechendes Ergebnis (Tabelle 3.11)

	Klartext :	Geheimtext :
	andasoberkommandoder	HDQYFHFAHNQDQNKOVYFH
Stäbeschema		
0	ALGHBIOAWEEKCGVKCYNS	URXGXRBNUWQBRNAVRLDH
	IAOOQJQORFTCRYOXRGCN	WGKZGNPPHLYQXVPCFYVP
	BNQDIRTKZNORMNUYZMUB	ZOLFBFLSWDRDEOKRBNKI
	HCSLXXCCSTWMUABGBBJX	IQTMPUDBOSXSTUSZTFFO
	OUVNSMXRYIPUNPQMDTEP	DSZBLHSWBNEKBBLBISNV
	DHEPAELEFAVNTHYBGIME	RVOJDWFKCVTXDQRDVTGK
	LIZSTTHTUPCTAUATPDFR	NEGLSOUGKOBYFYYGKBMS
	NQNBZOZLCKRAPVCIKLLG	FZVNFBMYQUDGIANPCHTU
	PWJWGWOYESZPXDFDYESY	UNQQUCZNFBFMRCVKPWIW
	SLBKVPBZGLBXZJOLUKHL	HJYZMKAAXQIBMFXYQOQZ
	BDQGDVQHJRDZBYJEMRPM	WBRUZQIPMYRTAOZUYDSI
	WSDYFCINSYGBEQXKBGRU	OQXIAFOHHAMIWJCMEYUD
	KNSNHRVCNNPENFTROOTA	BDEEIXDUPCADOXLBTGXR
	GVKAKZWUBVKNIALGDQWP	CSTWOMVVIFWLDTGOLZGN
	YOXPTBEJXXYIWIAOVSFH	KKBLDHKDOOOEQLUDAFBF
	NUYHODKEPZUWSBNQIVAW	QXDYVPFJVJDKFAQVVMPU
	ABGUCGZMECMSKHCSJEOR	FYFNKINYKXQRXNIIDBLH
	PQMVYPRFRLBKZOUVRZKZ	XGIFFOGQSTFGKCXJWJDW
	HYBDQKGLGGOZMDHEXNCS	MMRSNVMFULXOLUKRCLSO
	UATJFYBSYUDMBLIZMJRY	HBMTGKTAWAKQTHZXJNFB
	VCIYSUJHLQVBTNQNEBEF	PTABMSIIZNLSZIRMYQUC
	DFDQHMCPMIITGPWJTQTU	IIWHTUQBICTVOQEEGZMK
	JOLFZBIRUXJGHSLBODLC	ODOWIWSHDUZEGWFTIUZQ
	YJEAMOPTAKRHPBDQWSYE	VLDOQZUORHOZVLNOKIAF
24	*QXKINDEWPZXPVWSDPKZG*	*KEQDSIXDNIGNQDTWNEIX*
	FTRBVVMFHRMVKKNSVXHJ	SKFYUDGLFQVJYSIPWWOM

Tabelle 3.11:

Zeile 24 herausgegriffen: Die Anfangsstellung vor Chiffrierung des ersten Buchstabens liegt einen Buchstaben zurück. Die Trennstelle liegt zwischen den Paaren `(EX)` und `(WD)`. Die Trennstelle soll die Stelle andeuten, an der offenbar die mittlere Walze bewegt wurde. Das folgt einmal aus dem Ergebnis des ersten Schrittes, der Bestimmung der ersten Walze, ausserdem tritt hier die Abweichung des Paares (`WD`) vom Paar (`DI`) auf, während das vorhergehende Paar (`EX`) noch mit dem vorhergegangenen Paar (`XE`) übereinstimmt.

```
Q X K I N D E     W P Z X P V W S D P K Z G
K E Q D S I X     D N I G N Q D T W N E I X
```

Aus dem Ergebnis von Tabelle 3.11 folgen für den Teil 1 (vor dem Rücken der zweiten Walze) die Zweierzyklen

`(DI)(EX)(KQ)(NS)`

für Teil 2

`(DW)(EK)(IZ)(NP)(QV)(ST)(XG)`

Links bzw. rechts von der Trennstelle gilt

$$\begin{aligned} C_l &= P_l R_1^{i+l} M_1 R_1^{-i-l} \\ l &= 1 \ldots s \\ C_r &= P_r R_1^{i+r} M_2 R_1^{-i-r} \\ r &= s+1 \ldots l \end{aligned}$$

mit den Verkürzungen

$$\begin{aligned} M_1 &= R_2^j R_3^k K R_3^{-k} R_2^{-j} \\ M_2 &= R_2^{j+1} R_3^k K R_3^{-k} R_2^{-j-1} \end{aligned}$$

Beide Ausdrücke haben den gemeinsamen Kern

$$K = R_3^k K R_3^{-k}$$

Damit gelten

$$\begin{aligned} C_l &= P_l R_2^j K R_2^{-j} \\ C_r &= P_r R_2^{j+1} K R_2^{-j-i} \\ C_l R_2^j &= P_l R_2^j K \\ C_r R_2^{j+1} &= P_r R_2^{j+1} K \end{aligned}$$

d.h. zwischen den Paaren (C_l, P_l) und (C_r, P_r) besteht für ein bestimmtes j eine monoalphabetische Substitution K. Es gilt also, dieses j zu finden.
Mit den Paaren vor der Trennstelle

`(D I) (E X) (K Q) (N S)`

ergibt das Verfahren mit den Walzen I (Mitte) und III (letzte) die Lösungen `T` (Mitte), `B` (letzte)
Die Substitution aus Walzen Nr I (Mitte) , III (letzte) und der Umkehrwalze lautet:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
VYWIXGFZDMQTJSURKPNLOACEBH
```

Mit den Paaren nach der Trennstelle

`(D W) (E K) (I Z) (N P) (Q V) (S T)`

ergibt das Verfahren mit den Walzen I (Mitte) und III (letzte) die Lösungen `U` (Mitte), `B` (letzte)
Die Substitution aus Walzen Nr I (Mitte) , III (letzte) und der Umkehrwalze nach der Trennstelle lautet:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
LFOWKBXMZREAHPCNVJTSYQDGUI
```

Mit der mittleren Walze, hier angenommen Nr. I, werden von den Klartextelementen die Elemente `d, e, k, n` und `q` und die zugehörigen entsprechende Geheimtextelemente `I, X, Q, S` und `K` (Teil 1) und ebenso, um eine Position versetzt (weitergeschaltet), die genannten Klarbuchstaben und die zugehörigen Geheimbuchstaben nach der Trennstelle `W, K, E, P`, und `V` substituiert. In Tabelle 3.12 sind diese Substitutionen für jede Stellung ausgedruckt. Gesucht ist die Stellung, bei der die einzelnen Teile durch eine einfache Substitution verbunden sind. In Zeile `T` ist das der Fall, wie das Paar (`RI`) zeigt. Als letzten Schritt musste man noch die Lage der letzten Walze und der Umkehrwalze bestimmen. Dazu diente am einfachsten ein Katalog, unter dessen 26 durch die letzte Walze bestimmten Eintragungen die richtige zu finden war. Erfolg bei Walze I bei Stellung 19 d.h. bei `T`

0	DEKNQ	IXQSK	DEKNQ	WKEPV
	FLNWX	VRXSN	KFSXT	QSFWA
	KFSXT	YBTOS	EBMFQ	AMBSP
	EBMFQ	LHQYM	ANTUM	GTNPZ
	ANTUM	QBMFT	MRUQW	AURLF
	MRUQW	KGWXU	QUCND	FCUVZ
	QUCND	RHDMC	THRJV	GRHCE
	THRJV	SZVWR	GMNTK	YNMUF
	GMNTK	AEKCN	LGKAU	DKGJX
	LGKAU	PYUWK	FNGSA	XGNTC
	FNGSA	LUABG	MOQHU	TQOZW
	MOQHU	IGUCQ	NWXRZ	FXWTS
	NWXRZ	EKZUX	VLPXA	JPLYE
	VLPXA	ONAZP	KHERS	MEHZI
	KHERS	VASTE	GEOWX	ZOERL
	GEOWX	NFXPO	DAUXR	EUAWY
	DAUXR	CZRBU	ZKOPN	YOKQD
	ZKOPN	MGNFO	JRTUZ	FTRMX
	JRTUZ	SHZIT	QJUOD	GUJYE
	QJUOD	MPDVU	IYMKG	OMYCF
19	*IYMKG*	*REGAM*	*XIRWT*	*DRIFN*
	XIRWT	SATUR	HOLAY	ZLOSC
	HOLAY	KXYBL	NIHDS	WHIXY
	NIHDS	PTSCH	HNTQZ	STNRV
	HNTQZ	JDZKT	MOXVA	CXOYR
	MOXVA	FKAZX	NGAPI	JAGZB
	NGAPI	RCIVA	FLNWX	BNLHI

Tabelle 3.12:

```
IYMKG      XIRWT
REGAM      DRIFN
```

Mit den Paaren aus der zweiten Stufe `(I R) (Y E) (M G) (K A)` ergibt das Verfahren mit der Walze III die Lösung `B`.

Die Substitution aus Walze III und der Umkehrwalze lautet:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
KHUXYWMBRQAZGTPOJIVNCSFDEL
```

Man konnte aber auch für jede ermittelte erste Walze einen Katalog der Permutationen für alle Stellungen der übrigen Walzen erstellen und so nach dem ersten Schritt für die erste Walze die restlichen Stellungen auf einmal bestimmen.

Für den Fall, dass während der Chiffrierung des Klartextstückes die mittlere Walze nicht rückte, musste von Anfang an ein solcher Katalog zu Hilfe genommen werden, da die vorher geschilderte Methode das Rücken benötigt.

Ein Beispiel[28] verdeutlicht das Vorgehen noch weiter (Klartext und Geheimtext untereinander geschrieben, Chiffrierung mit der Kommerziellen Enigma, ohne Steckerbrett):

`f o u r t h b a t t a l i o n`
`J D N Q G X P L L H T O W E K S A L B C B G U C S F W A W B`

Das bisherige Vorgehen weist aus: Rechte Walze: III; Anfangsstellung: `Z` Damit ergibt sich im ersten Schritt:

Stellung : `Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C`
Klartext : `f o u r t h b a t t a l i o n`
Geh.-Txt: `J D N Q G X P L L H T O W E K S A L B C B G U C S F W A W B`

Mit III :

Pseudo : w x a k i a t l x h t s e e t
Pseudo : M Q I T A I K F Q G K R D D K

Deutlich erkennbar sind die Paare `(QX),(AI),(KT),(ED)`.
Eine Fortführung ab Stellung `O` mit den erkannten Paaren führt zu

Stellung: `O P Q R S T U V W X Y Z A B C`
Pseudo : . q . . k l t g
Pseudo : C X J O T F K H K G X R C Z U

Dies zurücktransformiert:

Stellung : `O P Q R S T U V`
Klartext : `. k . . w c h m`
Geh.-Txt: `S A L B C B G U`

Daraus ist zu schliessen, dass die mittlere Walze zwischen `N` und `S` weitergerückt sein muss. Ein Versuch, die Pseudozeilen mit den Daten der Walze I weiter zu bearbeiten, führt zu Widersprüchen. Daher wird als mittlere Walze nun II angenommen.
Die ersten obigen Pseudo-Zeilen mit den Daten von Walze II, Anfangsstellung (angenommen) `A`, transformiert, führt zu

Pseudo : d f k l n k w c f o w h v v w
Pseudo : R Y N W K N L T Y B L U I I L

Der zweite Teil (`CXJ...`)wird mit Anfangsstellung `B` transformiert und erkennbare Paare werden eingefügt:

Pseudo : u . . . f i k n k v . . u c o
Pseudo : H A M J Y V N K N I A Q H T B

Diese Zeilen werden mit den Daten von Walze II zurücktransformiert:

Pseudo : s . . . b g h k h f . . s w i
Pseudo : C X J O T F K H K G X R C Z U

Zurück zum Klartext mit den Daten von Walze III, ab Stelle `O` führt zu:

Klartext: `r . . . e a t e d t . . i l`

Zu vermuten ist der Text „ retreated to hill “ , was schliesslich zur Zeile

Pseudo : s a m n b g h k h f a q s w i

führt, keine Widersprüche, aber ein neues Paar von Übereinstimmung.

Aus der nun bekannten Stelle des Rückens der nächsten Walze lässt sich sofort auch die Ringstellung ableiten.
Nach der Identifizierung der ersten Walze erhält man Zweierzyklen der Kombination der mittleren, der linken Walze und der Umkehrwalze. Mit Hilfe von Katalogen dieser Kombinationen sind Walzennummer und Walzenstellung der zweiten und der dritten Walze ablesbar.

[28] «Analysis of the Cipher Machine Enigma Type K», NARA Dokument, Nr. 3448, Box CBQM33

Kapitel 4

Polnische Erfolge bis 1939

4.1 Fortsetzung Walzenverdrahtung

Wegen der unbekannten Steckerlage konnte das ab Seite geschilderte Verfahren von REJEWSKI nicht angewandt werden: Die Produkte UV, VW und WX hatten keine übereinstimmende Zyklenstruktur. Zur Abschätzung, wie gross die Wahrscheinlichkeit p war, zwei Tage mit identischen Walzenlagen und Walzenstellungen zu finden, oder wenigstens nur eine Positionsdifferenz von 1 bei der (gleichen) rechten Walze:
In einem Quartal mit fester Walzenlage waren 26^3 Walzenstellungen möglich. Ausgehend vom ersten Tag des Quartals gibt es am nächsten Tag 17576-3 weder identische noch um eins abweichende Stellungen, am übernächsten sind es 17576-6 Stellungen, nach 90 Tagen 17576-3(90-1). Daraus folgt die Wahrscheinlichkeit, dass im Quartal das gewünschte Ereignis nicht eintritt zu

$$\begin{aligned} q &= (17573 \cdot 17570 \cdot \ldots \cdot 17309)/17576^{89} \\ q &\approx 0,5 \end{aligned}$$

(Bei GAJ liegt eine ähnliche Rechnung vor.)[1] Für alle Quartale eines Jahres würde die Wahrscheinlichkeit p für das Auftreten des erwünschten Ereignisses betragen

$$\begin{aligned} p &= (1 - q^4) \\ p &\approx 0,94 \end{aligned}$$

Durch geschicktes Untereinanderschreiben der jeweils ersten (zweiten, dritten) Zeilen der beiden Charakteristiken sah man aber, welche Buchstaben in beiden Schlüsseln durch die Stecker unbeeinflusst geblieben waren. Wenn an zwei solcherart günstigen Tagen die Tagesschlüssel nur durch die Steckerlagen unterschieden waren, konnte man schreiben (die Angaben für den 2. Tag sind unterstrichen):

$$\begin{aligned} AD &= SPR_1P^{-1}MPR_1{}^{-1}P^3R_1P^{-4}MP^4R_1{}^{-1}P^{-4}S^{-1} \\ BE &= SP^2R_1P^{-2}MP^2R_1{}^{-1}P^3R_1P^{-5}MP^5R_1{}^{-1}P^{-5}S^{-1} \\ CF &= SP^3R_1P^{-3}MP^3R_1{}^{-1}P^3R_1P^{-6}MP^6R_1{}^{-1}P^{-6}S^{-1} \end{aligned}$$

$$\begin{aligned} &1.\ Tag \\ AD &= ST_1S^{-1} \\ BE &= ST_2S^{-1} \\ CF &= ST_3S^{-1} \end{aligned}$$

[1] Geburtstags-Paradoxon

2. *Tag*

$$
\begin{aligned}
\underline{AD} &= \underline{S}T_1\underline{S}^{-1} \\
\underline{BE} &= \underline{S}T_2\underline{S}^{-1} \\
\underline{CF} &= \underline{S}T_3\underline{S}^{-1}
\end{aligned}
$$

Wegen der reziproken Eigenschaft der Stecker gilt

$$S^{-1} = S$$

also

$$
\begin{aligned}
S\underline{S}^{-1} &= S\underline{S} \\
T_1 &= S^{-1}ADS
\end{aligned}
$$

und

$$
\begin{aligned}
T_1 &= \underline{S}^{-1}\underline{ADS} \\
\underline{AD} &= \underline{S}S^{-1}ADS\underline{S}^{-1} \\
\underline{AD} &= (S\underline{S}^{-1})^{-1}(AD)(S\underline{S}^{-1})
\end{aligned}
$$

$\underline{AD}$ und AD sind also ähnlich. Damit war das Produkt $S\underline{S}$ bestimmbar. Wenn der Unterschied der Walzenstellungen nur eine Position der ersten Walze betraf, musste die eben angestellte Überlegung auch für den Vergleich von AD mit $\underline{BE}$ bzw. BE mit $\underline{CF}$ gelten .
Ein Beispiel soll das erläutern. (Es handelt sich, zur Kontrolle für den Leser, um Strukturen mit der Walzenstellung III, I, II, der Ringstellung `A, B, F` - bzw. `A, B, G` - und der Grundstellung `L, M, T`.)

$AD =$ `(AWFJBCPTDRZO)(EMIULGXHNKYQ)(S)(V)`
$BE =$ `(AKXCMERNJQGW)(BOLSUFPTHDYV)(I)(Z)`
$CF =$ `(ARUDGXKPQVLWO)(BTIYZNEFHCJMS)`

und

$\underline{AD} =$ `(AXVYQNLIGZKRC)(BFESDJMTHOUPW)`
$\underline{BE} =$ `(AJBYPTXRSOQW)(CDIUVEGLHFNK)(M)(Z)`
$\underline{CF} =$ `(APTFXCMBOGZE)(DLWQKHYUIRNJ)(S)(V)`

Passend untereinander positioniert, zeigen sich die Zusammenhänge

$AD =$ `(AWFJBCPTDRZO)(EMIULGXHNKYQ)(S)(V)`
$\underline{BE} =$ `(QWAJBYPTXRSO)(IUVEGLHFNKCD)(M)(Z)`

$BE =$ `(AKXCMERNJQGW)(BOLSUFPTHDYV)(I)(Z)`
$\underline{CF} =$ `(QKHYUIRNJDLW)(BOGZEAPTFXCM)(S)(V)`

Das Produkt $S\underline{S}$ ergibt sich somit zu

`(AQDXHF)(CY)(EIVMU)(GL)(SZ)`

Dieses Produkt muss aufgelöst werden. Dazu werden die Zyklen so untereinandergeschreiben, dass sich bei richtiger Lage geeignete Steckerpaare ergeben. Es ist hier günstig, S mit `(MV)` und `(SZ)` zu belegen:

`(AQDXHF)(EIVMU)(CY)(GL)(SZ)`
`(HXDQAF)(EUMVI)(YC)(LG)(ZS)`

Senkrecht bzw. schräg herausgelesen: (vgl. S. 63)

$S =$ `(AH)(QX)(IU)(MV)(SZ)(CY)`
$\underline{S}=$ `(HQ)(DX)(AF)(EI)(UV)(GL)`

Rechnet man die Stecker heraus, ergeben sich für AD und $\underline{BE}$ bzw. für BE und $\underline{CF}$ jeweils identische Ausdrücke.

Es ergab sich nun eine relativ geringe Anzahl von Prüfungen, zu welcher Charakteristik welche der möglichen Steckerstellungen gehörte. Ein Kriterium für die Richtigkeit einer so erreichbaren Charakteristik für die Grundstellung ohne Stecker (die nach wie vor selbst unbekannt waren) war die Durchführbarkeit des Verfahrens zur Gewinnung von H und damit der Verdrahtungsvarianten. Dieses so ermittelte H entschied auch, ob es sich bei dieser Eingangswalze weder um die Walze Nr. I noch um die Walze Nr. III , also um die Walze Nr. II gehandelt hatte. GAJ[2], der richtig darauf hinweist, dass das oben beschriebene Tun nur mit Hilfe von Material möglich war, das entweder durch direkte Spionage oder durch die „angekauften“ Quartalslisten möglich war, zeigt, dass unter zwei Bedingungen auch ohne diese Vorgaben Erfolge zu erzielen waren:

1) H musste bekannt sein
2) Glück bei mühsamer Arbeit.

Weiter oben wurde bereits auf die Bedeutung der Rekonstruktion der Produkte der Zweierzyklen A bis F hingewiesen. Anfangs hatten die Fehler der Chiffrierer, Spruchschlüssel aus drei gleichen Buchstaben oder aus drei auf dem Tastenfeld benachbarten Buchstaben zu wählen, den polnischen Kryptologen die Arbeit erheblich erleichtert. Nach dem Verbot solcher Buchstabenfolgen waren die bisherigen Methoden zunächst wirkungslos geworden. Hier hat aber die genaue Beobachtung und Statistik gezeigt, dass manche Chiffrierer gewisse Vorlieben zeigten für z.B. für `A` bzw. `Q` als ersten Buchstaben, als zweiten einen Vokal, als dritten `L` bzw. `O`. Seltener traten die Buchstaben `Y` oder `J` auf. Diese statistischen Gegebenheiten änderten sich im Laufe der Zeit, sie waren auch verschieden bei Heer oder Luftwaffe.[3] Damit wurde die Suche nach den Korrespondenzen zwischen Indikator und Spruchschlüssel auf geringere Mannigfaltigkeiten eingeschränkt. Auch, wenn die Liste der täglichen Indikatoren nicht alle Buchstaben des Alphabets in den Positionen 1 bis 6 abdeckte, konnte die Tagescharakteristik in vielen Fällen angegeben werden. (Hierbei half die Tatsache, dass immer Permutationen gleicher Länge paarweise auftreten mussten.)

Selbst für die Fälle, in denen das Verbot von Buchstabenwiederholungen strikt eingehalten wurde, entwickelten die polnischen Kryptologen eine Methode, aus der Tagescharakteristik die Produkte A bis F der Zweierzyklen zu finden. In einer Matrix wurden die Kombinationen von Permutationen zweier Stufen daraufhin überprüft, ob für die möglichen verschobenen Stellungen der Permutationen etwa gleiche Buchstaben für den Spruchschlüssel resultierten. Damit wurde diese Kombination von Verschiebungen ausgeschlossen.[4] Die Tabellen 4.1 bis 4.5 zeigen das Verfahren.

[2] GAJ, S.105 -111
[3] GAJ, S. 113
[4] DEAVOURS gibt ein Programm an (FACTORS.BAS), das in dieser Richtung arbeitet. In GAJ, S. 114 - 120 ist ein Schema dargestellt, das wegen seiner grösseren Effizienz verwendet wird.

Walzenanordnung: 312; Umkehrwalze B; Ringstellung: AAA ; Grundstellung: AAA;
Steckverbindungen: (RE)(CI)(OM)(HK)(YF)(JQ); 90 Indikatoren

MFZ	CIW	EZV	IFD	AIQ	XZT	THD	GGQ	UUT	IWN	AEI	XPA
CMS	MVY	KYC	GAL	TNK	QGM	QWE	DEV	GPB	BNJ	ZAR	YRW
VEH	UWG	STX	RQN	PSI	ALA	SCP	NBF	VIG	SAU	NNM	VGQ
IXO	AKT	XVF	CMI	MVN	KYY	DGK	QHL	LAR	BDE	ZTV	YSB
IUN	AYI	XHA	HGL	KHK	PAM	YAB	ENA	BGE	JMF	XVP	OYO
EDK	YTL	MSR	TXY	GKS	UVI	SCZ	NBW	VIV	WQK	LSL	ZLR
ALZ	IOW	RQV	XGW	JHZ	IAJ	TUA	GYB	UHN	ZRS	BZY	WNC
WZU	LRM	ZFQ	IFC	AIX	XZS	DPO	QJT	LWF	PWF	REP	HPO
SFA	NIB	VZN	BUL	ZYK	YHM	FNE	OAV	NRB	KSU	HQM	CDQ
XBA	JCB	IJN	JPN	XAF	ORG	KFN	HII	CZA	XZL	JRK	IFM
LSM	WQU	DDL	QIG	DFH	GCP	SWN	NEI	VPA	OZS	FRY	JFC
PNK	RAL	HRR	NZG	SRH	FFP	GYE	TUV	QMB	GXU	TKM	QVQ
MWH	CEG	EPX	OZJ	FRR	JFW	MKA	CXB	EON	EZX	YRC	MFH
PAL	RNK	HGM	OIV	FFE	JCZ	DET	QWO	LTD	VQY	USS	SLI
JVQ	XMD	OXU	XFV	JIE	IZZ	LKV	WXE	DOZ	IQC	ASX	XLS
JSC	XQX	ODS	IXH	AKG	XVX	UBW	VCZ	TJJ	YUJ	EYR	BHW
ELZ	YOW	MQV	UFC	VIX	TZS	CFH	MIG	KZX	PCE	RBV	HIB
ADX	ITC	RSH	LQR	WSJ	DLK	IJC	APX	XBS	VHQ	UGD	SUU
JNC	XAX	ORS	UTF	VDP	TEO	ADM	ITU	RSL	RVM	PMU	AXL
OIP	FFF	JCG	XRF	JZP	INO	PIQ	RFD	HCU	LBP	WCF	DJG
HGY	KHS	PAI	AJF	IPP	RBO	HRL	KZK	PNM	BAJ	ZNR	YGW
PMV	RVE	HYZ	XUY	JYS	IHI	IHF	AGP	XUO	LOX	WLC	DKH
EMS	YVY	MYC	NUP	SYF	FHG						

Tabelle 4.1:

Walzenanordnung: 312; Umkehrwalze B; Ringstellung: AAA ; Grundstellung: AAA;
Steckverbindungen: (RE)(CI)(OM)(HK)(YF)(JQ); 90 Indikatoren

AEIXPA	AGPXUO	AIQXZT	AIXXZS	AKGXVX
AKTXVF	APXXBS	ASXXLS	AYIXHA	BZYWNC
CEGEPX	CIWEZV	CXBEON	DEVGPB	DFHGCP
ENABGE	EYRBHW	FFEJCZ	FFFJCG	FRRJFW
FRYJFC	GGQUUT	GKSUVI	GYBUHN	HIICZA
HQMCDQ	IOWRQV	IPPRBO	ITCRSH	ITURSL
JCBIJN	JHZIAJ	JIEIZZ	JRKIFM	JYSIHI
JZPINO	KHKPAM	KHSPAI	KZKPNM	LRMZFQ
LSLZLR	MIGKZX	MVNKYY	MVYKYC	NBFVIG
NBWVIV	NEIVPA	NIBVZN	NNMVGQ	OAVNRB
PMUAXL	PSIALA	QHLLAR	QJTLWF	QWOLTD
RALHRR	RBVHIB	REPHPO	RFDHCU	RNKHGM
RVEHYZ	SRHFFP	SYFFHG	TKMQVQ	TNKQGM
TUVQMB	UGDSUU	USSSLI	UWGSTX	VCZTJJ
VDPTEO	VIXTZS	WCFDJG	WLCDKH	WQUDDL
WSJDLK	WXEDOZ	XAFORG	XAXORS	XMDOXU
XQXODS	XVPOYO	YOWMQV	YRCMFH	YTLMSR
YVYMYC	ZARYRW	ZNRYGW	ZTVYSB	ZYKYHM

Die Permutationszyklen für die Indikatorstellen
1 - 4 (AXONVTQLZYMKP)(BWDGUSFJIRHCE)
2 - 5 (ARFCJWTSLKVYH)(BIZNGUMXOQDEP)
3 - 6 (AEZJKMQTFGXSI)(BNYCHPODULRWV)

Tabelle 4.2:

I	1	2	3	4	5	6	7	8	9	0	1	2	3
A	E	C	H	R	I	J	F	S	U	G	D	W	B
X	C	H	R	I	J	F	S	U	G	D	W	B	E
O	H	R	I	J	F	S	U	G	D	W	B	E	C
N	R	I	J	F	S	U	G	D	W	B	E	C	H
V	I	J	F	S	U	G	D	W	B	E	C	H	R
T	J	F	S	U	G	D	W	B	E	C	H	R	I
Q	F	S	U	G	D	W	B	E	C	H	R	I	J
L	S	U	G	D	W	B	E	C	H	R	I	J	F
Z	U	G	D	W	B	E	C	H	R	I	J	F	S
Y	G	D	W	B	E	C	H	R	I	J	F	S	U
M	D	W	B	E	C	H	R	I	J	F	S	U	G
K	W	B	E	C	H	R	I	J	F	S	U	G	D
P	B	E	C	H	R	I	J	F	S	U	G	D	W

II	A	R	F	C	J	W	T	S	L	K	V	Y	H
1	P	E	D	Q	O	X	M	U	G	N	Z	I	B
2	E	D	Q	O	X	M	U	G	N	Z	I	B	P
3	D	Q	O	X	M	U	G	N	Z	I	B	P	E
4	Q	O	X	M	U	G	N	Z	I	B	P	E	D
5	O	X	M	U	G	N	Z	I	B	P	E	D	Q
6	X	M	U	G	N	Z	I	B	P	E	D	Q	O
7	M	U	G	N	Z	I	B	P	E	D	Q	O	X
8	U	G	N	Z	I	B	P	E	D	Q	O	X	M
9	G	N	Z	I	B	P	E	D	Q	O	X	M	U
10	N	Z	I	B	P	E	D	Q	O	X	M	U	G
11	Z	I	B	P	E	D	Q	O	X	M	U	G	N
12	I	B	P	E	D	Q	O	X	M	U	G	N	Z
13	B	P	E	D	Q	O	X	M	U	G	N	Z	I

I	1	2	3	4	5	6	7	8	9	0	1	2	3
II													
1											X	X	
2													
3													
4							X						
5												X	
6													
7	X												
8										X			
9													
10					X								
11													
12													
13													

Tabelle 4.3:

I	1	2	3	4	5	6	7	8	9	0	1	2	3
A	E	C	H	R	I	J	F	S	U	G	D	W	B
X	C	H	R	I	J	F	S	U	G	D	W	B	E
O	H	R	I	J	F	S	U	G	D	W	B	E	C
N	R	I	J	F	S	U	G	D	W	B	E	C	H
V	I	J	F	S	U	G	D	W	B	E	C	H	R
T	J	F	S	U	G	D	W	B	E	C	H	R	I
Q	F	S	U	G	D	W	B	E	C	H	R	I	J
L	S	U	G	D	W	B	E	C	H	R	I	J	F
Z	U	G	D	W	B	E	C	H	R	I	J	F	S
Y	G	D	W	B	E	C	H	R	I	J	F	S	U
M	D	W	B	E	C	H	R	I	J	F	S	U	G
K	W	B	E	C	H	R	I	J	F	S	U	G	D
P	B	E	C	H	R	I	J	F	S	U	G	D	W

II	A	R	F	C	J	W	T	S	L	K	V	Y	H
1	P	E	D	Q	O	X	M	U	G	N	Z	I	B
2	E	D	Q	O	X	M	U	G	N	Z	I	B	P
3	D	Q	O	X	M	U	G	N	Z	I	B	P	E
4	Q	O	X	M	U	G	N	Z	I	B	P	E	D
5	O	X	M	U	G	N	Z	I	B	P	E	D	Q
6	X	M	U	G	N	Z	I	B	P	E	D	Q	O
7	M	U	G	N	Z	I	B	P	E	D	Q	O	X
8	U	G	N	Z	I	B	P	E	D	Q	O	X	M
9	G	N	Z	I	B	P	E	D	Q	O	X	M	U
10	N	Z	I	B	P	E	D	Q	O	X	M	U	G
11	Z	I	B	P	E	D	Q	O	X	M	U	G	N
12	I	B	P	E	D	Q	O	X	M	U	G	N	Z
13	B	P	E	D	Q	O	X	M	U	G	N	Z	I

I	1	2	3	4	5	6	7	8	9	0	1	2	3
II													
1													
2								1			3		
3					2								
4		3										1	2
5						1	3						
6	2	1											3
7				3			1				2		
8				1									
9						3							
10			1										
11													
12									2				
13										2			

Tabelle 4.4:

I	1	2	3	4	5	6	7	8	9	0	1	2	3
A	E	C	H	R	I	J	F	S	U	G	D	W	B
X	C	H	R	I	J	F	S	U	G	D	W	B	E
O	H	R	I	J	F	S	U	G	D	W	B	E	C
N	R	I	J	F	S	U	G	D	W	B	E	C	H
V	I	J	F	S	U	G	D	W	B	E	C	H	R
T	J	F	S	U	G	D	W	B	E	C	H	R	I
Q	F	S	U	G	D	W	B	E	C	H	R	I	J
L	S	U	G	D	W	B	E	C	H	R	I	J	F
Z	U	G	D	W	B	E	C	H	R	I	J	F	S
Y	G	D	W	B	E	C	H	R	I	J	F	S	U
M	D	W	B	E	C	H	R	I	J	F	S	U	G
K	W	B	E	C	H	R	I	J	F	S	U	G	D
P	B	E	C	H	R	I	J	F	S	U	G	D	W

III	A	E	Z	J	K	M	Q	T	F	G	X	S	I
1	V	W	R	L	U	D	O	P	H	C	Y	N	B
2	W	R	L	U	D	O	P	H	C	Y	N	B	V
3	R	L	U	D	O	P	H	C	Y	N	B	V	W
4	L	U	D	O	P	H	C	Y	N	B	V	W	R
5	U	D	O	P	H	C	Y	N	B	V	W	R	L
6	D	O	P	H	C	Y	N	B	V	W	R	L	U
7	O	P	H	C	Y	N	B	V	W	R	L	U	D
8	P	H	C	Y	N	B	V	W	R	L	U	D	O
9	H	C	Y	N	B	V	W	R	L	U	D	O	P
10	C	Y	N	B	V	W	R	L	U	D	O	P	H
11	Y	N	B	V	W	R	L	U	D	O	P	H	C
12	N	B	V	W	R	L	U	D	O	P	H	C	Y
13	B	V	W	R	L	U	D	O	P	H	C	Y	N

I III	1	2	3	4	5	6	7	8	9	0	1	2	3
1									X				
2				X					X				
3													
4													
5			X										
6													
7													
8													
9						X							
10													
11													
12													X
13					X								

Tabelle 4.5:

Tabelle 4.1 gibt das Material vor, mit dem das Verfahren beispielhaft erläutert wird, die Indikatoren sind in Tabelle 4.2 alphabetisch geordnet. Tabelle 4.3 erläutert das Verfahren für die Stufen *AD* (I) und *BE* (II). Der erste Zyklus von *AD* ist über der Matrix senkrecht geschrieben, der zweite waagerecht (umgekehrt und zeilenweise verschoben). Entsprechendes gilt für die Zyklen von *BE*. Jedes Matrixfeld repräsentiert eine Stellung des zweiten Zyklus von *AD* bzw. *BE*. Beim ersten Indikator `(AGPXUO)` muss ausgeschlossen werden, dass `A` und `E` zum selben Textschlüssel-Buchstaben gehören. Unter Anwendung der Sätze von Kap. 3.1.2.1 werden die einzelnen möglichen Paare von Klar- und Geheimtext-Buchstaben für jeden Indikator durchgetestet.

> Im Beispiel: Zu `A` könnte `C` als Klartext-Geheimtext-Partner gehören, es wäre aber auch ein `EC`-Paar möglich (in Spalte `C` und Zeile 12), also muss das Feld (12,2) der Matrix ausgeschlossen werden. Ebenso führt die Annahme `AH` zum Ausschluss des Feldes (3,3), `AR` schliesst (1,4) aus usw. Dies mit allen Indikatoren durchgeprüft lässt die angekreuzten Matrixfelder als möglich offen, d.h. die Spalten 1, 5, 7, 10, 11 und 12 ergeben für den zweiten Zyklus von `AD` mögliche Stellungen. Wenn das gleiche Verfahren mit `AD` und `CF` durchgeführt wird (Tabelle 4.5), erhält man als mögliche Stellungen für den zweiten Zyklus von `AD` 3, 4, 5, 6, 8 und 9.

Die Zahl 1 in Tabelle 4.4 bezieht sich auf den zweiten Indikator der Tabelle 4.1 `(AGPXUO)`, die 2 auf den sechsten `(AKTXVF)` und die 3 auf den vierzehnten `(DEVGPB)`. Für jeden Indikator werden die möglichen Paare von Klar- und Geheimbuchstaben durchgetestet. Im Beispiel: Zu `A` könnte `C` als Klartext-Geheimtext-Partner gehören, es wäre aber auch ein `GC` - Paar möglich (in Spalte `C` und Zeile 6), also muss das Feld (6,2) der Matrix ausgeschlossen werden. Ebenso führt die Annahme `(AH)` zum Ausschluss des Feldes `(10,3)`, `(AR)` schliesst (8,4) aus usw. Im Falle des Indikators `(AKTXVF)` müssen alle Fälle ausgeschlossen werden, in denen in Zeile `A` von Walze I und Spalte `K` von Walze II gleiche Buchstaben zu finden sind. Im dritten Falle (`DEVGPB`) werden alle Felder markiert, für die beim Auftreten des ersten Indikatorbuchstabens in Walze I der zugehörige Zeilenbuchstabe in Walze II als Spaltenbuchstabe auftritt und der zweite Indiktorbuchstabe in dieser Spalte zu finden ist.

Dies mit allen Indikatoren durchgeprüft lässt die in der Tabelle 4.3 als angekreuzt markierten Matrixfelder als möglich erscheinen, d.h. die Spalten 1, 5, 7, 10, 11 und 12 ergeben für den zweiten Zyklus von AD mögliche Stellungen. Wenn das gleiche Verfahren mit AD und CF durchgeführt wird (Tabelle 4.5), erhält man als mögliche Stellungen für den zweiten Zyklus von AD 3, 4, 5, 6, 8 , 9 und 13. Beiden Verfahrensstufen gemeinsam ist für den zweiten Zyklus von AD die Spalte 5. Eindeutig ergibt sich daraus für A:

$$A = \texttt{(ai)(xj)(of)(ns)(vu)(tg)(qd)(lw)(zb)(ye)(mc)(kh)(pr)}$$

Daraus folgt die Spalte 10 für B und schliesslich Spalte 13 (In Tabelle 4.4, Walze II) für C. Damit sind aber auch die Produkte D bis F bekannt. Hier zeigt sich, dass jede starre Regel („Kein Buchstabe doppelt“) immer eine Schwäche jedes Schlüsselsystems darstellt.

Man könnte nun mit den Klartext/Geheimtext-Paaren der Spruchschlüssel und den dazugehörigen Indikatoren alle Möglichkeiten der Verdrahtungsvarianten durchprobieren, um festzustellen, für welche Kombination aus den Spruchschlüsseln die Indikatoren entstehen. Dabei stellte man aber fest, dass jede Kombination die Bedingung erfüllen könnte, aber jeweils mit einer anderen Verdrahtung der Umkehrwalze !

DIE UMKEHRWALZE IST ABER EINE INVARIANTE IM CHIFFRIERUNGSSYSTEM !

Aus dieser Tatsache ergab sich eine Methode, die Verdrahtung der Chiffrierwalzen zweifelsfrei festzustellen. Die im folgenden dargestellte Herleitung bezieht sich auf die spätere Umkehrwalze `B`. REJEWSKI hat natürlich die damalige Walze `A` bestimmt. Ausgehend von zwei Tagesschlüsseln aus zwei verschiedenen Quartalen, also mit verschiedenen Walzenlagen, wurden zu diesen Tagesschlüsseln gehörende Paare für die Klargruppen `aaaaaa, bbbbbb, ... , zzzzzz` mit den dazugehörigen Geheimgruppen, die aus den Indikatoren gebildet werden konnten, benutzt. Man musste nur solche Tage heranziehen, für die man alle Spruchschlüssel ermittelt hatte. Legte man nun eine angenommene Kombination von Verdrahtungsvarianten mit der Walzenlage des ersten Quartals zugrunde, so erhielt man eine Verdrahtung der Umkehrwalze, die sich i.a. im Widerspruch befand zur entsprechend mit derselben Kombination bestimmten Verdrahtung der Umkehrwalze im zweiten Quartal. Damit war die angenommene Kombination von Verdrahtungsvarianten auszuschliessen. Eine Schwierigkeit schien zunächst noch bei der Walze zu liegen, für die noch kein Zusammenhang der Verdrahtungsvarianten mit der Anfangsstellung bekannt war. Man kannte aber wohl den Abstand der beiden Anfangsstellungen (erstes Quartal / zweites Quartal) voneinander und dementsprechend die relative Verschiebung der beiden Stellungen. (Vgl. Tabellen A.7 bis A.10 im Anhang A)

Nun musste geprüft werden, für welche Kombination von Verdrahtungsvarianten bezüglich der Umkehrwalze kein Widerspruch auftrat.

Als vereinfachtes Beispiel sind folgende Grunddaten angenommen:

1. Quartal	:	Walzenlage	: III II I
		Ringstellung	: A A A
		Grundstellung	: A O A
2. Quartal	:	Walzenlage	: I II III
		Ringstellung	: A A A
		Grundstellung	: A O A

Da im ersten Quartal die erste Walze die Nr. I hat, sind für diese die Verdrahtungsvarianten bekannt, ebenso die aus dem zweiten Quartal für die Walze Nr. III. Für die mittlere Walze liegt aus einem zurückliegenden Quartal nur ein Ausdruck für das in Tabellen A.7 bis A.10 definierte H vor, der aber nicht einer Grundstellung dieser Walze zugeordnet werden kann. Mit den zu diesen verschiedenen H gehörenden eventuellen Verdrahtungen wurde nun probiert, welche Kombination für beide Quartale widerspruchsfrei eine Umkehrwalzen-Konfiguration erlaubte.

Wie aus Tabelle 4.6 zu sehen ist, reduzieren sich die 26^4 Fälle auf nur 26 mögliche Kombinationen. (Aus Gründen der Vereinfachung sind nur die ersten vier von 26 Ergebnissen wiedergegeben.) Dabei war es noch nicht einmal nötig, die Gesamtheit durchzuproben; nach wenigen Versuchen war das Schema, wie Tabelle 4.6 zeigt, klar zu erkennen.

Ringstellung: AAA , Grundstellung: A O A; Walzenlage: 3 2 1

	Erfolg Nr. 1		
Schnelle Walze	(Variante Nr. 4)	:	DJLEKFCPUYMSNVXGWTROZHAQBI
Mittelwalze	(Variante Nr. 1)	:	JDKSIRUXBLHWTMCQGZNPYFVOEA
Letzte Walze	(Variante Nr. 1)	:	ACEGIKBOQSWUYMXDHVFZJLTRPN
Umkehrwalze		:	QTGPRKCOWMFNJLHDAEYBVUIZSX
	Erfolg Nr. 2		
Schnelle Walze	(Variante Nr. 5)	:	EKMFLGDQVZNTOWYHXUSPAIBRCJ
Mittelwalze	(Variante Nr. 1)	:	AJDKSIRUXBLHWTMCQGZNPYFVOE
Letzte Walze	(Variante Nr. 2)	:	BDFHJLCPRTXVZNYEIWGAKMUSQO
Umkehrwalze		:	YRUHQSLDPXNGOKMIEBFZCWVJAT
	Erfolg Nr. 3		
Schnelle Walze	(Variante Nr. 6)	:	FLNGMHERWAOUPXZIYVTQBJCSDK
Mittelwalze	(Variante Nr. 1)	:	EAJDKSIRUXBLHWTMCQGZNPYFVO
Letzte Walze	(Variante Nr. 3)	:	CEGIKMDQSUYWAOZFJXHBLNVTRP
Umkehrwalze		:	UZSVIRTMEQYOHPLNJFCGADXWKB
	Erfolg Nr. 4		
Schnelle Walze	(Variante Nr. 7)	:	GMOHNIFSXBPVQYAJZWURCKDTEL
Mittelwalze	(Variante Nr. 1)	:	OEAJDKSIRUXBLHWTMCQGZNPYFV
Letzte Walze	(Variante Nr. 4)	:	DFHJLNERTVZXBPAGKYICMOWUSQ
Umkehrwalze		:	CVATWJSUNFRZPIQMOKGDHBEYXL

Tabelle 4.6:

Gemeinsam ist diesen Restmöglichkeiten im hier gezeigten Beispiel die Variante Nr. 1 der Walze Nr. II. Eine erneute Probe mit derselben Logik aber unter Verwendung von anderen Grundstellungen und mit Beschränkung auf die Variante Nr. 1 bei der Walze Nr. II liefert dann eine andere Mannigfaltigkeit von 26 möglichen Kombinationen. Der Durchschnitt beider Mengen ist die gesuchte einzige Möglichkeit der Verdrahtung der drei Walzen und der Umkehrwalze - hier Umkehrwalze B (Tabelle 4.7).

Ermittlung der Verdrahtung der Walzen
Ringstellung: `AAA` , Grundstellung: `A O A`; Walzenlage: 3 2 1

Schnelle Walze	(Variante Nr. 5)	:	`EKMFLGDQVZNTOWYHXUSPAIBRCJ`
Mittelwalze	(Variante Nr. 1)	:	`AJDKSIRUXBLHWTMCQGZNPYFVOE`
Letzte Walze	(Variante Nr. 2)	:	`BDFHJLCPRTXVZNYEIWGAKMUSQO`
Umkehrwalze		:	`YRUHQSLDPXNGOKMIEBFZCWVJAT`

Tabelle 4.7:

Somit war das Ziel erreicht:

Die Verdrahtungen der drei Walzen I, II und III der ENIGMA waren erkannt. (Siehe S.6)

Es blieb noch die Frage offen, bei welchen Schaltstellen die jeweils folgenden Walzen weiterrückten. Die Antwort war allerdings mit den in zwei Quartalen vorliegenden Sprüchen und ihrer Dechiffrierung mit Hilfe bekannter Einstellungen der Walzen und der Ringe mit den nunmehr bekannten Walzen leicht zu finden: An der Stelle, von der ein dechiffrierter Spruch in eine sinnlose Buchstabenfolge überging, hatte mindestens eine Folgewalze weitergeschaltet. Damit war die zugehörige Ringstellung als Schaltstelle der Walze erkannt.

Nun war der Weg frei für den Nachbau der ENIGMA, der dann auch von der Firma AVA[5] bewältigt wurde.

4.2 Tagesschlüssel

4.2.1 Rasterverfahren

Von diesem Moment an änderte sich die Zielrichtung der Arbeit von REJEWSKI und seinen Mitarbeitern, die ihm dann zur Verfügung standen: Es galt nun, die jeweiligen Tagesschlüssel zu ermitteln mit dem Ziel, möglichst viele (im Idealfalle alle) Sprüche eines Tages „lesen“ (d.h. dechiffrieren) zu können.
Beim Dechiffrieren der Sprüche aus den beiden Quartalen, zu denen ihnen die Schlüsselunterlagen zur Verfügung gestanden hatten, erwuchs dem polnischen Team über den reinen punktuellen Inhalt jedes einzelnen Spruchs hinaus eine Fülle von weiteren Erfahrungen. Von diesen ist auch in den Veröffentlichungen die Rede: z.B. `/a n x/` als Spruchanfang, Namen von Kommandeuren (hier waren die bis 1933 alljährlich veröffentlichten Ranglisten aller deutschen Berufsoffiziere hilfreich), Standorte, Truppengliederung u. dgl. Man kann wohl davon ausgehen, dass solches Material bei den Versuchen, Klartext in den Sprüchen auszumachen, so intensiv genutzt worden ist, wie es später auch auf britischer Seite geschehen ist.
Im folgenden wurden für die Simulation des polnischen Vorgehens jeweils nach dem Zufallsprinzip ausgewählt: Walzenanordnung, Ringstellung, Grundstellung und für jede Tageseinstellung 100 Spruchschlüssel. Mit diesem Material ist dann versucht worden, die einzelnen Schritte des polnischen Teams um REJEWSKI nachzuvollziehen. In den Anlagen ist zur Kontrolle und als Vergleichsmöglichkeit für den Leser diese zufällig entstandene Einstellung mit angegeben.
Die Fussnoten geben bei REJEWSKI der Kürze halber nur eine Quelle an. Dieselben Inhalte finden sich auch in anderen Aussagen von REJEWSKI bzw. Veröffentlichungen anderer Autoren, die sich auf REJEWSKI stützen. Abweichende Darstellungen sind angeführt. Weiter oben ist bereits beschrieben, wie aus der Tagescharakteristik die einzelnen Permutationen $A \dots F$ für die ersten sechs Buchstaben eines Geheimtextes erhalten werden. Diese Länge entsprach der Länge des Indikators, der das Ergebnis der Chiffrierung des verdoppelten jeweiligen Spruchschlüssels war.

[5] AVA Rundfunkgerätebaugesellschaft, Wytwórnia Radiotechnicza AVA

Hier soll zunächst wieder die Voraussetzung gemacht werden, dass sich während dieser ersten sechs Chiffrierungsschritte die zweite (und entsprechend auch die dritte) Walze nicht bewegt. Der erste Schritt war die Bestimmung der Tagescharakteristik, wobei hier davon ausgegangen werden soll, dass diese auch vollständig gelungen sein soll, d.h. die Zyklenprodukte AD, BE und CF liegen vollständig vor. Anfangs war ja die Überführung der Zyklenprodukte in die einzelnen Zweierzyklen $A \ldots F$, die die Chiffrate der ersten sechs Buchstaben darstellten, erleichtert worden durch die wiederholte Verwendung bevorzugter Spruchschlüssel wie aaa, bbb, xxx, Folgen benachbarter Tasten im Tastenfeld der ENIGMA (z.B. wer, tgb, ...). Wenn dann noch in der Tagescharakteristik Zyklen mit geringer Gliederzahl auftraten, war die Umwandlung in die Zweierzyklen $A \ldots F$ i.a. ohne grosse Schwierigkeit möglich gewesen. Damit waren auch die zu den einzelnen Indikatoren gehörenden Spruchschlüssel bekannt. Bis etwa Mitte 1933 galten diese günstigen Umstände, danach war die Benutzung von drei gleichen Buchstaben für die Spruchschlüssel (die vom Funker der Absendestelle selbst gewählt wurden) verboten. Nach der Feststellung der einzelnen Zweierzyklen $A \ldots F$ war es möglich, die Gleichungen von Seite 60 mit dem Kern Q - der fiktiven Umkehrwalze -

$$Q = R_2 R_3 K R_3{}^{-1} R_2{}^{-1}$$

weiter zu bearbeiten.[6]

Die Permutation S (Stecker) veränderte nur 12 Buchstaben, sodass immerhin 14 ungeändert blieben. Zur Vereinfachung sei hier zunächst angenommen, dass k e i n e Stecker verwendet wurden, also S die identische Abbildung sei. Eine einfache Umformung führte zu

$$\begin{array}{lcl} Q & = & P R_1{}^{-1} P^{-1} A P R_1 P^{-1} \\ Q & = & P^2 R_1{}^{-1} P^{-2} B P^2 R_1 P^{-2} \\ \ldots & & \\ Q & = & P^6 R_1{}^{-1} P^{-6} F P^6 R_1 P^{-6} \end{array}$$

Die Verdrahtung von R_1 war bekannt, nicht aber ihre Anfangsstellung. Um dies in Rechnung zu stellen, musste für P der Faktor P^x eingeführt werden, sodass das System nun lautete

$$\begin{array}{lcl} Q & = & P^x R_1{}^{-1} P^{-x} A P^x R_1 P^{-x} \\ Q & = & P^{x+1} R_1{}^{-1} P^{-x-1} B P^{x+1} R_1 P^{-x-1} \\ \ldots & & \\ Q & = & P^{x+5} R_1{}^{-1} P^{-x-5} F P^{x+5} R_1 P^{-x-5} \end{array}$$

Für einen bestimmten Wert x aus der Menge $(1 \ldots 26)$ mussten die berechneten linken Seiten Q aller sechs Zeilen übereinstimmen, sodass damit die Anfangsstellung der Eingangswalze R_1 zu finden war. REJEWSKI fand ein Verfahren, diese Berechnung gewissermassen zu automatisieren : Das Rasterverfahren (Metoda „rusztu"). Dazu schrieb er für jede Walze als Eingangswalze eine Tabelle mit den Eintragungen der Permutationsprodukte

$$R_1,\ P R_1 P^{-1},\ P^2 R_1 P^{-2},\ \cdots,\ P^{25} R_1 P^{-25},\ R_1,\ P R_1 P^{-1},\ \cdots,\ P^4 R_1 P^{-4}$$

untereinander, also 31 Zeilen. Darüber legte er ein mit Schlitzen versehenes Blatt, das das Alphabet und die aus der Charakteristik gewonnenen Zweierzyklen $A \ldots F$ enthielt[7]. Dieses Blatt wurde so lange vertikal verschoben, bis für Q in allen sechs Zeilen der gleiche Transposition erschien. In Tabelle 4.8 ist das Prinzip für eine „erfolgreiche" Stellung gezeigt (zur Verdeutlichung ist ein Fall ohne Stecker angenommen).

[6] REJEWSKI b), S. 254

[7] GARLINSKI beschreibt S. 202 die Rasterblätter umgekehrt: Auf dem geschlitzten Blatt die Permutationen, auf dem darunterliegenden die $A \ldots F$

Eingangswalze Nr. 1
Anfangsstellung : A

			A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Exponent	:	1	j	l	e	k	f	c	p	u	y	m	s	n	v	x	g	w	t	r	o	z	h	a	q	b	i	d
A			F	W	P	O	V	A	Y	M	L	R	N	I	H	K	D	C	U	J	X	Z	Q	E	B	S	G	T
			A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Exponent	:	2	k	d	j	e	b	o	t	x	l	r	m	u	w	f	v	s	q	n	y	g	z	p	a	h	c	i
B			T	U	Y	M	F	E	X	P	Q	K	J	O	D	W	L	H	I	S	R	A	B	Z	N	G	C	V
			A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Exponent	:	3	c	i	d	a	n	s	w	k	q	l	t	v	e	u	r	p	m	x	f	y	o	z	g	b	h	j
C			Z	P	V	S	T	R	M	W	J	I	Y	N	G	L	Q	B	O	F	D	E	X	C	H	U	K	A
			A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Exponent	:	4	h	c	z	m	r	v	j	p	k	s	u	d	t	q	o	l	w	e	x	n	y	f	a	g	i	b
D			M	G	L	E	D	K	B	Y	X	S	F	C	A	P	Z	N	R	Q	J	U	T	W	V	I	H	O
			A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Exponent	:	5	b	y	l	q	u	i	o	j	r	t	c	s	p	n	k	v	d	w	m	x	e	z	f	h	a	g
E			G	N	D	C	P	M	A	K	S	X	H	T	F	B	Z	E	V	U	I	L	R	Q	Y	J	W	O
			A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Exponent	:	6	x	k	p	t	h	n	i	q	s	b	r	o	m	j	u	c	v	l	w	d	y	e	g	z	f	a
F			I	W	G	E	D	U	C	R	A	L	M	J	K	P	Q	N	O	H	V	X	F	S	B	T	Z	Y

Tabelle 4.8:

Erläuterung zu Tabelle 4.8:
Grosse Buchstaben sollen die Daten auf dem geschlitzten Papier darstellen, in kleinen Buchstaben sind die Produkte $P^x R_1 P^{-x}$ geschrieben. Geht man von `a` zum darunterstehenden Buchstaben (bei Exponent 01: E) und von diesem im Alphabet oben wieder in die Mitte, findet man den zu `a` gehörigen zugeordneten Buchstaben von Q (hier: `f`). Dies gilt für alle sechs Fälle. Beim Ausgangsbuchstaben `b` erhält man entsprechend `o` usw.

Mit Steckerpaaren konnte es aber nicht mehr vorkommen, dass die sechs Ausdrücke für Q übereinstimmten. Dann musste man suchen, wo auffällige Häufungen von gleichen Buchstaben in den verschiedenen Spalten zu finden waren. Bei ungünstiger Lage der Steckerverbindungen konnte das sehr schwierig sein. Für die folgenden Arbeitsschritte musste man dann die einzelnen Möglichkeiten durchprobieren. In Tabelle 4.9 ist ein solcher Fall mit sechs Steckerpaaren gezeigt, an dem demonstriert werden kann, wie hier bereits - bei günstigen Verhältnissen - die Steckerstellung gefunden werden konnte.

Erläuterung zu Tabelle 4.9:
Offenbar muss beim Exponenten 01 in QA wie bei fast allen anderen gelten: `a` $\mapsto$ `f`. Das bedeutet `a` $\mapsto$`U`, aber `E` $\mapsto$ `f`, also müssen `E` und `U` miteinander vertauscht werden, was auch die Vertauschung von `Q` und `V` nach sich zieht. Weiter (in QA): `m` $\mapsto$ `r`, also `m` $\mapsto$ `A`, aber `R` $\mapsto$ `r`, daher müssen `A` und `R` miteinander vertauscht werden, was zur Vertauschung von `C` und `J` führt, usw. Wenn durch solche Vertauschungen erreicht worden ist, dass alle $QA \ldots QF$ zueinander gleich sind, (es erfordert Probieren, hierbei die richtigen Buchstaben zu finden), dann erkennt man durch Vergleich der Vertauschungen in jeder Zeile die Steckerstellungen. (U.U. muss man Zwischenstufen ausschalten, z.B. führen `(CJ)` und `(JF)` zu `(CF)`)[8]. In dem hier dargestellten Beispiel ergeben sich die Steckerstellungen

`(AR) (CF) (EU) (GL) (MZ) (PT)`

[8]REJEWSKI b), S.258

Eingangswalze Nr. 1
Anfangsstellung : A

			A	B	C	D	$\underline{E}$	F	G	H	I	J	K	L	M	N	O	P	Q	$\underline{R}$	S	T	U	V	W	X	Y	Z
Exponent	:	1	j	l	e	k	$\underline{f}$	c	p	u	y	$\underline{m}$	s	n	v	x	g	w	t	r	o	z	h	$\underline{a}$	q	b	i	d
A			J	W	R	O	Q	T	I	Z	G	$\underline{A}$	N	Y	P	K	D	M	E	C	X	F	V	$\underline{U}$	B	S	L	H
			A	B	C	D	E	F	G	H	I	J	K	L	M	$\underline{N}$	O	P	Q	R	S	T	U	V	W	X	Y	Z
Exponent	:	2	k	d	j	e	b	o	t	x	l	r	m	u	w	$\underline{f}$	v	s	q	n	y	g	z	p	$\underline{a}$	h	c	i
B			S	E	U	Z	B	Y	O	T	Q	K	J	X	V	W	G	R	I	P	A	H	C	M	$\underline{N}$	L	F	D
			A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	$\underline{S}$	T	U	V	W	X	Y	Z
Exponent	:	3	c	i	d	$\underline{a}$	n	s	w	k	q	l	t	v	e	u	r	p	m	x	$\underline{f}$	y	o	z	g	b	h	j
C			C	T	A	$\underline{S}$	X	V	N	W	J	I	Y	Z	R	G	Q	U	O	M	D	B	P	F	H	E	K	L
			A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	$\underline{V}$	W	X	Y	Z
Exponent	:	4	h	c	z	m	r	v	j	p	k	s	u	d	t	q	o	l	w	e	x	n	y	$\underline{f}$	$\underline{a}$	g	i	b
D			Q	L	K	U	P	G	F	Y	X	S	C	B	O	T	M	E	A	Z	J	N	D	W	$\underline{V}$	I	H	R
			A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	$\underline{W}$	X	Y	Z
Exponent	:	5	b	y	l	q	u	i	o	j	r	t	c	s	p	n	k	v	d	w	m	x	e	z	$\underline{f}$	h	$\underline{a}$	g
E			E	N	Z	F	A	D	P	K	S	X	H	R	O	B	M	G	V	L	I	U	T	Q	Y	J	$\underline{W}$	C
			A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Exponent	:	6	x	k	p	t	h	n	i	q	s	b	r	o	m	j	u	c	v	l	w	d	y	e	g	z	f	a
F			H	W	E	U	C	L	J	A	R	G	Z	F	Y	T	Q	X	O	I	V	N	D	S	B	P	M	K

Tabelle 4.9:

Dieses Rasterverfahren, das erhebliche Konzentration erfordert und sehr zeitaufwendig ist, wenn es von Hand versucht wird, lieferte jedoch als Ergebnis die Identifizierung der ersten Walze, falls dies nicht schon vorher geschehen konnte, und ihre Anfangsstellung (bei gedachter Ringstellung A). Es blieben noch die entsprechenden Aussagen für die restlichen beiden Walzen.

4.2.1.1 Katalog.

REJEWSKI blieb zunächst nichts anderes übrig, als alle 676 möglichen Stellungen der anderen beiden Walzen durchzuprobieren, bis er beim Eintippen der Buchstaben des Indikators als Ergebnis den verdoppelten Spruchschlüssel erhielt. (Es konnte dabei vorkommen, dass dabei das Rücken der mittleren Walze vorausgesetzt werden musste, was den Rückschluss auf die Ringstellung der Eingangswalze mit sich brachte). REJEWSKI erstellte zur Beschleunigung des eben geschilderten Verfahrens einen Katalog mit allen Permutationen

$$Q = R_2 R_3 K {R_3}^{-1} {R_2}^{-1}$$

sodass nach den Ergebnissen für die Eingangswalze einfaches Nachschlagen im Katalog die Reihenfolge und die Anfangsstellungen der restlichen Walzen lieferte (immer bezogen auf die Ringstellung AAA). Weil aber ein Teil des gefundenen Ausdruckes für Q durch die Stecker beeinflusst sein musste, konnten für dieses Suchen im Katalog nur ausgewählte Buchstabenpaare verwendet werden, das hiess wiederum: Probieren !

Hier soll noch eine Abweichung vom eben beschriebenen Normalfall angeführt werden, die zwar zu Komplikationen geführt hat, die jedoch überwunden werden konnten: In Tabelle 4.11 sind die für einen Tag aufgefangenen Indikatoren und die zugehörige Tagescharakteristik angegeben.
Angenommen, das Rasterverfahren mit anschliessender Katalogsuche führt (bei angenommener Ringstellung AAA) zur Anfangsstellung HLL der Walzen (in der Schreibweise

steht, wie immer, die erste Walze rechts). Die damit aufgestellte Charakteristik ist in Tabelle 4.10 gezeigt.

Simulation mit Walzenanordnung: 312; Ringstellung: AAO ; Grundstellung: HLL; Umkehrwalze B; Keine Stecker !
Die Zyklenschreibweise für die Permutationen für die Indikatorstellen

AD	(AIQUYE)(BRJHPD)(FVMLZX)(KOWTSN)(C)(G)
BE	(AXHNKPQFYZ)(BGROUMTIEJ)(DW)(LS)(C)(V)
CF	(AXGYHINDRJVM)(BWPEKTQLSUOF)(C)(Z)

Tabelle 4.10:

Verfahrenssimulation.
Walzenanordnung: 312; Umkehrwalze B; Ringstellung: INO ; Grundstellung: PYZ;
Steckverbindungen: (UF) (RM) (WX) (JI) (NQ) (BA); 100 Indikatoren

ADQMXD	AVEMVK	AXPMDE	BOXJFP	BPJJNQ
CGHCMJ	CMTCON	CQACKX	DNJAUQ	DORAFB
DPTANN	DRWATG	DXBADW	ECFBCO	ECXBCP
EJYBEH	EKRBPB	ENOBUU	FIPYAE	FVWYVG
FYCYZC	FZEYBK	FZEYBK	FZEYBK	GBGGWY
GLMGSI	GMFGOO	GVLGVS	GVZGVZ	HISPAF
HWHPHJ	ICAHCX	IEVHIR	ILWHSG	ILWHSG
INZHUZ	IXNHDL	JMYNOH	JRCNTC	KFQORD
KIBOAW	KSWOLG	KXKODT	LEMZII	LPUZNA
LVRZVB	LXVZDR	LZBZBW	MNMIUI	NBMFWI
NBPFWE	NIQFAD	NXDFDM	NXDFDM	ORSXTF
PDZDXZ	PTCDJC	PXNDDL	PXNDDL	PXNDDL
PXNDDL	QSLKLS	QZQKBD	QZQKBD	RBJLWQ
RKOLPU	RQOLKU	SEDQIM	SGFQMO	SRSQTF
SWDQHM	THNSQL	THNSQL	TKPSPE	TZRSBB
UJGVEY	UJLVES	VEQRID	VOFRFO	VRYRTH
WBAUWX	WFQURD	WISUAF	WVDUVM	XADTGM
XADTGM	XHYTQH	XIQTAD	XLSTSF	XPTTNN
YBAEWX	YCHECJ	YCKECT	YCKECT	YHDEQM
YRWETG	ZIYWAH	ZUFWYO	ZWPWHE	ZXNWDL

Die Zyklenschreibweise der Permutationen lauten:

AD	(XTSQKO)(IHPDAM)(NFYEBJ)(ZWUVRL)(G)(C)
BE	(HQKPNUYZBW)(GMOFRTJEIA)(XD)(LS)(C)(V)
CF	(VRBWGYHJQDMI)(NLSFOUAXPEKT)(C)(Z)

Tabelle 4.11:

Wie man sieht, weicht sie in der Stufe Zeile CF von der tatsächlichen Tagescharakteristik ab. Daraus muss man schliessen, dass (entgegen der Anfangsannahme) die mittlere Walze vor der Chiffrierung des sechsten Buchstabens (und zwar nur dort) weitergerückt ist. Dieses Weiterrücken ist allerdings bei der Grundstellung HLL (und Ringstellung AAA) nicht möglich - die Eingangswalze ist Nr. II, sie schaltet die mittlere Walze bei E/F. Also müssen die durch den Tagesschlüssel gegebenen Ring- und Anfangsstellungen so beschaffen sein, dass sie das beobachtete Weiterrücken der mittleren Walze ermöglichen.

Die Anfangsstellung der ersten Walze muss somit Z gewesen sein, d.h. ihre Ringstellung war O. Die Probe mit Ringstellung AAO und Grundstellung HLZ führt nunmehr, wie Tabelle 4.12 zeigt, zu einer Charakteristik, die mit der Tagescharakteristik übereinstimmt. Die Steckerstellungen sind ablesbar.

Simulation mit Walzenanordnung: 312; Ringstellung: AAO ; Grundstellung: HLZ; Umkehrwalze B; Keine Stecker !
Die Zyklenschreibweise der Permutationen für die Indikatorstellen

1 - 4	(AIQUYE)(BRJHPD)(FVMLZX)(KOWTSN)(C)(G)
2 - 5	(AXHNKPQFYZ)(BGROUMTIEJ)(DW)(LS)(C)(V)
3 - 6	(AXGYHINDRJVM)(BWPEKTQLSUOF)(C)(Z)

Tabelle 4.12:

Die bisher beschriebenen Schritte waren u.U. auch möglich, wenn die Tagescharakteristik nur unvollständig vorlag. Das System der $QA \ldots QF$ war zwar dann ebenfalls unvollständig, aber manchmal reichte es aus, die Bestimmung des Tagesschlüssels durchzuführen. Bei DEAVOURS ist dafür ein Beispiel angegeben.[9] Die bisherige teilweise Bestimmung des Tagesschlüssels, die zur Dechiffrierung einiger Spruchschlüssel ausreichte, genügte aber nicht, alle Sprüche des Tages zu lesen. Soweit er schon bekannt war, waren damit zwar einzelne Spruchschlüssel bekannt, aber ein wesentliches Element des vollständigen Schlüssels, die Stellungen der Ringe, fehlte noch.
(Es sei daran erinnert, dass das oben geschilderte Verfahren eine Ringstellung von AAA voraussetzte.) Ohne die Kenntnis der Ringstellungen gelang auch der Versuch nicht, mit dem Spruchschlüssel einen Spruch zu entziffern. Notwendig für den weiteren Fortgang des Verfahrens war nun die Kenntnis von einem Stück Klartext. REJEWSKI hatte inzwischen bemerkt, dass etwa 20% der Sprüche des Heeres mit den drei Buchstaben /a n x/ begannen, wobei das x hier als Worttrenner diente[10]. Ausserdem waren ihm aus der Beobachtung des Verkehrs anschliessende Adressen, Namen, Schlussformeln u.dgl. bekannt. Er konnte nun also versuchen, mit dem vermuteten Spruchbeginn /a n x/ einen vorliegenden Geheimtext anzugehen. (Die Walzenanordnung konnte als bekannt vorausgesetzt werden.) Ausgehend vom Klartext und den inzwischen bekannten Steckerpositionen musste für die Eingangswalze eine Anfangsstellung vorausgesetzt werden (Exponent x). Ebenso, „rückwärts arbeitend" vom Geheimtext unter Berücksichtigung der Stecker und der rückwärts durchlaufenen ersten Walze erhielt man drei Zweierzyklen aus dem gesuchten Kern Q. Im oben beschriebenen Katalog musste dazu eine passende Stelle gesucht werden. Falls dies nicht zum Ende führte, musste der Exponent x geändert werden, bis der Erfolg sich einstellte. REJEWSKI gibt zu, dass dies eine sehr langwierige Prozedur war (Im Extremfall mussten 17576 Möglichkeiten durchgeprüft werden !), aber sie war wirksam. In Tabelle 4.13 ist für einen Spruch mit dem Beginn EDI[11] das Ergebnis dieser aufwendigen Prozedur dargestellt. Wie man sieht, gibt es hier mehrere Möglichkeiten der Korrespondenz zwischen /a n x/ und E D I . Alle diese Verfahren lieferten ja nicht notwendig vollständige und eindeutige Lösungen, sondern nur immer mit der Lösung kompatible Aussagen. Die Entscheidung, welche Möglichkeit die richtige war, musste durch einen Dechiffrierungsversuch erbracht werden. Die Ergebnisse sind in den Tabellen 4.14 und 4.15 zu sehen. (Die dritte Möglichkeit erweist sich ebenfalls als untauglich.)

[9] DEAVOURS, S. 28/30
[10] REJEWSKI b), S. 259
[11] Bezug: Walzenlage 312; Umk.-W.: B; Ringst.: VIM; Grundst.: JWS; Stecker: (EZ)(PR)(XT)(YV)(GL)(AS)

Simulation mit Walzenanordnung: 312; Ringstellung: AAA ; Umkehrwalze B
Steckverbindungen: (EZ) (PR) (XT) (YV) (GL) (AS);
Aus Indikator ermittelter Spruchschlüssel (Grundstellung): FFF
Unter der Annahme, dass der Spruch mit anx beginnt, gehört zum Spruchanfang EDI die
Anfangsstellung des Walzenkörpers : J W S
Dazu gehört die Ringstellung : V I M
Unter der Annahme, dass der Spruch mit anx beginnt, gehört zum Spruchanfang EDI die
Anfangsstellung des Walzenkörpers : M M S
Dazu gehört die Ringstellung : S S M
Unter der Annahme, dass der Spruch mit anx beginnt, gehört zum Spruchanfang EDI die
Anfangsstellung des Walzenkörpers : Q D O
Dazu gehört die Ringstellung : O B Q

Tabelle 4.13:

Simulation mit Walzenanordnung: 312; Ringstellung: VIM ; Grundstellung: FFF; Umkehrwalze B
Steckverbindungen: (EZ) (PR) (XT) (YV) (GL) (AS)

Geheimtext:	EDIIU	SPYZF	GIVUA	VWECJ	LABZA	GZQPT	JOHXI	TFSWZ	KACWX
Klartext:	anxko	mmand	antxv	ierte	sxkor	psxer	bitte	xnaeh	erexa
	WAFTK	FTUOK	PLQPD	RTKLF	LIDOB	BHHUV	YVCXY	UXVBC	JKBWZ
	ngabe	nxzur	xange	nomme	nenxl	agexm	anoev	erxse	ptemb
	UEGLX	RJSLN	PWSZW	UBRNT	JKDZB	RSBUN	KZSEU	DVPNX	RLHRZ
	erxwi	exwei	txist	xderx	einsa	tzxvo	nxpan	zerat	trapp
	WSFFC	OFNRG	AAMPK	QMTSB	ITXNG	NOTRC	SEEJK	ZDVQB	HLRDH
	enxsi	nnvol	lxsqn	eider	xkomm	andeu	rxinf	regtx	zehnx

Tabelle 4.14:

Simulation mit Walzenanordnung: 312; Ringstellung: SSM ; Grundstellung: FFF; Umkehrwalze B
Steckverbindungen: (EZ) (PR) (XT) (YV) (GL) (AS)

Geheimtext:	EDIIU	SPYZF	GIVUA	VWECJ	LABZA	GZQPT	JOHXI	TFSWZ	KACWX
Klartext:	anxdt	imjen	stqxk	fidhm	kodsr	tbubg	xdeoz	mvaqg	jswry
	WAFTK	FTUOK	PLQPD	RTKLF	LIDOB	BHHUV	YVCXY	UXVBC	JKBWZ
	ggwbr	nwhyx	tdyta	nglme	omlxg	ygbci	elksm	pffxq	xqyrx
	UEGLX	RJSLN	PWSZW	UBRNT	JKDZB	RSBUN	KZSEU	DVPNX	RLHRZ
	wqkgs	bbzdk	mbhju	skhsm	nsbty	lvjds	gumrg	prbpj	jtzed
	WSFFC	OFNRG	AAMPK	QMTSB	ITXNG	NOTRC	SEEJK	ZDVQB	HLRDH
	mbzay	xkluf	yrnmb	bqkgj	axols	pmcjo	cxlml	nbzeu	nwoqn

Tabelle 4.15:

Das Ergebnis ist nun eindeutig: Die Ringstellung ist V I M . Diese Aussage ergänzt auch die bisherige, unvollständige Ermittlung des Tagesschlüssels zur Aussage, dass die Grundstellung J W S lautet. Die Ringstellung gilt aber für alle Spruchschlüssel des Tages, sodass damit alle Sprüche des Tages lesbar sind. Im weiteren Verlauf, nachdem REJEWSKI zwei weitere Mitarbeiter - ZYGALSKI und RÓŻYCKI - sowie Hilfspersonal erhalten hatte, bestimmten die Hauptbeteiligten jeweils den Tagesschlüssel (der nun die Ringstellung einschloss), das Hilfspersonal dechiffrierte mit diesen Vorgaben nach Möglichkeit alle Sprüche des Tages. REJEWSKI erwähnt, dass er aus mathematische Überlegungen heraus Vereinfachungen bei der Suche nach dem Spruchschlüssel bei vorgegebenem Klartextfragment /a n x/ eingeführt hätte, die die Anzahl der durchzuprobierenden Möglichkeiten um etwa den Faktor 10 reduziert hätten. Er erinnerte sich aber weder an das, was er getan hatte, noch an das Wie oder die Begründungen dafür. Diese Seite seines Vorgehens soll hier nicht weiter verfolgt werden[12].

[12] REJEWSKI b), S. 260

Vergleich der Geheimtexte mit den Spruchschlüsseln (Grundstellungen)

```
NYE      ,      NYT
XOQJIDAFRCOJWNSBJVPNWIULWDBSRADPPCTUAMDIQREFIPKEME
...........PEIFVBOZKDMYTQCCFFUOHMMRYZXWHZBJHWVAVAN
BTXQOJXLMISKHUVDPUOQZVETETFDPUBTPMTXEYMHYAWAKIRMWZ
TKASRABIGQYJCFKMGCWSNIYKCWTKMPQBGRIQYKARZJGHNDPHVT
GWYSRVYBOOJHGYBBZPISDCDKSWNRAMVCIKTIXTVYEPTOMHERDH
PUTBILHMJEVXNZXVABLTQINVTMXECQSFBPGXZJGWVOGEREDWBR
FTRCLMMWXJEJWFKAVFKEDNCMXZUURBLJZGKRABACMC........
SSSJVHQSTGNSASVXOWWXUAVJMFTBQXSTWKITYVSLUD........
```

Walze I wurde als Eingangswalze angenommen:
0.00 % Übereinstimmungen werden gezählt.

```
XOQJIDAFRCOJWNSBJVPNWIULWDBSRADPPCTUAMDIQREFIPKEME
...........PEIFVBOZKDMYTQCCFFUOHMMRYZXWHZBJHWVAVAN
BTXQOJXLMISKHUVDPUOQZVETETFDPUBTPMTXEYMHYAWAKIRMWZ
TKASRABIGQYJCFKMGCWSNIYKCWTKMPQBGRIQYKARZJGHNDPHVT
GWYSRVYBOOJHGYBBZPISDCDKSWNRAMVCIKTIXTVYEPTOMHERDH
PUTBILHMJEVXNZXVABLTQINVTMXECQSFBPGXZJGWVOGEREDWBR
FTRCLMMWXJEJWFKAVFKEDNCMXZUURBLJZGKRABACMC........
SSSJVHQSTGNSASVXOWWXUAVJMFTBQXSTWKITYVSLUD........
```

Walze II wurde als Eingangswalze angenommen:
0.00 % Übereinstimmungen werden gezählt.

```
PEIFVBOZKDMYTQCCFFUOHMMRYZXWHZBJHWVAVANTKASRABIGQY
...............XOQJIDAFRCOJWNSBJVPNWIULWDBSRADPPCT
JCFKMGCWSNIYKCWTKMPQBGRIQYKARZJGHNDPHVTPUTBILHMJEV
UAMDIQREFIPKEMEBTXQOJXLMISKHUVDPUOQZVETETFDPUBTPMT
XNZXVABLTQINVTMXECQSFBPGXZJGWVOGEREDWBRSSSJVHQSTGN
XEYMHYAWAKIRMWZGWYSRVYBOOJHGYBBZPISDCDKSWNRAMVCIKT
SASVXOWWXUAVJMFTBQXSTWKITYVSLUDHRILYPNUAPMXBRFPWQM
IXTVYEPTOMHERDHFTRCLMMWXJEJWFKAVFKEDNCMXZUURBLJZGK
OSGRZMA...........................................
RABACMC...........................................
```

Walze III wurde als Eingangswalze angenommen:
8.33 % Übereinstimmungen werden gezählt.

```
LWJ      ,      LWT
RIUHMRMAJBUHVLNUKKUQUIZZTGFSSHTTMYYTNGNAYEBWKMBJUQ
................CFNXQCBRSXLYWMVNKPPJGLPVWJZCHNLDCX
FIUOCKZRXADXSLMULYADXRIQDVAELKRWVZWJPDDAKYPHBFGDRY
DAHSWVOOWMOJFZZWNSHXQMQSQNHNAWWINVZUMFPLFAWRBYZVQI
PYVCPTPXINFALJKUPOPQNHGJFZSVRXJXKNOGHZSCBYAQDOHCZC
TPNSXJHPSWTZSQPJDBQRYLJRYXXZIMPGUQKZYOAULYULGFYYBZ
OXHRHEQESZLSHNYVEIMYXESIDVCYDANKCKNDJZLXEE........
THWPKDRZIOLPZGSCICCMBJKINSXITPJHYOPGFAXMHA........
```

Walze I wurde als Eingangswalze angenommen:
2.27 % Übereinstimmungen werden gezählt.

```
CFNXQCBRSXLYWMVNKPPJGLPVWJZCHNLDCXDAHSWVOOWMOJFZZW
..........RIUHMRMAJBUHVLNUKKUQUIZZTGFSSHTTMYYTNGNA
NSHXQMQSQNHNAWWINVZUMFPLFAWRBYZVQITPNSXJHPSWTZSQPJ
YEBWKMBJUQFIUOCKZRXADXSLMULYADXRIQDVAELKRWVZWJPDDA
DBQRYLJRYXXZIMPGUQKZYOAULYULGFYYBZTHWPKDRZIOLPZGSC
KYPHBFGDRYPYVCPTPXINFALJKUPOPQNHGJFZSVRXJXKNOGHZSC
ICCMBJKINSXITPJHYOPGFAXMHAABGCFJQNVBZGFUPURWICSWBJ
BYAQDOHCZCOXHRHEQESZLSHNYVEIMYXESIDVCYDANKCKNDJZLX
EM................................................
EE................................................
```

Walze II wurde als Eingangswalze angenommen:
3.65 % Übereinstimmungen werden gezählt.

```
CFNXQCBRSXLYWMVNKPPJGLPVWJZCHNLDCXDAHSWVOOWMOJFZZW
..........RIUHMRMAJBUHVLNUKKUQUIZZTGFSSHTTMYYTNGNA
NSHXQMQSQNHNAWWINVZUMFPLFAWRBYZVQITPNSXJHPSWTZSQPJ
YEBWKMBJUQFIUOCKZRXADXSLMULYADXRIQDVAELKRWVZWJPDDA
DBQRYLJRYXXZIMPGUQKZYOAULYULGFYYBZTHWPKDRZIOLPZGSC
KYPHBFGDRYPYVCPTPXINFALJKUPOPQNHGJFZSVRXJXKNOGHZSC
ICCMBJKINSXITPJHYOPGFAXMHAABGCFJQNVBZGFUPURWICSWBJ
BYAQDOHCZCOXHRHEQESZLSHNYVEIMYXESIDVCYDANKCKNDJZLX
EM................................................
EM................................................
```

Walze III wurde als Eingangswalze angenommen:
3.65 % Übereinstimmungen werden gezählt.

Tabelle 4.16:

Uhrenmethode. RÓŻYCKI versuchte zur Identifizierung der Eingangswalze auch eine Methode, die die Eigenheiten der Sprache gegenüber zufällig aufeinander folgenden Buchstaben benutzte[13]. Er nannte sie die „metoda zegara, «clock-method»“ . Er benötigte dazu zwei Sprüche genügender Länge (i.a. reichten wohl etwa 200 Buchstaben), deren Spruchschlüssel sich nur im dritten Buchstaben unterschieden. Wenn man diese Sprüche, jeweils unter der Annahme, welche Walze als erste Walze diente, so untereinander schrieb, dass die Stellen, an denen die mittlere Walze weiterrückte, übereinanderstanden (die Versetzung der Sprüche musste also dem „Abstand“ der 3. Buchstaben der Spruchschlüssel entsprechen), dann musste einfaches Abzählen genügen, um festzustellen, ob die Anzahl der Übereinstimmungen sich sprachspezifisch abhob von der rein zufälligen Übereinstimmung. Der Grundgedanke für diese Versuche liegt darin, dass durch die Versetzung der Sprüche gleiche Geheimtext-Buchstaben, die sich untereinander finden lassen, auf gleiche Klarbuchstaben schliessen lassen[14]. In der Tabelle 4.16 sind zwei Beispiele vorgestellt. Die tatsächliche erste Walze ist in jedem der beiden Beispiele die Walze Nr. III.
Erläuterung zur Tabelle 4.16:
Die Spruchschlüssel sind `NYE` und `NYT`, der erste Buchstabe wird also von der ersten Walze in den Stellungen `F` bzw. `U` chiffriert. a) Bei der Annahme, die erste Walze sei Walze Nr. I, muss der zu `NYE` gehörende Spruch (`PEIFV...`) also so unter den zu `NYT` gehörenden geschrieben werden, dass beide bei `Q` die Mittelwalze weiterschalten, d.h. der obere hat einen „Vorlauf“ von 11 Stellen. b) Bei der Annahme, die erste Walze sei Walze Nr. II liegt die Schaltstelle dieser Walze bei `E`. Beim ersten Spruch wird also bereits der erste Buchstabe mit weitergeschalteter Mittelwalze chiffriert, dementsprechend muss die Stellung der beiden Sprüche zueinander wie im Falle a) sein. c) Die Annahme bzgl. der ersten Walze lautet nun: Nr. III. Die Schaltstelle ist bei `V`. Nun hat der erste Spruch als oberer einen Vorlauf von 15 Stellen.
Wie man an Tabelle 4.16 unten sieht, ist dieses Verfahren zur Identifizierung der Eingangswalze sehr unsicher. Umso mehr, wenn man bedenkt, dass im militärischen Funkverkehr „unsprachliche“ Abkürzungen sehr häufig verwendet werden. Offenbar hängt die „Schärfe“ dieses Kriteriums auch davon ab, wie die Stellungen der dritten Buchstaben der beiden Spruchschlüssel zur Schaltstelle der Eingangswalze liegen. Aus diesen Gründen scheint das Verfahren wohl zunächst keine grosse Bedeutung erlangt zu haben. Es wurde jedoch von den Briten zur Grundlage des sog. Banburismus gemacht. (Siehe Kap. 6.2.3.1.6, S. 152)

4.2.2 Zyklometer.

Ab Anfang 1936 wurde die Walzenanordnung nicht mehr, wie bisher, vierteljährlich festgelegt, sondern monatlich, ab Herbst 1936 sogar täglich. Dies bedeutete, dass schliesslich die gesamte Palette der Routinen täglich voll zu durchlaufen war. Bedeutend erschwert wurde die tägliche Dechiffrierungsarbeit aber neben dem zwischenzeitlichen Verbot, für die Spruchschlüssel gleiche Buchstaben oder Buchstabenfolgen der Schreibmaschine zu verwenden, ab 1. 10. 1936 dadurch, dass die Anzahl der Steckerpaare von sechs (konstant) auf fünf bis acht (täglich wechselnd) geändert wurde.
Das Team um REJEWSKI konzentrierte seine Aufmerksamkeit daher auf die steckerunabhängige Charakteristik. Mit einem Zusammenbau von zwei Walzensätzen, beim zweiten war die erste Walze um drei Stellen gegenüber der im ersten Satz versetzt, bestimmten sie die Charakteristiken für alle 6·26·26·26 Möglichkeiten der Einstellung der ENIGMA (bei Ringstellung `AAA`) und hielten die Ergebnisse in einer Kartei fest. Es genügte allerdings, nur die Längen der Zyklen zu registrieren. Sie nannten das Gerät ZYKLOMETER[15] Diese Arbeit dauerte etwa ein Jahr, dann war es aber nur noch nötig,

[13]REJEWSKI b), S. 260
[14]DEAVOURS/KRUH a), S. 112/113
[15]REJEWSKI b), S. 261

mit der Tagescharakteristik in die Kartei zu gehen und die entsprechenden Maschineneinstellungen zu entnehmen. Die Steckerstellungen erhielt man dann durch Vergleich mit der Tagescharakteristik. Im Beispiel von Tabelle 4.17, das relativ ungünstig ist (es gibt in der Charakteristik zu viele Zyklen der Länge 13), sind ausschnittweise einige der insgesamt 197 mit der Tagescharakteristik bezüglich der Zyklenlängen übereinstimmende Möglichkeiten von Walzenanordnung und Walzenstellung dargestellt. Aus diesen lässt sich durch Vergleich der inneren Struktur der Zyklen die einzig passende schnell herausfinden.

Alle Angaben sind bezogen auf die Walzenlage 312, Ringstellung `AAA`

Grundstellung `NBQ`; Referenzzyklen: Lfd. Nr 134

```
(BXEZGNWQL) (CSUKRTPDO) (AMI) (FYH) (J) (V)
(AKXVTRYLPDENJ) (BSGOIZFWHUQCM)
(ALVIMBFCTURSP) (DOZWJHXQGKENY)
```

Grundstellung `NVT`; Referenzzyklen: Lfd. Nr 135

```
(AMNBVRJLS) (DEUOQHGXW) (FKP) (IYZ) (C) (T)
(APBRXLSHNIDZM) (CQJFTGWVUKYOE)
(ADYJWKQOSMVBZ) (CPNRXFIUHEGTL)
```

Grundstellung `OOG`; Referenzzyklen: Lfd. Nr 136

```
(BLGQESNCY) (IJOTKWVRZ) (AHD) (FXU) (M) (P)
(AKZWYFLQBNDUS) (COPRHEMXJVGIT)
(ATPDUWFYCVGRJ) (BQNHISXLKOZEM)
```

Grundstellung `PCP`; Referenzzyklen: Lfd. Nr 137

```
(AMSXFGUHT) (BRVDWPKZC) (EYQ) (IOJ) (L) (N)
(ATYXJZSNLCVUP) (BDEROMKGIHFQW)
(ANUSTGDHJPOIC) (BZLWMERQXYVKF)
```

Grundstellung `PFB`; Referenzzyklen: Lfd. Nr 138

```
(APUMXCQVH) (BDZFJTSRG) (EIL) (KWY) (N) (O)
(ALITSHWZPFBQY) (CGEODVJMUNRKX)
(ASHUDOJICKZMR) (BNLYGXWQVTPFE)
```

Grundstellung `PQG`; Referenzzyklen: Lfd. Nr 139

```
(ABRIWHXSC) (EPZKOMYLT) (DNF) (GUJ) (Q) (V)
(ABENXKGTSWIQD) (CLZOMJRUVHFYP)
(AYVMCERNKTSUQ) (BXLFGPHWOZIDJ)
```

Tabelle 4.17:

Erläuterung zu Tabelle 4.17:

In dem zur Suche eingegebenen Zyklensystem[16]

Stufe AD: `(VBGLQZANC)(EIJOXKWYP)(DSH)(TUF)(M)(R)`
Stufe BE: `(WVFGQBNDUASKE)(RPHZMTJYLIXCO)`
Stufe CF: `(XRDUWFVCYLPJS)(NHIATGKOEZMBQ)`

werden folgende Tatsachen festgehalten:

1) Die Buchstaben der Einerzyklen sind in Stufe 2 - 5 im selben Zyklus im Abstand vier
2) In Stufe 3 - 6 sind sie in verschiedenen Zyklen.
3) Zwei Buchstaben eines Dreierzyklus `(DSH)` sind in Stufe 2 - 5 im selben Zyklus im Abstand 3
4) In Stufe 3 - 6 liegen sie im selben Zyklus im Abstand 10, bzw. drei
5) Der dritte Buchstabe ist im anderen Zyklus
6) Zwei Buchstaben des anderen Dreierzyklus `(TUF)` liegen in Stufe 2 - 5 im selben Zyklus im Abstand 6
7) In Sufe 3 - 6 liegen sie im selben Zyklus im Abstand zwei
8) Der dritte Buchstabe ist im anderen Zyklus

Diese Struktureigenschaften sind unabhängig von Steckerstellungen.

Beispielhaft ist an dem vorliegenden Ausschnitt aus der Menge der scheinbar gleich strukturierten Zyklensysteme das Verwerfen der nicht genau passenden zu sehen:

[16] siehe Fussnote S. 92

Nr. 134: Bedingung 6 nicht erfüllt,
Nr. 135: Bedingung 2 nicht erfüllt,
Nr. 136: alle Bedingungen sind erfüllt,
Nr. 137: Bedingung 8 nicht erfüllt,
Nr. 138: Bedingung 6 nicht erfüllt,
Nr. 139: Bedingung 2 nicht erfüllt.

Es ist deutlich, dass dieses Aussortieren ungeeigneter Strukturen recht schnell gehen kann. Von den 197 Möglichkeiten bleibt letzten Endes nur die lfd. Nr. 136 übrig. Der Vergleich mit der obigen Tagescharakteristik liefert die Steckerstellungen

`(EZ) (PR) (XT) (YV) (GL) (AS)`[17].

Tabelle 4.18 zeigt ein Beispiel, das mit günstigeren Vorgaben nur eine Lösung liefert. Es liege die Tagescharakteristik vor:

(Grundstellung BPH; Ringstellung UMY; Walzenstellung 312)

```
(AVXWBQUIOFLT) (CRMJZEYPGSHD) (K) (N)
(DEVPZ) (HRUXN) (AYQJ) (BWGM) (CFSL) (IKTO)
(ARSMLH) (GKVXQN) (TZCIF) (DEOUJ) (P) (B) (W) (Y)
```

Der Katalog liefert hier nur eine einzige Entsprechung.

Alle Angaben sind bezogen auf die Walzenstellung 312, Ringstellung AAA
Grundstellung HDJ; Referenzzyklen: Lfd. Nr. 1

```
(AWYVTQUENFZB) (CRMJLIXPGSHD) (K) (O)
(DIWPL) (HRUYO) (AXQJ) (BNEK) (CFSZ) (GMTV)
(ARSMZH) (GKWYQO) (BLCEF) (DINUJ) (P) (T) (V) (X)
```

Tabelle 4.18:

Ohne Schwierigkeiten sind die Steckerstellungen

`(NO)(IE)(YX)(LZ)(TB)(WV)`

ablesbar.
Dieser Katalog von Zyklensystemen führte also sehr schnell zur Reihenfolge der Walzen, ihren Anfangsstellungen und den Steckerstellungen. Selbst, wenn die mittlere Walze vor der Chiffrierung des sechsten Buchstabens weiterrückte (davon wurde nur die Stufe 3 - 6 des Zyklensystems beeinflusst), war i.a. der Katalog noch brauchbar, indem man nur die Übereinstimmungen in den Stufen 1 - 4 und 2 - 5 suchte. Man musste dann allerdings in Kauf nehmen, dass sehr viel mehr kompatible Strukturen auftraten. Dafür erhielt man aber den Vorteil, dass die Tatsache des Rückens vor dem sechsten Buchstaben sofort die Ringstellung der ersten Walze lieferte ! (Diese Kenntnis wiederum hatte zur Folge, dass bei der Suche nach dem Spruchschlüssel mit dem `/a n x/` -Anfang nur noch 676 Versuche nötig waren.)
Es war kein Wunder, dass bei einer Untersuchung der Effektivität Anfang 1938 festgestellt wurde, dass rd. 75 % aller abgehörten Funksprüche dechiffriert worden waren[18]. Das ist eine gute Ausbeute von etwa 93 % bezogen auf die 81 % , bei denen die Voraussetzung erfüllt war, dass die mittlere Walze während der Chiffrierung des Spruchschlüssels nicht weiterrückte.

4.2.2.1 Umkehrwalze B.

Am 1.11.1937 wurde im gesamten ENIGMA - Verkehr die Umkehrwalze ausgetauscht gegen eine neue, die „Umkehrwalze B“ . BLOCH zitiert aus einem Interview mit Colonel LISICKI, dass von deutscher Seite in den ENIGMA - Netzen daran erinnert wurde, ab 1.11.1937 (nach anderer Lesart ab 2.11.) 0.00 Uhr die Umkehrwalze B zu benutzen[19].

[17] Siehe Fussnote S. 92
[18] REJEWSKI b), S. 263
[19] BLOCH b), S. 229

Als von diesem Zeitpunkt an die deutschen Sprüche nicht mehr zu lesen waren, war dem polnischen Team die Ursache bekannt, und es konnte daran gehen, die Verdrahtung dieser neuen Walze zu bestimmen. Die erste Walze und ihre Anfangsstellung waren – wie bisher – leicht zu ermitteln Damit war aber auch der Kern Q bekannt

$$Q = R_2 R_3 K R_3^{-1} R_2^{-1}$$

Da auch die Verdrahtungen der restlichen beweglichen Walzen bekannt waren – unbekannt waren nur die Anfangsstellungen – musste es genügen, die bekannte Permutation Q von links (invers) und von rechts mit den allen Anfangsstellungen entsprechenden Permutationen zu multiplizieren, und das für mehrere Tage. Dasjenige Produkt, das sich als tagesunabhängige Invariante zeigte, musste die neue Umkehrwalze darstellen.

Der grundlegende Fehler, der hier von deutscher Seite gemacht worden war, bestand darin, nicht gleichzeitig mit der Umkehrwalze andere Walzen ausgetauscht zu haben bzw. die Einführung weiterer Walzen oder auch die Änderung des Chiffrierverfahrens, wie es ja 1938 dann geschah, angeordnet zu haben.

Seit September 1937 war ein neues Funknetz beobachtet worden (es handelte sich um das Funknetz des Sicherheitsdienstes - SD), in das zunächst kein Einbruch gelang, obwohl die Tagescharakteristiken und auch die Steckerstellungen ermittelt werden konnten. Die Ringstellungen entzogen sich aber dem Zugriff, möglicherweise waren nicht die üblichen Buchstaben anx am Spruchanfang. Man versuchte daraufhin beliebige mittlere Stücke der Sprüche mit allen möglichen Ringstellungen und erhielt einmal die Buchstaben `/e i n/` [20]. Das konnte ein Textteil sein, aber auch Zufall. Auffällig war aber, dass in diesem „Klartext“ Wiederholungen von Gruppen von vier Buchstaben auftraten und diese Wiederholungen als Abstand voneinander jeweils Vielfache von vier hatten. Dies fand sich auch in den anderen mit dieser Ringstellung dechiffrierten Sprüchen dieses Tages. Daraus musste geschlossen werden, dass der Klartext zunächst über ein Codebuch in Gruppen zu je vier Buchstaben chiffriert worden war, die dann mit der Chiffriermaschine ENIGMA überchiffriert worden waren. Bei der Gruppe `/ein/`, die die Aufmerksamkeit des polnischen Teams erregt hatte, handelte es sich in der Tat um ein Klartextwort zwischen Codegruppen. Dieser fundamentale Fehler (Vermischung von Klartext mit chiffriertem Text) zusammen mit dem Glück, diese Stelle zufällig zu finden, verhalf REJEWSKI und seinen Mitarbeitern zu einem vollständigen Tagesschlüssel und damit zum Einstieg in die Rekonstruktion des Codebuches. Diese Rekonstruktion gelang bald, weil es sich nicht um einen schwierigen Code gehandelt haben soll. [21]

Mit dem 15.9.1938 wurde das bisherige Verfahren zur Chiffrierung durch ein neues ersetzt.[22] Nunmehr wurde nicht mehr per Schlüsseltafel (neben Walzenlage, Ringstellung und Steckerlage) eine gemeinsame Grundstellung für alle Sprüche festgelegt, mit der der vom Chiffrierenden jeweils gewählte Spruchschlüssel zu chiffrieren war, sondern die Schlüsseltafel schrieb nur noch Walzenanordnung, Ringstellung und Steckerlage vor. Für jeden Spruch wählte der Chiffrierer zunächst eine Grundstellung, die vor dem Spruch klar eingefügt wurde, dann einen Spruchschlüssel, dessen Verdoppelung, mit der vorher gewählten Grundstellung chiffriert, gesendet wurde. Der für den Empfänger zur Dechiffrierung nötige Teil des Gesamtspruches bestand nunmehr aus neun Buchstaben statt bisher aus sechs. Im Funknetz des SD wurde dieses neue Chiffrierverfahren aber nicht mit dem 15.9.1938 übernommen, sondern erst ab 1.7.1939. Die Verwendung zweier verschiedener Verfahren, von denen das eine als kompromittiert zu gelten hatte, sollte sich als schwerer Fehler erweisen. Als Folge dieser Zweigleisigkeit konnten die Sprüche des SD - Netzes weiter wie bisher bearbeitet werden, bei den militärischen Funknetzen war das zunächst nicht mehr möglich.

[20] Bei LISICKI, S. 71: „eins“
[21] REJEWSKI b), S. 263
[22] KOZACZUK b), S. 69 ff. und REJEWSKI b), S. 263 ff.

Verfahrenssimulation.
Walzenanordnung: 312; Umkehrwalze B; Ringstellung: CMJ ; 250 Grundstellungen und Indikatoren
7 Steckverbindungen

ACJ GLMPPP	ADC BBGVYW	ADV RBFEMO	AFL CYMJJY	AGZ ZEJYCC	AIY PFVXUW
AUF AMGRKB	AXC FOWCJD	AXL PADPBK	AYI XPOLZW	BCA YNFVFT	BDS DFXNAT
BEH ABAMMX	BIH NCJZMK	BKZ VHCVXG	BNG KOEWBC	BQJ FUFPPE	BQL PHMWVF
BTX QSJRTB	BVL PZLQJH	BWJ NPRHRZ	BWT INEDMQ	CAM NBLEBP	CMY ALGAWG
CNI TGSYTH	COJ SRWHLY	CPE CXRVVF	CQB TPAZDA	CRV EBLQXQ	CUK IFDLXM
CUP TRQFSI	CWD QMXTCR	CXZ BLBKWC	CZT TFUYYB	CZX JFFHBG	DAN NCRNEV
DEC IVHYFC	DFL FGOTPA	DLF SOXLMZ	DMU DGMIBC	DMZ ZPXYFN	DOR BCAGVB
DQL ONIOPH	DSE GQFYUK	DTE HGXHVK	DUG EDDLQA	DZH KXFFMS	DZS KBYHSX
EDG IXTADS	EKF UMSIGE	EMK KDZFLR	EMQ VJIOSI	EOH RHBUHG	EQY ONBJMT
ERA IEEAIN	ESL WZGSLY	EVH DUGTIJ	EWG DGNLPJ	FDC BGLCXK	FGK VHWUUY
FHQ OOLRQL	FJO ZEFPIU	FJY JPXECW	FMU RDEOJO	FPY JUOUYF	GCV SOATXV
GFN UACHQS	GSQ FUHXUN	GTZ FEOVYB	GXB COVISE	GXZ PJCCOI	HAB HJASLO
HFD LHQOMW	HFQ COFJBV	HTM XMNNNV	HVX YYIAJD	HXY VMLXGW	HYD HSXWCE
HZJ DQKPKB	IAR THOMTT	IBX HMOSZI	IEH RUQURE	IGM ZDLRXC	IGS PGVCKV
IKC IUZGCU	IKE NEBLIM	INH PVABTG	INQ UYKSIO	IRB SRNFLH	ISA SFVNRR
IUS WTXFOC	JBW FIRVCH	JCO CPJVCN	JDC LTVLID	JGN IDQDMW	JIB SEDRLZ
JLN MBJWZA	JRF BIUAJB	JRL UMLBUF	JRO BTLYRZ	JSO OTCROI	JTX OKVGDJ
JXP BQYMZU	JZQ LBSGJM	KDZ WSFXBO	KFN KXMHKA	KHC XOQRKD	KID CEPJQM
KIS NLNTGJ	KRI JWJAAK	KTH EVLKQS	KUV FIQGPM	KWU MOZCTP	LCB NTERKX
LIC IHHQJG	LNT EDPZIQ	LWG NNMZOJ	LZA FORABN	MFE NTWEPV	MFT OSQFUV
MHP DYXRFD	MJR ASPTLE	MNA IEPQQZ	MQH AYQEYZ	MRP JLUYYB	MTS GTRKRQ
MWB YYBNMG	MWI JDGAEK	MWU IDDFWT	MZU BDVBSL	NAO WCXMLN	NCY QTBLXO
NEL KRHRUV	NFJ QORMRI	NKF DTMZJT	NLV HNPTUH	NMD NFBACJ	NOC SEMGLP
NRM LDDRBJ	NRS IUNRZB	OBM FRUDLJ	OFU NJUTJP	OHL SSKQDV	OHM NLNEJG
OLJ HSUALL	ORN MCGVPM	OTE NBAGMD	OTE DWYWSA	OUI FQWDLG	OXN YYHJMS
OYP KTFSZO	PDE DUUCCE	PGC EANRDR	PLU ASNXNN	PRU WPEJPD	PXL VUPTUU
PXL GBBLIT	PXT RHVZLS	PYH AVJDYL	QGK PBOLKR	QMV XRCAOZ	QOE MYPYSB
QTN QHWXCF	QWA TJSQPX	QZU HVGRDR	RCZ VLWXFJ	RDG DGMDGW	RFB NKCYQZ
RGQ WIPCHN	RIJ AHMOHL	RSK OTYIDN	RTU ZGMKZM	RXG QCFRNQ	RZV WDRMHL
SAC TLMFIM	SCI EMKXXX	SDK TRXTMX	SGK EYMCTE	SIR XVJHVJ	SIX GSZIYV
SLD ZLHXTO	SLT SVVOFQ	SMU OMPIVR	SNH BXNGRQ	SNO RUQXAM	SRD WEXMPM
TAR AKLATL	TJR QHVUVC	TLI ZZTFWJ	TMZ GEBROF	TZI MYSBAD	UCG DYHTMX
UJX ZIQTMV	UKX ROQHOD	UNE ZFDKIX	UPT OEMTDX	UQR IIBTFB	YRS XUAPDJ
USO EKLXGG	UVX SPBGEC	UYH QBWBZH	UYN MTHAUI	VDP GMQXNP	VGT QZWJWJ
VJH UIQFBC	VJY MDEQMX	VLH NFOKRA	VOI CTRMCF	VQJ GDZEGX	VRI KLXKZZ
VXJ LZGKFJ	VYP WHZGKD	VZN SXUYDO	WDZ YTLRXK	WFA SFXXYM	WIJ DUIZPH
WIU MWAEQF	WJF TYCQFI	WKG CQRNBU	WKQ YMNOOC	WPR KYGHDI	WTY GKOVWJ
WUT TXNGVF	WVN WMLXYE	WYV WKNEMK	XCR IZXNZW	XLA AKAJMN	XUV ALQMYG
XZE ZGREUG	YAZ KSZACX	YIA DLSEOO	YKJ LHPFUT	YLZ RGOTXF	YMB VEULEJ
YNL THYLSH	YNR LXBRGO	YNX WSHRFM	YPF NNCRLI	YPW ORTBGI	YUA ZDPOUV
YVQ PLTVNB	YWG JIEXIX	ZCY BLZCSB	ZIO HTAHPM	ZJI NHLFQH	ZQL IJWFMK
ZSL YKCUWL	ZSX SFAIUK	ZXG QLEZMN	ZYR EVSFAO		

Es gibt 34 Fälle von «females»

PAD PBK; VHC VXG; NBL EBP; ALG AWG; TPA ZDA; NCR NEV; ONI OPH; HGX HVK; VJI OSI; RHB UHG; OOL RQL; FUH XUN; PGV CKV; LTV LID; AYQ EYZ; BDV BSL; NJU TJP; ASN XNN; WPE JPD; VUP TUU; DGM DGW; AHM OHL; ZGM KZM; TLM FIM; TRX TMX; XVJ HVJ; AKL ATL; ROQ HOD; IIB TFB; KLX KZZ; IZX NZW; VEU LEJ; JIE XIX; HTA HPM;

Tabelle 4.19:

Die bislang vom polnischen Dechiffrierdienst angewandten Methoden beruhten darauf, dass alle Indikatoren (d.h. Chiffrierungen der verdoppelten Spruchschlüssels) auf e i n e Grundstellung zurückgingen und somit eine Tagescharakteristik entwickelt werden konnte. Nunmehr existierte aber keine Charakteristik mehr. In Tabelle 4.19 sind Beispiele für solche klar gesendeten Grundstellungen und die Ergebnisse der damit erhaltenen Chiffrierungen der verdoppelten Spruchschlüssel für eine Schlüsselperiode (ab 1.1.1936: ein Monat, ab 1.10.1936: ein Tag) aufgeführt. Im Kopf sind zur Information die zugrundegelegten Daten mit angegeben, es handelt sich um nach einem Zufallsprinzip erzeugte Spruchschlüssel und die daraus entstandenen Indikatoren. Vor dem Ausdruck sind die Daten sortiert worden.
Wie man sofort erkennt, folgt in den Positionen 1 und 4 auf `G`(1) im ersten Beispiel `(ACJ GLMPPP)` `P`(4), im Beispiel `DSE GQFYUK` aber `Y`(4).
Der oben erwähnte Verlust der Charakteristik erzwang die Suche nach anderen Methoden. Manchmal war es möglich, aus dem Indikator, wie er vorlag, bereits Aussagen über die schnelle Walze zu gewinnen[23]. Ein Beispiel soll das verdeutlichen:

```
T K P   A N V   C K B
T L R   V T S   J Q M
```

Hier ist sofort deutlich, dass die schnelle Walze nicht Walze I sein kann. Die Walze I würde die mittlere Walze beim Übergang von `Q` nach `R` weiterschalten. Beim Buchstaben `V` im ersten Indikator wäre demnach die Walzenstellung `T L R`, wie die Startposition beim zweiten Indikator. Dann müsste der zweite Indikator lauten

```
T L R   V T S   B Q M
```

Bei der Chiffrierung des verdoppelten Spruchschlüssels traten jedoch gewissermassen Reste der Charakteristik auf, nämlich gleiche Geheimtext-Buchstaben an den Stellen 1 und 4 bzw. 2 und 5 bzw. 3 und 6 des Indikators. Sie sind beim Chiffrieren jeweils aus ein und demselben Klarbuchstaben hervorgegangen. In der ihnen jeweils zuzuordnenden, aber nicht mehr vorhandenen, Charakteristik wären sie durch Zyklen der Länge eins vertreten. Das ist auch der Grund dafür, dass sie sich in das neue Verfahren „gerettet“ hatten.

4.2.2.2 «females.»

Diese Auffälligkeiten in den Schlüsseln wurden von D. KNOX «females» genannt,[24] in der deutschen Literatur ist auch „Fixpunkte“ oder „Festpunkte“ gebräuchlich. Auf diese Reste der Charakteristik gründeten nun REJEWSKI und seine Mitarbeiter zwei Methoden, den jeweiligen Tagesschlüssel (hier handelt es sich „nur“ noch um die Bestimmung der Ringstellung und später der Steckerlage) zu ermitteln.

4.3 BOMBA

REJEWSKI ging von dem Fall aus, dass ein und derselbe Buchstabe als 1–4 - female, als 2–5 - female und auch als 3–6 - female auftrat. Im Beispiel der Tabelle 4.20 ist das der Buchstabe `B`, der in `MZU BDVBSL` (1–4) , `CAM NBLEBP` (2–5) und in `UQR IIBTFB` (3–6) vorhanden ist. Da die Abstände `M - C - U` , `Z - A - Q` und `U - M - R` bekannt und fest sind (die Ringstellung ist ja für alle Sprüche der Periode gleich), konnte REJEWSKI die Suche nach der Ringstellung mechanisieren:[25]
Er koppelte sechs ENIGMA - Walzensätze so aneinander, dass die ersten Walzen synchron weiterrückten. Im obigen Beispiel hätte er die ersten beiden Sätze auf die Stellungen `MZU` bzw. `MZX` eingestellt, die nächsten beiden auf `CAN` bzw. `CAQ` und die letzten auf `UQT` bzw. `UQW`. Bei dieser Einstellung musste berücksichtigt werden, dass zwischen den Stellungen der beiden ENIGMA - Sätze eines Paares evtl. die mittlere oder die

[23] DEAVOURS u. KRUH a), S. 115
[24] KNOX
[25] REJEWSKI b), S. 264

linke Walze weiterrückte. Als zu „chiffrierender“ Buchstabe wurde immer der in den Stellungen (1 - 4) , (2 - 5) und (3 - 6) gemeinsam aufgetretene Buchstabe eingegeben (Im Beispiel der Tabelle 4.20 der Buchstabe B). Dann wurden alle ENIGMA - Walzensätze synchron weitergedreht. Wenn eine Stellung erreicht war, bei der jedes Paar für sich zwei gleiche Buchstaben als Resultat lieferte, leuchtete eine Lampe auf und die Maschine blieb stehen, sodass die momentanen Stellungen abgelesen werden konnten.

B o m b a - Durchlauf mit dem Buchstaben B und

Indik.-Schlüssel	Indikator
MZU	BDVBSL
CAM	NBLEBP
UQR	IIBTFB

Walzenlage	Ermittelte Ringstellungen
1 2 3	EKS, GFC, TYU
1 3 2	IWF , QRA
2 1 3	-
2 3 1	ZAV
3 1 2	CMJ
3 2 1	-

Tabelle 4.20:

Zwei Voraussetzungen waren in dieses Verfahren gesteckt worden.:

1) Die Ringstellungen waren alle zu AAA angenommen.

2) Es wurde angenommen, dass keine Steckverbindungen geschaltet waren.

Zu 1): Diese Annahme konnte das Ergebnis verfälschen, weil die Bewegungen der mittleren (und evtl. der linken) Walze in anderen Positionen des Walzenkernes stattfinden konnten als bei der tatsächlichen Ringstellung des Tagesschlüssels;
zu 2): Wenn der im Verfahren verwendete Buchstabe in einer Steckverbindung vorkam, dann konnte das Verfahren nicht mehr zum Ziel führen. Bei 5 bis 8 Steckverbindungen, wie seit dem 1. 1. 1936 üblich, blieben im Mittel 12 bis 14 Buchstaben ungesteckert, also konnte man immerhin in etwa 50% der Fälle mit einem Erfolg rechnen.

REJEWSKI nannte die Vorrichtung BOMBA[26].

In der erstaunlich kurzen Zeit von wenigen Wochen hat die Firma AVA sechs solcher BOMBY, je eine für eine mögliche Walzenlage, hergestellt, sodass ab November 1938 selbst bei unbekannter Walzenlage parallel alle Möglichkeiten durchgeprüft werden konnten. Nach den Angaben bei KOZACZUK dauerte ein solcher Durchlauf nur etwa zwei Stunden.[27] Danach konnte mit den wenigen erhaltenen Stellungen der Walzen, bei denen die BOMBAs stehengeblieben waren, geprüft werden, welche einer Ringstellung entsprach, mit der alle Sprüche des Tages gelesen werden konnten. In Tabelle 4.20 sind die Ergebnisse der Durchläufe von allen Varianten der Walzenlage für das Beispiel von Tabelle 4.19 mit dem Buchstaben B dargestellt. Diese Stellungen mussten geprüft werden, ob sie aus den Indikatoren (verdoppelte) Spruchschlüssel lieferten und darüber hinaus diese Spruchschlüssel zur Dechiffrierung der zugehörigen Geheimtexte führten.

In Tabelle 4.21 sind für drei der in Tabelle 4.20 aufgeführten Beispielsfälle diese Versuche dargestellt. (Einbezogen sind hierbei auch die Fälle, in denen die Indikatoren den Geheimbuchstaben B, der dem Beispiel zugrunde liegt, zweimal nebeneinander aufweisen.)

[26] Der Name war nach LISICKI beim Essen einer Eiskrem-Bombe entstanden.(KOZACZUK engl., S. 63)
[27] KOZACZUK b), S. 69

Versuche zur Rückübersetzung der Indikatoren
mittels der durch Bomba ermittelten Ringstellungen

Walzenlage	Grund-stellg.	Ring-stellg.	Indikator	Text--schlüssel
1 3 2	MZU	IWF	BDVBSL	NCINLS
	CAM	IWF	NBLEBP	INIFNK
	UQR	IWF	IIBTFB	LBLQOL
	ADC	IWF	BBGVYW	AEJKRE
	PXL	IWF	GBBLIT	UPOPXN
	MZU	QRA	BDVBSL	TTPTYM
	CAM	QRA	NBLEBP	LMGYMD
	UQR	QRA	IIBTFB	NQKJKK
	ADC	QRA	BBGVYW	GAMEUZ
	PXL	QRA	GBBLIT	BHHPZM
3 1 2	MZU	CMJ	BDVBSL	SXCSWF
	CAM	CMJ	NBLEBP	ZNXDNV
	UQR	CMJ	IIBTFB	GFJGDJ
	ADC	CMJ	BBGVYW	TSITJI
	PXL	CMJ	GBBLIT	FTPJTP

Tabelle 4.21:

Es ist deutlich, dass nur die Ringstellung CMJ weiteren Erfolg versprechen kann. Man könnte auch versuchen, bei der Zeile

PXL - CMJ - GBBLIT - FTPJTP

anzusetzen. Als Spruchschlüssel käme dabei jede Möglichkeit ATP ...ZTP in Betracht. Hier zeigt sich der offenbar richtige Spruchschlüssel durch Probieren und Betrachten der Häufigkeiten der Klarbuchstaben. Bei DTP treten deutlich Maxima hervor, die den Rückschluss auf den Buchstaben e (und den Worttrenner x) zulassen. In Tabelle 4.22 sind beispielhaft einige der Ergebnisse der Durchmusterung mit dem folgenden Geheimtext abgedruckt.

Verfahrenssimulation
Walzenanordnung: 312, Umkehrwalze B; Ringstellung: CMJ; Keine Steckerverbindungen
G e h e i m t e x t:

```
EIJHW GHXSB TIPVA KPNUM RBXXI OQORM YBOZG MOOXN NKDIH ALLIU
MAMZF PSROA HDGCK ISCGU HHUNY KOMOD BZSTN TUWFR MYMZD WGZPE
KLZBS EATSU SXTVL DXSOT FDSZQ UTJSC YOCKG RUVAY UVUNB UNERM
URFBC TFHLI YBRHS YENBL IGKUT PKRJE ..... ..... ..... .....
```

S t a t i s t i k:

6	6	10	7	6	10	3	9	6	6	8	4	3
A	B	C	D	E	F	G	H	I	J	K	L	M
8	6	6	5	10	3	6	14	8	6	8	7	9
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

G r u n d s t e l l u n g: ATP
K l a r t e x t:

```
yhknk lrfrr bwieu cbhxt ecojf kmcwf crnod yzjts cmmau uowoq
vknkk higyv qhqqd pkznr kfsll rnren atyaw uzcid vaphq xhdnr
fzbzh vvzcp ugjai yclsu jzvur fwbjy ufpvz upugf epfad reybc
wxxdo hnoeu juutx xvutx hczfx ditib ..... ..... ..... .....
```

S t a t i s t i k:

6	6	10	7	6	10	3	9	6	6	8	4	3
A	B	C	D	E	F	G	H	I	J	K	L	M
8	6	6	5	10	3	6	14	8	6	8	7	9
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Grundstellung: `CTP`

Klartext:

```
dzigf hsdgd fhuxm ygvag eqhay rhins zrmbk eceqj qigsf vhwxr
gshkd xwcsk nrhud tcnol aalkk thrnf hubev lebjz vuwfx uuory
fjgon yfsms okzqg qqrfa uqjhf fpuys ibhqd bxkfo vbyri bfaea
llmeo yndzu fmpsh awqug hdbhd rbtkd ..... ..... ..... .....
```

Statistik:

8	9	3	10	7	13	9	14	5	4	8	5	5
A	B	C	D	E	F	G	H	I	J	K	L	M
6	6	2	9	9	9	3	10	5	4	5	7	5
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Grundstellung: `DTP`

Klartext:

```
jnxbz amrnf mntjx iyrtx sjfkr xehyh oisyy kyval yrjjj busby
fbyit jmned ruaby nysjh vtyjp mbbrg ywjsy ptymb nnxsr yjmyu
tprst iwyrj ywnsv kvjwz vnpew oyomw bkwpp ynjxz nnvzh hjfcv
yidym jyeba cnfiu ikine rygtj oylag ..... ..... ..... .....
```

Statistik:

5	10	2	2	5	5	3	5	8	17	5	2	8
A	B	C	D	E	F	G	H	I	J	K	L	M
14	4	6	0	10	8	8	4	7	7	6	25	4
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Grundstellung: `FTP`

Klartext:

```
xcrsi ezpev nfyoh rlqgw jaswt bjuab owrpn rkmft zryyo tuxdd
aevju fpjam dufbe vqsro vxdph zfnsz vbxic yjfsp ycqtl rpgqj
astkc wwjrx imvrm pagns wpmmu aecfz wlvbb lkokr rfvzz abhue
rsljw wdybo ozvzd pxsrq xymbe xonag ..... ..... ..... .....
```

Statistik:

9	9	5	6	7	8	4	3	3	8	4	5	7
A	B	C	D	E	F	G	H	I	J	K	L	M
5	8	9	5	13	9	5	6	9	9	8	7	9
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Tabelle 4.22:

Bisher war von der Voraussetzung ausgegangen worden, dass keine Stecker verwendet worden seien. Der „Geheimtext“ dazu ist in den Tabellen 4.23 bis 4.25 in Grossbuchstaben zu erkennen, es handelt sich um das Beispiel der Zeile `ADC - CMJ - BBGVYW - TSITJI ,` Es entsteht noch kein verständlicher Text. An dieser Stelle kam zum Tragen, was die genaue Beobachtung und Archivierung der bisher dechiffrierten Sprüche an Stereotypen und Eigenheiten des Funkverkehrs der einzelnen Truppenteile bzw. Funker an Erfahrung zur Verfügung stellten - zumindest konnte man versuchen, ob auch dieser Spruch in eins der bekannten Schemata passte. WELCHMAN schreibt dazu:

> *Obgleich meine Deutschkenntnisse begrenzt waren, konnte ich erkennen, dass die Leute (im Funkverkehr) miteinander höchst diszipliniert sprachen. Sie waren sehr höflich zueinander und legten grossen Wert darauf, den vollen Titel des Offiziers oder der Dienststelle des Adressaten zu nennen. Darüber hinaus wurde am Spruchende sehr sorgfältig der volle Titel des Absenders angegeben*[28].

Die Versuche, mit der angenommenen Ringstellung den Spruchschlüssel zu gewinnen, führen zu der Vermutung, dass – ausser `B` – noch die Buchstaben `I, T, G` und `W` nicht in den Steckerverbindungen vorkommen. Die Vermutung liegt nahe, dass der Spruchschlüssel `TSI` lautet. (Oben war gezeigt, wie diese Vermutung gestützt werden kann.)

In den Tabellen 4.23 bis 4.25 ist die Prozedur des schrittweisen Dechiffrierens zu sehen:

[28] WELCHMAN b), S. 38. In Polen hat man die gleichen Erkenntnisse gehabt.

Verfahrenssimulation

Walzenanordnung: 312, Umkehrwalze B;Ringstellung: CMJ; Grundstellung: TSI; Keine Steckerverbindungen

```
IMLHX GSDEB PMQSG UEMAC EHKWE GJOCC BCDXU XBBRQ LQVGG TMCWD
mlavy aatzf ythji nhgxl rwyig spbrf jwmbb eryib eojam ntlvo
ERKLM XZVMD NZEWI YBZDC TIJZC DBAHS MVZPZ UVSBK PQVLH TEQAY
fjmbu bsgqr yxmya jykgy cwiyx qnzjj wzpbs niyrt ybjfg naelt
VQGPK AJDUP NLUAT QMSLF GNCFP FOHYN DVOOD IVFAZ ..... .....
jpitj miimb tnvxy tzhsa dytek eaauk madjm fmjyl ..... .....
```

Klartext-Statistik:

10	9	1	2	5	5	5	3	8	12	3	5	10
A	B	C	D	E	F	G	H	I	J	K	L	M
6	2	3	2	5	4	9	2	3	4	4	14	4
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

1) Ausgehend von der Vermutung, der Spruch beginne mit `anx` und der weiteren Vorgabe, dass I nicht gesteckert sei, wird als erstes Steckerpaar `(AM)` angenommen.

Steckerverbindungen: (AM)

```
IMLHX GSDEB PMQSG UEMAC EHKWE GJOCC BCDXU XBBRQ LQVGG TMCWD
anmvy mmtzf yuhji nhryl rwyig spbrf jwabb eryib eojma nzlvo
ERKLM XZVMD NZEWI YBZDC TIJZC DBAHS MVZPZ UVSBK PQVLH TEQAY
fjabd bsgjr yxaym jykgy cwiyx qnkjj kzpbs niyrt ybjfg nmett
VQGPK AJDUP NLUAT QMSLF GNCFP FOHYN DVOOD IVFAZ ..... .....
jpitj miiab tnviy tjhsm dytek emmuk amdja fajtl ..... .....
```

Klartext - Statistik:

9	9	1	3	5	5	4	3	9	14	5	3	11
A	B	C	D	E	F	G	H	I	J	K	L	M
7	2	3	1	6	4	9	2	3	3	2	14	3
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

2) Die Statistik lässt die Paare `(EY)` und `(JX)` – x als Worttrenner – oder `(EX)` und `(JY)` vermuten. Ersteres führt weiter, es treten bereits Wortteile wie „`eins`“ , „`..berei..`“, „`.e.tembe.`“ hervor.

Steckerverbindungen: (AM) (EY) (JX)

```
IMLHX GSDEB PMQSG UEMAC EHKWE GJOCC BCDXU XBBRQ LQVGG TMCWD
anmvz mmtnf euhxi ndrel twein snbrf xwarb ereib yoxma nzlvo
ERKLM XZVMD NZEWI YBZDC TIJZC DBAHS MVZPZ UVSBK PQVLH TEQAY
rxabd asgxr ejtem bekge cweej qnkxx kzpbs niert ebxfg nsyto
VQGPK AJDUP NLUAT QMSLF GNCFP FOHYN DVOOD IVFAZ ..... .....
xpitx mgiab tnvie txhsm detyk ymmsk amdxa faxtl ..... .....
```

Klartext - Statistik:

9	8	1	4	15	4	4	2	7	2	5	3	10
A	B	C	D	E	F	G	H	I	J	K	L	M
10	3	2	1	7	6	10	1	3	3	13	4	3
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Tabelle 4.23:

3) Die Buchstabenfolge nach „`ANM` „ lässt vermuten, dass darauf folgt „`KOMMAND`“ (`-eur` oder `-ant` oder `-o`). Da `B` sicher nicht gesteckert ist (sonst würde das Verfahren von Anfang an nicht funktioniert haben), kann man auf das Steckerpaar `(DF)` schliessen.

Steckerverbindungen: (AM) (EY) (JX) (DF)

```
IMLHX GSDEB PMQSG UEMAC EHKWE GJOCC BCDXU XBBRQ LQVGG TMCWD
anmvz mmand euhxi nfrel twein snbrd xwzrb ereib yoxma nzlve
ERKLM XZVMD NZEWI YBZDC TIJZC DBAHS MVZPZ UVSBK PQVLH TEQAY
rxabf asgxs ejtem bekxe cweej unkxx kzpbs niert ebxdg nsyto
VQGPK AJDUP NLUAT QMSLF GNCFP FOHYN DVOOD IVFAZ ..... .....
xpitx mgxab tnvie txhsu fetxk zmmsk zmfxn dantl ..... .....
```

Klartext - Statistik:

7	8	1	4	16	4	3	2	6	2	5	3	9
A	B	C	D	E	F	G	H	I	J	K	L	M
12	2	2	0	6	7	9	3	3	3	15	2	6
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

4) Wenn die Annahme „ `KOMMAND` “ weiter verfolgt wird, müsste `(OZ)` das nächste Steckerpaar sein, das könnte an anderen Stellen ebenfalls vermutete Wörter deutlicher hervortreten lassen, z.B. „`MANO.VER`“.

Steckerverbindungen: (AM) (EY) (JX) (DF) (OZ)

```
IMLHX GSDEB PMQSG UEMAC EHKWE GJOCC BCDXU XBBRQ LQVGG TMCWD
anmvo mmand euhxi nfrel twein snurd xworb ereib yzxma nolve
ERKLM XZVMD NZEWI YBZDC TIJZC DBAHS MVZPZ UVSBK PQVLH TEQAY
rxabf angxs eptem berxe cwerj unkxx kombi niert ebxdg nsytz
VQGPK AJDUP NLUAT QMSLF GNCFP FOHYN DVOOD IVFAZ ..... .....
xpitx mgxab tnvie txhsu fetxk ormsk omman dantx ..... .....
```

Klartext - Statistik :

8	7	1	4	15	3	3	2	7	1	4	2	10
A	B	C	D	E	F	G	H	I	J	K	L	M
13	6	2	0	9	5	9	4	3	3	15	2	2
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

5) Es fällt auf, dass offenbar fehlende Buchstaben in dem schon fast lesbaren Text mit `L, Q, C,` und `H` verknüpft sind. Versuch mit den im Text zuerst vorkommenden `(HL)`:

Steckerverbindungen: (AM) (EY) (JX) (DF) (OZ) (HL)

```
IMLHX GSDEB PMQSG UEMAC EHKWE GJOCC BCDXU XBBRQ LQVGG TMCWD
anxko mmand eulxi nfreh txein snurd xworb ereib ezxma nohve
ERKLM XZVMD NZEWI YBZDC TIJZC DBAHS MVZPZ UVSBK PQVLH TEQAY
rxanf angxs eptem berxe cwerj unktx kombi niert ebxei nsytz
VQGPK AJDUP NLUAT QMSLF GNCFP FOHYN DVOOD IVFAZ ..... .....
xpitx mgxab txvie txlau fetxk orpsk omman dantx ..... .....
```

Klartext - Statistik:

9	6	1	3	17	3	2	2	8	1	5	2	8
A	B	C	D	E	F	G	H	I	J	K	L	M
13	6	3	0	9	4	10	4	2	2	17	1	6
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Tabelle 4.24:

6) Es bleibt noch `(CQ)`.

Steckerverbindungen: (AM) (EY) (JX) (DF) (OZ) (HL) (CQ)

```
IMLHX GSDEB PMQSG UEMAC EHKWE GJOCC BCDXU XBBRQ LQVGG TMCWD
anxko mmand eurxi nfreg txein snull xvorb ereit enxma noeve
ERKLM XZVMD NZEWI YBZDC TIJZC DBAHS MVZPZ UVSBK PQVLH TEQAY
rxanf angxs eptem berxs qwerp unktx kombi niert erxei nsatz
VQGPK AJDUP NLUAT QMSLF GNCFP FOHYN DVOOD IVFAZ ..... .....
xmitx mgxab txvie rxlau ferxk orpsk omman dantx ..... .....
```

Klartext - Statistik :

10	4	0	2	17	3	3	0	8	0	5	3	9
A	B	C	D	E	F	G	H	I	J	K	L	M
14	6	3	1	12	5	9	4	3	1	17	0	1
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Tabelle 4.25:

Der Spruch ist vollständig dechiffriert, sieben Steckerpaare sind erkannt, es gibt keine weiteren.

4.3.1 Lochblätter

Die beiden für die Verwendung der BOMBA gemachten Voraussetzungen:

1) Der Prüfbuchstabe war nicht gesteckert und
2) Der Prüfbuchstabe trat als «female» in allen drei Positionen auf

waren sehr einschränkende Bedingungen. Man suchte nach einer Möglichkeit, den einzigen Zugriff auf die Schlüsselstruktur, nämlich über die «females», ohne diese Bedingungen auszunutzen.

Bekannt war schon, dass die Charakteristik unbeeinflusst von der Steckerlage blieb (das hatte bei der Verwendung des Charakteristik - Kataloges zur Ermittlung der Steckerlage beigetragen). Bekannt war weiter, dass etwa 40% aller Charakteristiken «females» (Zyklen der Länge eins) enthielten.

Innerhalb einer Schlüsselperiode konnte man (bei Beschränkung z.B. auf die 1 - 4 - «females») aus den klar gesendeten Grundstellungen für die Chiffrierung des verdoppelten Spruchschlüssels (die den Indikator lieferte) die Abstände voneinander ablesen. Da alle Grundstellungen eine gemeinsame Ringstellung hatten, spielte die Ringstellung bei der Abstandsermittlung (d.h. Differenzenbildung) keine Rolle. Wenn es gelang, die in einem bestimmten Abstandsmuster voneinander auftretenden «females»(z.B. 1 - 4) mit den Charakteristiken in der Kartei zu vergleichen und dort nach diesem Muster zu suchen, musste man auf Einstellungen stossen, die mit denen in der untersuchten Schlüsselperiode kompatibel waren. Diese wären dann weiter zu untersuchen.

ZYGALSKI, einer der Mitarbeiter REJEWSKIs, fand eine Lösung für dieses Problem, die zunächst sehr umständlich erscheinenden Vergleiche zu vereinfachen, allerdings um den Preis, umfangreiche Vorarbeiten leisten zu müssen. Zunächst zog er aus der Kartei der Charakteristiken alle die Grundstellungen heraus, die in den Stellen 1 - 4 «females» aufwiesen.[29] (Der Katalog der Charakteristiken war unter der Voraussetzung erstellt worden, dass die Ringstellung `AAA` lautete). Dann übertrug er die Karteiaussagen „female existiert“ bzw. „female existiert nicht“ in eine Matrix mit den Eingängen „Stellung der mittleren Walze“ und „Stellung der ersten Walze“. Um die Vergleiche zu vereinfachen, befand sich die Matrix auf einem Papierbogen, in den an den Stellen „female existiert“ ein rechteckiges Loch geschnitten wurde (mit einer Rasierklinge !). Wegen der zyklischen Eigenschaften der Walzenstellungen mussten längs jeder Achse zwei Alphabete aufgetragen werden, sodass jede Matrix insgesamt $51 \cdot 51$ Felder

[29] REJEWSKI b), S. 265

enthielt. (Es musste also für jede Stellung der langsamen Walze eine solche Matrix erstellt werden, was jedesmal das Schneiden von rd. 1000 Löchern bedeutete.) Für jede mögliche Anordnung der drei Walzen mussten demnach 26 solcher Lochblätter hergestellt werden, insgesamt waren somit 6 Sätze von je 26 Blättern nötig, um für alle Kombinationen von Walzenlagen gerüstet zu sein. [30] Bei ZYGALSKI (und auch später bei JEFFREY im britischen Bletchley Park (siehe Kap. 6.1), wo zunächst auch diese Lochblätter benutzt wurden) war die Anordnung etwas anders, das ändert aber wegen der zyklischen Eigenschaften der Grundstellungen das darzustellende Prinzip nicht.) Wesentlich war der folgende Gedanke: Abb 4.1 zeigt einen angenommenen Ausschnitt aus einem Matrixschema (vor dem Lochen). Als Bezugsfeld sei für die folgende Über-

IP cc	IQ cb	IR ca	IS cz	IT cy	IU cx
JP bc	JQ bb	JR ba	JS bz	JT by	JU bx
KP ac	KQ ab	*KR* *aa*	KS az	KT ay	KU ax
LP zc	LQ zb	LR za	LS zz	LT zy	LU zx

Abbildung 4.1:

legung das Feld *KR* gewählt. Dies entspricht der Stellung K der mittleren Walze und der Stellung R der ersten Walze. (Wie oben gesagt, ist das Matrixblatt als Ganzes der Stellung der langsamen, linken Walze und der Walzenlage zugeordnet.) Die Grossbuchstaben bedeuten Walzenstellungen für die Ringstellungen aa - hier des Verständnisses wegen klein geschrieben. Die Kleinbuchstaben machen eine Aussage, welche Ringstellungen den Walzenstellungen des Bezugsfeldes (hier: *KR*) zugeordnet werden müssen, damit dieselbe Charakteristik auftritt wie die durch die darüberstehenden Grossbuchstaben beschriebenen Anfangsstellungen der mittleren und der ersten Walze mit den Ringstellungen aa.

Im Beispiel: Die Grundstellungen KR liefern bei den Ringstellungen cx dieselbe Charakteristik wie die Grundstellungen IU mit den Ringstellungen aa:

$$\begin{array}{llcccll} \mathtt{K} & \text{(mit Ring } \mathtt{c}) & - & \text{Ring } \mathtt{c} & = & \mathtt{I} & \text{(mit Ring } \mathtt{a}) \\ & 10 & - & 2 & = & 8 & \text{(mod 26)} \end{array}$$

(I gibt die Stellung des Walzenkernes in der Anfangslage wieder, wenn mit Ringstellung c die Grundstellung der Walze K ist.)

[30] REJEWSKI b), S. 266

Als Bezugsfelder für die Auswertung der gelochten Matrixbögen gelten jeweils die an einem Tag in den Grundstellungen der Sprüche, in deren Indikatoren «females»gefunden wurden, genannten Stellungen der mittleren bzw. der ersten Walze, bezogen auf die angenommenen Ringstellungen aa.

Wenn zwei Matrixbögen so aufeinander gelegt werden, dass ihre Bezugsfelder übereinander liegen, dann liegen überall Felder mit gleicher Ringstellung bzgl. dieser Bezugsfelder übereinander. Von unten beleuchtet, schien Licht durch diejenigen Felder (= Ringstellungen bzgl. Bezugsfelder), die «females»anzeigten. Dabei deckte das zweite Blatt alle diejenigen Felder zu, bei denen wohl für die erste Grundstellung, nicht aber für die zweite, «females»möglich waren.

Wenn nun für alle vorkommenden «females»die entsprechenden Matrixblätter so übereinander gelegt wurden, dass die zu den Grundstellungen gehörenden Bezugsfelder übereinander lagen, dann schien - im Idealfall - nur noch Licht durch das eine Feld, das zu allen Grundstellungen diejenige Ringstellung anzeigte, bei der alle «females»möglich waren.

Allerdings waren Einschränkungen zu machen:
1) Es traten in der Schlüsselperiode auch 2–5 – «females»und 3–6 – «females»auf. Diese waren aber leicht auf die 1–4 – Lage zu transformieren: Die Grundstellung der ersten Walze musste nur um eins bzw. zwei verändert werden, um in die Stellung 1–4 zu kommen.

2) Beim Weiterstellen nach 1) oder zwischen der ersten und der zweiten Stellung der ersten Walze könnte die mittlere Walze weiterrücken. Diese Fälle mussten ausser Betracht bleiben.[31] Es konnte allerdings auch vorkommen, dass ein solches Weiterrücken der mittleren Walze zwischen der ersten und der zweiten Stellung wegen der noch unbekannten Ringstellung unerkannt blieb. Hier musste beim Übereinanderlegen der Matrixbögen u.U. durch Probieren das eine oder andere Blatt ausgelassen werden. Dafür musste man u.U. in Kauf nehmen, dass die Zahl der noch offenen Löcher, d.h. der mit den Grundstellungen kompatiblen Ringstellungen grösser als optimal war.
Jedesmal, wenn bei hinreichend vielen aufeinander liegenden Blättern (d.h. bei hinreichend vielen verwendeten Grundstellungen) Stellen mit durchgehendem Licht (d.h. mögliche Ringstellungen) zu finden waren, mussten diese möglichen Ringstellungen weiter untersucht werden, ob eine davon die des Tagesschlüssels war. Da alle Stellungen `A` bis `Z` der langsamen Walze und auch (falls keine anderen Erkenntnisse über die Walzenlage vorlagen) alle sechs mögliche Walzenlagen durchprobiert werden mussten, hatte man im Mittel $13 \cdot 6 = 78$ Versuche des Bögenstapelns zu unternehmen.

Nach Kenntnis der Methode hat D. KNOX in BP den arbeitsaufwendigen Prozess vereinfacht (siehe Kap. 5.1)

Für die Grundstellung `G` der langsamen Walze bei der Walzenlage III, II, I ist das zugrunde liegende Material - Grundstellungen und Indikatoren - in Tabelle 4.26 vorgestellt. Die nächsten Tabellen zeigen die Entwicklung. Mit den Grundstellungen `CSX`, `EJA` und `ENX` ergibt sich das Bild von Tabelle 4.27 oben, wobei die nach Aufeinanderlegen der drei Bögen noch offenen Löcher markiert sind.

Die weitere Entwicklung mit den (zusätzlichen) Grundstellungen `FRY`, `HGB`, `HSY` und `IJB` zeigt Tabelle 4.27 unten.
Weiter werden die Blätter `TMZ`, `WMC`, `XBY` und `EIR` hinzugefügt (Tabelle 4.28 oben) und schliesslich `EIS`, `THR` und `LTQ` (Tabelle 4.28 unten). Das einzige noch verbleibende Loch ist bei der Stellung Q der mittleren Walze und U der ersten Walze zu finden. Tabelle 4.29 zeigt die Anzahlen der noch offenen Löcher nach Auflegen der ZYGALSKI-Bögen für die in der linken Spalte gegebenen Grundstellungen und die in der ersten Zeile ausgewiesenen Walzenlagen.

[31] WELCHMAN a), S. 91

Verfahrenssimulation.
Walzenanordnung: 321; Umkehrwalze B; Ringstellung: GQU;
250 Grundstellungen und Indikatoren; 7 Steckerverbindungen

ABM EOKKCI	AEH AMUAMI	AKN VIDSUO	ASF BPCRWY	AUK ZTEUJM	BIA WFVEVA
BJQ FQRTJX	BLP SVEVGJ	BML IKOKUA	BOH LIELGT	BQY DWVQKA	BRP YMENVS
CDL RRUIMG	CDP EUUBSW	CFN UVOBEM	CJI MUMSEQ	CJK TPFMFT	CKA AWPKSM
CLH GJAXBR	CNY GMFIXZ	CPU COVALU	CRO JHKKNT	CSW MCASCM	CXK DPDGLC
CYH ACAYKF	DFG KCARPF	DJY WVRFQS	DMR UTEJRR	DOQ GHXPOZ	DQS FBHLDQ
DRV XDCMZU	DUX FKDUXA	DXS IJOTQO	DZG QEZTAI	EBP QKJJRD	EHQ WIHUIH
EJZ SJYFJU	EMC FFMKIA	EMV DNWBIR	ENV BGMLNM	EPR KQZGPI	ERH VXUOGX
EUR NOMNES	EXQ VYZNUW	FGE RUXFYG	FMX GYKROC	FOL PTYPCY	FRX TPSVPN
FTY JQWQEJ	FVW QLNGBD	FZI MPEAIE	GCM QJRYAG	GHD AOKVUP	GID IQRMJW
GIT VDFWIK	GOS YJBZLI	GVJ WEWJOQ	GYR YOPETV	HEB ONPPPC	HGZ DNGZBG
HNX WQRNAY	HSX LIBOIJ	HSX PBFUER	HVK NMLRLX	HVL XGZTLR	HVT TXZSZU
HWX SQWWVS	HXR JPXPMN	HXU ZJYCTK	HYW CPDRNX	HZV EJAXMW	IBO QJSGKL
ICW ORZSGV	IJB EAXEDG	IKJ LXGLVU	IKQ GNHMGE	ILF AUGDBF	ILV RKGMNY
IMG CTUPOZ	IMQ LFUDEC	IRK IUPHPP	IRM NWXHWA	ISR FHITVH	ITQ YFUXCM
IUX QZFAQV	IWE MAIFDG	IZS FFCQHJ	IZU TANYRB	JAZ AESFVF	JPA MNGCQU
JSF CBQKHY	JTR NRDACF	JWO NCQIFC	JZC SMAFPQ	JZL WHMDRN	KDR YLSTTG
KGX RKWBCR	KGZ KIPNWR	KIZ NKIRZC	KOM FNWMYF	KQC EJRFNG	KTZ JCRIXB
KUX GXHPEQ	KVA YLEARY	KZT UCNVWD	LAD QRPMWG	LAP JIMIGC	LEX RIGDPT
LHB ECWCJY	LHZ ZRFQEL	LJC OILUXO	LNJ MEJJPY	LOI NHHQTA	LOW VCNTTD
LSP NDWYDR	LUC VOOENU	MAF KNOSVN	MEQ CQJMWP	MFS BLQYCX	MGC MFRCJV
MGV TYYHND	MOI ZLHCPY	MOK LKBXBO	MON ALCQAH	MRF LAOSSH	MSP XNFUJM
MTQ XNXRWD	MTU BAAICD	MUN IVVOCM	MVA CMJPTC	NFR LQZCWL	NFY UKUMCR
NGV BENGBK	NHQ DWFYNQ	NPE PGTZON	NPJ BYGDVH	NPY XNXWUL	NSJ FCZLEV
NTI ECJNQL	NXU NSZTGR	NZR ZRPTKY	ODB HKHSPL	ODR UENKRC	ODU ORUITG
ONB FEZOYA	OQI BHRRGX	OTD TEAFLY	OTR ADLKEB	PFE KYUWRR	PHU HEVWAZ
PJY NJTRFN	PNO LOSGYS	PQX EQHBCI	PRL FWKMHI	PSN AXWAFB	PTJ FQRXJC
PUN JTTEJF	PVM QLWXHC	PXT CLOHMA	PYH GPZHBT	QCJ SADDII	QEA JTEREO
QEJ XTCSSF	QEP BFOOYR	QFL GIMAOU	QFN UPXBLL	QIZ QFTKJG	QJE CSNNVF
QMD RLYWZH	QMS NVXTTO	QMU MVJZQP	QOP BVURSI	QOR KDIRYD	QVP ZOPDSI
QXJ NWELQV	QXV UGCGHU	QYF DGHPYI	QYS XHELOT	RCG GRIJUA	RHE DZFUMA
RHG OLLDFV	RLN CSZSGQ	RNX QVTGRS	RSJ PJCOON	RYH USEHZN	SJK EBWSVE
SKZ XWOUUY	SLJ OWWCQG	STG FRBGUS	TAQ BEQLMF	TDF DDLXOX	TEB CIDKBO
TGP GAJSNJ	TJQ BAGPLA	TMY XNTNNR	TXJ FLENPJ	TZQ FOWLRZ	UCJ CVNUXO
UDB OQLQUE	UFV LQDCEW	UGR WNYQPX	UIW VQJTHT	UOK SFNWDO	UPE SAXNQJ
UVJ PJGIJX	UVX BQZCNO	UZK FQYGEH	UZS OKLNAE	VAB HASPEL	VAF HODOYH
VBI TMENBT	VEQ CHKZAD	VHU HMTDQS	VKM XXIBBL	VMF TYXOBN	VOR ATXSHE
VRW XENJUE	VWH YHMVEO	VYQ QTVPPN	WFT YPZRZY	WMA UYUADU	WOV RDHWVD
XBW DZWQDW	XEZ CTGLQZ	XFA SMHODF	XFS TQLBPQ	XLK BHQGGS	XRW USXOCA
YBA OJIAIE	YBF VGTWFY	YBV JHZAOE	YFV ICSKGH	YFW AOMYSL	YJS XOCGEX
YKQ REBGYZ	YLK YPMAFX	YUL SGPNRK	YUV XDMHLG	YWA YHLOQY	YWE MLVXHT
ZBN FCTXIO	ZEY QHKGYQ	ZFY ASBOWD	ZJO NRNIKG	ZJW TZRYYA	ZNG YQKHZV
ZQD ERCJNS	ZVM PBLDLY	ZYL MMJTNO	ZYM LFUBWZ		

Es gibt 25 Fälle von «[females»

AMUAMI LIELGT MCASCM IJOTQO WIHUIH SJYFJU BGMLNM NOMNES PTYPCY
TPSVPN MPEAIE DNGZBG LIBOIJ EAXEDG LXGLVU IUPHPP NWXHWA NDWYDR
LOSGYS AXWAFB GAJSNJ XNTNNR PJGIJX UYUADU DZWQDW

Tabelle 4.26:

```
                        schnelle Walze ⟶
        Ring            a z y x w v u t s r q p o n m l k j i h g f e d c b
        a               . . o . . . . . . . . . . . . . . . . . . . . . . .
        z               o o . . . . . . . . . . . o . . . . . . . . . . . o
        y               . . . . . . . . . . . . . . . . . . . . . . . . . .
        x               . . . . . . . o . . . . . . . . . . . o o . . . . .
        w               . . . . . . . . . . . . . . o . . . . . . . . . . .
m       v               o . . . . . . . . . . . . . . . . . o . . . . . . .
i       u               . . o . . . . . . . . . . . . . . . . . . . . . . .
t       t               . o . . . . . . . . . . . . . . . . . o . . . . . .
t       s               . . . . . . . . . . . o . . . . . . . . . . . . . .
l       r               . . . . . . . . . . . . . . . . . . . . . . . . . .
e       q               . . . . . . o . . . . . . . o . . . . o . . . . . .
r       p               . . . . . . . . . . . . . . . . . . . . . . . . . .
e       o               . . . . . . . . . . . . o . . . . . . . . . . o . .
        n               . . . . . . . o . . . . . . . . . . . . . . . . . .
W       m               . . . o . o . . . . . . . . . . . . . . . . . . . .
a       l               . . . o . . . . . . . . . . . . . . . . . . . . . .
l       k               . . . . . . o . . . . . o . . . . . . . . . . . . .
z       j               . . . . . . . . . . . . . . . . . . . . . . . . . o
e       i               . . . . . . . o . . . . . . . . . . . . . . . . . .
↓       h               . o . . . o . . . o . . . . . . . . . . . . . . . .
        g               . . o . . . . . . . . . . . . . . . . . . . . . . .
        f               . . . . . . . . . . . . . . . . o . . . o . o . . .
        e               . . . . . . . . . . . . . . . . . . . . . . . . . .
        d               o . o . . o . . . . . . . . o . . . . . . . . . . .
        c               . . . . . . . . . . . . . . o . . . . . . . . o . .
        b               . . . . . . . . . . . . . o . o . o . . o . . . o .
```

```
                        schnelle Walze ⟶
        Ring            a z y x w v u t s r q p o n m l k j i h g f e d c b
        a               . . . . . . . . . . . . . . . . . . . . . . . . . .
        z               . . . . . . . . . . . . . . . . . . . . . . . . . .
        y               . . . . . . . . . . . . . . . . . . . . . . . . . .
        x               . . . . . . . . . . . . . . . . . . . . . . . . . .
        w               . . . . . . . . . . . . . . . . . . . . . . . . . .
m       v               . . . . . . . . . . . . . . . . . . . . . . . . . .
i       u               . . . . . . . . . . . . . . . . . . . . . . . . . .
t       t               . . . . . . . . . . . . . . . . . . . o . . . . . .
t       s               . . . . . . . . . . . o . . . . . . . . . . . . . .
l       r               . . . . . . . . . . . . . . . . . . . . . . . . . .
e       q               . . . . . . o . . . . . . . . . . . . . . . . . . .
r       p               . . . . . . . . . . . . . . . . . . . . . . . . . .
e       o               . . . . . . . . . . . . . . . . . . . . . . . . . .
        n               . . . . . . . . . . . . . . . . . . . . . . . . . .
W       m               . . . . . . . . . . . . . . . . . . . . . . . . . .
a       l               . . . . . . . . . . . . . . . . . . . . . . . . . .
l       k               . . . . . . . . . . . . . . . . . . . . . . . . . .
z       j               . . . . . . . . . . . . . . . . . . . . . . . . . .
e       i               . . . . . . . . . . . . . . . . . . . . . . . . . .
↓       h               . . . . . o . . . . . . . . . . . . . . . . . . . .
        g               . . . . . . . . . . . . . . . . . . . . . . . . . .
        f               . . . . . . . . . . . . . . . . . . . . . . o . . .
        e               . . . . . . . . . . . . . . . . . . . . . . . . . .
        d               . . . . . . . . . . . . . . . . . . . . . . . . . .
        c               . . . . . . . . . . . . . . o . . . . . . . . . . .
        b               . . . . . . . . . . . . . o . . . . . . . . . . . .
```

Tabelle 4.27:

schnelle Walze ⟶

	Ring	a	z	y	x	w	v	u	t	s	r	q	p	o	n	m	l	k	j	i	h	g	f	e	d	c	b
	a	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	z	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	y	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	x	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	w	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
m	v	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
i	u	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
t	t	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
t	s	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
l	r	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
e	q	.	.	.	.	.	.	o	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
r	p	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
e	o	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	n	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
W	m	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
a	l	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
l	k	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
z	j	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
e	i	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
↓	h	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	g	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	f	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	e	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	d	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	c	.	.	.	.	.	.	.	.	.	.	.	.	.	.	o	.	.	.	.	.	.	.	.	.	.	.
	b	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.

schnelle Walze ⟶

	Ring	a	z	y	x	w	v	u	t	s	r	q	p	o	n	m	l	k	j	i	h	g	f	e	d	c	b
	a	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	z	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	y	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	x	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	w	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
m	v	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
i	u	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
t	t	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
t	s	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
l	r	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
e	q	.	.	.	.	.	.	o	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
r	p	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
e	o	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	n	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
W	m	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
a	l	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
l	k	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
z	j	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
e	i	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
↓	h	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	g	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	f	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	e	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	d	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	c	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
	b	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.

Tabelle 4.28:

Walzenlage Grundst.	I,II,III	I,III,II	II,III,I	II,I,III	III,I,II	III,II,I
CSX	263	280	250	291	300	254
EJA	95	126	83	101	134	108
ENX	33	58	22	34	62	46
FRY	16	24	9	12	32	23
HGB	8	11	4	4	14	15
HSY	3	6	1	3	6	10
IJB	1	2	-	3	2	6
TMZ	-	-	-	1	1	5
WMC	-	-	-	1	-	3
XBY	-	-	-	1	-	2
EIR	-	-	-	1	-	2
EIS	-	-	-	-	-	2
THR	-	-	-	-	-	1

Tabelle 4.29:

Die ermittelten möglichen Ringstellungen für alle Walzenlagen und alle Grundstellungen der langsamen Walze lauten:

Walzenlage	Ringstellung
III, II, I	G Q U
III, I, II	D W I
II, III, I	---
II, I, III	---
I, II, III	O V P
I, III, II	P B F

Mit diesen möglichen Ringstellungen muss nun die „Rückübersetzung“ der Indikatoren in die (verdoppelten) Spruchschlüssel versucht werden. Tabelle 4.30 zeigt die Ergebnisse.

Ringstellung GQU, Walzenlage III, II, I,

Grundstellung	Indikator	Textschlüssel
E H Q	WIH UIH	EDU EDX
I R K	IUP HPP	GNI ANI
Q C J	SAD DII	PQY IXQ
V K M	XXI BBL	IVY QFV
H E B	ONP PPC	QAT SAS
T M Y	XNT NNR	OXZ IXZ

Ringstellung DWI, Walzenlage II, I, II

Grundstellung	Indikator	Textschlüssel
E H Q	WIH UIH	AJC JAG
I R K	IUP HPP	RPT CLK
Q C J	SAD DII	LDQ TTD
V K M	XXI BBL	SOH KDH
H E B	ONP PPC	ZRR GTY
T M Y	XNT NNR	RQM DJZ

Ringstellung OVP, Walzenlage I, II, III,

Grundstellung	Indikator	Textschlüssel
E H Q	WIH UIH	DUQ EFR
I R K	IUP HPP	XFW ONQ
Q C J	SAD DII	ODI QDW
V K M	XXI BBL	JYZ ZVO
H E B	ONP PPC	IGV SIS
T M Y	XNT NNR	NYE ATI

Ringstellung PBF, Walzenlage I, III, II

Grundstellung	Indikator	Textschlüssel
E H Q	WIH UIH	DUQ EFR
I R K	IUP HPP	LCZ GEM
Q C J	SAD DII	AZY JOZ
V K M	XXI BBL	EQG YNR
H E B	ONP PPC	DED BGU
T M Y	XNT NNR	ZNU YJH

Tabelle 4.30:

Es ist deutlich, dass nur die Ringstellung GQU bei der Walzenlage III, II, I weiteren Erfolg verspricht. WELCHMAN, der die Lochblätter in Unkenntnis der Ergebnisse von ZYGALSKI und der Arbeit von JEFFREY noch einmal erfunden hatte, gibt aber sehr richtig an, dass durch das Aufeinanderlegen der Lochblätter nur die Anzahl der zu prüfenden Möglichkeiten verringert werden konnte. Die meisten Versuche wären allerdings Fehlschläge gewesen.[32] Bis Mitte Dezember 1938 waren vom polnischen 3-Mann-Team immerhin zwei vollständige Sätze zu je 26 solcher Lochblätter angefertigt worden.[33]

Die weitere Entwicklung, nämlich zuerst den genauen Spruchschlüssel festzustellen und dann die Steckerlage mit Hilfe der Kenntnis von stereotypen Wendungen usw. herauszufinden, lief nach der oben gezeigten Methode ab.

Bei GAJ sind die Zeiten in Mannstunden angegeben, die für die einzelnen Schritte im Mittel anzusetzen waren:[34]

3 bis 4 Std. Ermittlung des Spruchschlüsses bei Voraussetzung verschiedener Buchstaben
1/2 Std. Bestimmung der Eingangswalze
3 Std. Steckerstellungen
1/2 Std. Stellung der restlichen Walzen (Katalog)
1 bis 2 Std. Ringstellungen
8 bis 10 Std. Geschätzter Gesamtaufwand

Bei 70 bis 90 Sprüchen eines Tages war i.a. auch der Tageschlüssel zu finden.
Zur Anzahl der «females», die notwendig waren, um den weiter zu untersuchenden Rest hinreichend zu verkleinern, hat WELCHMAN (für 1–4 «females») folgende Berechnung gegeben:[35]

> Zwei, um drei Stufen auseinander liegende Positionen der schnellen Walze (I und II) werden betrachtet. In jeder der beiden Positionen findet eine Permutation des Alphabets statt mit der durch die Umkehrwalze bedingten Eigenschaft der Umkehrung. Es gibt also in jeder der beiden Positionen 13 Buchstabenpaare. Die Wahrscheinlichkeit, dass z.B. der erste Buchstabe eines Paares aus I auch in II mit demselben zweiten Buchstaben wie in II ein Paar bildet, ist 1:25. Da es in I und in II je 13 Paare gibt, ist die Wahrscheinlichkeit, dass ein Paar aus I auch in II auftritt 13:25. Damit ein female entsteht, muss einer der beiden Buchstaben aus so einem wiederholten Paar gleich dem (ersten) Buchstaben des Spruchschlüssels sein. Die Wahrscheinlichkeit dafür ist 1:13. Somit ergibt sich die Wahrscheinlichkeit für das Auftreten eines 1–4 «females»zu
>
> $$(13:25)\cdot(1:13) = 1:25.$$
>
> Weiter gibt WELCHMAN die Wahrscheinlichkeit für das Auftreten eines 1–4 - oder eines 2–5 - oder eines 3–6 - «females»zu 3:25 oder etwa 1:8 an. Dabei berücksichtigt er nicht evtl. gleichzeitiges Auftreten (*aut* statt *vel*).

Dasselbe Ergebnis findet sich auch bei HEIDER-KRAUS-WELSCHENBACH[36], wobei die Voraussetzung genannt wird, dass die regellosen Zuordnungen beliebig wählbar seien, dass es sich bei der Chiffrierung also um eine beliebige Permutation handele. Diese Voraussetzung übersieht aber die Abhängigkeiten der Verwürfelung von Randbedingungen, nämlich von der vorherigen Stellung der Walzen. Bei DEAVOURS/KRUH ist als Beispiel genannt:[37]

---

[32] WELCHMAN a), S.89/90
[33] KOZACZUK b), S. 266
[34] GAJ, S. 132
[35] WELCHMAN b), S. 61 ff.
[36] HEIDER, KRAUS,WELSCHENBACH, S. 151
[37] DEAVOURS/KRUH a), S. 101

> Sowohl `BFR` $\mapsto$ `BFS` als auch `AER` $\mapsto$ `BFS` können für die Walzenanordnung III, II, I gelten. Im zweiten Fall kommt die Eigenheit zum Tragen, dass die mittlere Walze, wenn sie das Weiterrücken der langsamen Walze induziert, selbst auch noch einmal rückt.

Offenbar muss das Ergebnis der reinen Wahrscheinlichkeiten korrigiert werden durch einen systemtypischen Faktor, der auf dem Weiterrücken der mittleren und der linken Walze beruht.
In der Praxis liefern rd. 40% aller Stellungen der drei Walzen Festpunkte. Diese Angabe ist durch Auszählen der Ergebnisse aller möglichen Walzenstellungen (d.h. des Zyklenkataloges aus Kap. 4.2) für alle Walzenlagen bestätigt worden. Diese Abweichung wäre mit einem Faktor 20:26 (Anteil der nicht durch vorherige Positionen beeinflussten Buchstaben) erklärbar:

$$(13{:}25)\cdot(20{:}26) = 2{:}5$$

Mit dieser Korrektur wird auch die theoretisch zu 1:25 ermittelte Wahrscheinlichkeit für das Auftreten eines «females»in einer Stufe durch $(2{:}5)\cdot(1{:}13) \approx 3$ % mit der Realität in Deckung gebracht. Die Auszählung von 17·250 Fällen ergab etwas unter 3,3% für die Häufigkeit, mit der in einer Stufe allein ein female auftrat.

4.3.1.1 Walzen IV und V.

Am 15. 12. 1938 wurden Walze IV und V eingeführt. Ihre Verdrahtungen sind in Kapitel 1.1 auf Seite 6 angegeben.

Durch die so von 6 auf 60 gewachsene Anzahl von Kombinationen von je drei Walzen ergaben sich neue Probleme:

1) Die inneren Verbindungen der neuen Walzen mussten ermittelt werden.

2) Für die vollständige Nutzung der bisherigen Vorgehensweise fehlten nunmehr 58 Sätze der ZYGALSKIschen Lochblätter zu je 26 Blättern statt bisher nur vier, sowie 54 weitere BOMBAs (mit je sechs Walzensätzen).

Zu 1) Hier half entscheidend die Tatsache, dass im SD - Funknetz noch immer nach dem alten Chiffriersystems gearbeitet wurde, wie es in allen Bereichen vor dem 19.9.1938 angewandt worden war. Mit der Rastermethode wurde nach einem Tag gesucht, an dem eine der schon bekannten Walzen die erste Walze war. Unter der Annahme, dass eine der beiden restlichen Walzen eine neue, die andere eine alte, schon bekannte, war, fand das polnische Team die inneren Verdrahtungen der neuen Walze wie 1932 die der damals dritten.[38] Angeblich soll der polnische Geheimdienst schon seit Monaten gewusst haben, dass im Falle grosser internationaler Spannungen zwei zusätzliche Walzen, die sog. Mobilisierungswalzen, eingeführt werden würden. Sie sollen auch den Spruch dechiffriert haben, der die Anweisung gab, diese neuen Walzen einzusetzen.[39]

Zu 2) Zwar stellte die AVA einige wenige Duplikate der Walzen IV und V her, damit wenigstens im SD - Netz weiter Erfolge erzielt werden konnten. Die Anfertigung so vieler zusätzlicher Walzensätze überstieg jedoch die technischen und finanziellen Möglichkeiten der Polen.

---
[38] KOZACZUK b), S. 266
[39] BLOCH b), S. 200

> Trotz der Kenntnis aller Walzen war selbst das Entziffern des SD - Netzes nicht einfach. Zwar wurde manchmal die erste Walze — z.B. mit der Uhrenmethode (siehe Kap. 4.2.1, S. 93) — identifiziert, aber weitere Fortschritte wurden seltener, denn am 1.1.1939 wurde die Anzahl der Steckerpaare auf sieben bis zehn erhöht, was die Rastermethode nahezu wirkungslos werden liess. Die militärischen Netze waren nunmehr nur noch dann mit Erfolg anzugehen, wenn die drei Walzen die alten aus der Zeit vor dem 15.12.1938 waren. Im Mittel war das aber nur in etwa 10% der Tage der Fall.[40]

1.7.1939 übernahm dann auch das deutsche SD-Netz das Verfahren vom 15.9.1938, wahrscheinlich bezieht sich HINSLEY darauf als die Änderungen vom 1.7.1939.

Das bisher beschriebene Vorgehen umfasste auch Sprüche der deutschen Marine bis Ende April 1937. Bis dahin waren am Anfang und am Ende jedes Spruchs jeweils die erste bzw. die zweite Gruppe des chiffrierten verdoppelten Spruchschlüssels zu finden. Ab 1.5.1937 wurde bei der Marine aber das Indikatorsystem geändert (s.o. unter Schlüssel M). Es waren viele Sprüche mit Fortsetzungen darunter, deshalb war es möglich, mit ihrer Hilfe Tagesschlüssel für den 8. Mai zu ermitteln. Die Briten nannten die Methode FORTYWEEPY (siehe Kap. 1.3.2.2). Dabei stellten die Kryptologen fest, dass seit dem 30. April keine Änderung eingetreten war.

Als dann das Torpedoboot mit dem Rufzeichen AFÄ bis zum 4. Mai noch im alten System funken musste, weil es die neuen Vorschriften nicht besass, war es möglich, im Zeitraum bis zum 8.5. etwa 100 Sprüche zu lesen. Da das neue Indikator-Verfahren aber nicht bekannt war, mussten hier die Bemühungen um die Sprüche der Marine eingestellt werden.

---

[40] REJEWSKI b), S. 267

Kapitel 5

Arbeiten in Frankreich und Grossbritannien bis 1939

5.1 Vorfeld

Die deutsche Chiffriermaschine ENIGMA erregte auch die Aufmerksamkeit mindestens britischer und amerikanischer Stellen. 1925 soll D. KNOX in Wien bereits eine kommerzielle ENIGMA gekauft haben[1]. 1927 bekam FOSS den Auftrag, die „small machine“ zu untersuchen. Aus seinem Bericht über diese Maschine folgt aber, dass es sich dabei um den Typ D gehandelt haben muss, weil die Eingangswalze die Zeile QWERTZU... aufwies[2] Dabei stellte er fest, dass bei bekannter Verdrahtung der Walzen bereits 15 Klartext-Geheimtext-Paare ausreichen, um die Identität und die Stellung der rechten Walze zu ermitteln. Wenn die Walzenverdrahtung nicht bekannt ist, reichen 180 Paare zur Bestimmung der relativen Verdrahtung der rechten und der mittleren Walze. Im Mai 1928 erstand z.B. der amerikanische Militärattach ein Exemplar für 600 RM. Ebenfalls 1928 kaufte die britische Admiralität zwei kommerzielle ENIGMAs („D“) um sie daraufhin zu prüfen, ob sie zur Chiffrierung der besonders geheimen Nachrichtenverbindungen der britischen Regierung geeignet wäre. Es wurde ein hoher Grad an Sicherheit festgestellt, aber auch ihre kryptographische Verwundbarkeit. 1935 entschied sich das verantwortliche Komitee endgültig gegen die ENIGMA und gab eine auf ähnlichem Prinzip aufgebaute Maschine in Auftrag, die spätere TypeX, die ab 1939 bei der Army und der Air Force bis hinunter zur Ebene der Divisionen eingeführt wurde. Alle Experten waren sich einig, dass beide Maschinen Geheimtexte lieferten, in die (mit den damals bekannten Methoden) kein Einbruch möglich wäre, sofern sie fehlerlos angewandt würden. Diese Ansicht erwies sich im Nachhinein durchaus als richtig.

Das deutsche Heer stellte 300.000 RM in den Etat ein, um Chiffriermaschinen anzuschaffen.

Ein undatiertes Dokument (wahrscheinlich von 1930) zeigt, dass bereits Stecker verwendet wurden[3]. In der Tat übergaben die Franzosen den Briten 1931 u.a. Fotos der deutschen Heeres-ENIGMA, die an der Vorderseite einen unbekannten Zusatz zeigten. Es handelt sich dabei sicher um die in Kap. 1.1 genannten Dokumente. Die Funktion des Zusatzes wurde aber im September 1938 noch nicht verstanden. Diese Materialien wurden als nicht ausreichend wertvoll angesehen, um den Franzosen eine gemeinsame

[1] FOSS a)

[2] FOSS b)

[3] FOSS a), S. 3: «There is an undated translation of a secret German document published in 1930 which describes the method of plugging in the stecker, but does not give the cryptographic effect»

Arbeit vorzuschlagen oder einen finanziellen Beitrag zu leisten. Erst 1936 wurden Gespräche mit dem französischen Generalstab neu aufgenommen, und es wurde erwogen zu prüfen, ob das Indikatorsystem die Möglichkeit einer Rekonstruktion der Maschine böte, vorausgesetzt es lägen hinreichend viele Sprüche vor. Dabei tauschten Briten und Franzosen nur Abhörprotokolle von aufgefangenen Sprüchen aus.

Auch Schweden, Polen, die Niederlande und Japan kauften ENIGMAs. Die nationalspanischen Truppen und die italienischen Truppen im spanischen Bürgerkrieg (Kap. 3.2) wurden mit ENIGMAs vom Typ „D“ ausgestattet.

Es wird gelegentlich behauptet, die ENIGMA soll 1933 vom Markt genommen worden sein. Dem widerspricht nicht der Kauf von 80 Chiffriermaschinen ENIGMA durch die schweizer Streitkräfte im Frühjahr 1938 (14 Stück ENIGMA K)[4]. Der Stückpreis betrug 1941 nach schweizer Angaben 760 RM. 1942 besass die Schweiz 265 ENIGMAs.

1936 versuchte sich D. KNOX in GC&CS[5] an ENIGMA-Sprüchen mit der für die steckerlose ENIGMA geeigneten Streifenmethode («méthode des bâtons»), kam aber nicht zur Lösung, weil er von der falschen Voraussetzung ausging, die Eingangswalze wäre wie bei der kommerziellen ENIGMA verdrahtet (QWERTZU...). Nach der Änderung des Schlüsselverfahrens April 1937 resignierte DENNISTON[6]. Ende 1937 hatte man in GC&CS die Hoffnung aufgegeben, die mit der Marine-ENIGMA chiffrierten Sprüche zu lesen. Im Oktober 1938 nach der Münchenkrise mit vergeblichen weiteren Versuchen der Dechiffrierung meinte DENNISTON sogar, im Ernstfalle sei die ganze GC&CS nutzlos.

Die Briten wollten die Franzosen veranlassen, Informationen zur Heeres-ENIGMA zu liefern. PAILLOLE sagt, BERTRAND hätte im Frühjahr 1938 Schlüsselblätter geliefert, aber eine Denkschrift der GC&CS vom September 1938 weist nur auf das 1931er Material hin.

1937 isolierte JACOB aus den Funksprüchen von Heer und Luftwaffe zwischen Deutschland und Spanien (inzwischen war in Spanien der Bürgerkrieg ausgebrochen) eine kennzeichnende Gruppe aus jeweils drei Buchstaben („Diskriminante“), deren Position im Spruch von Tag zu Tag wechselte[7]. Für jede Funklinie bestand sie aus einer Permutation von vier Trigrammen. Wenn zwei Funklinien an einem Tage die gleichen Trigramme benutzten, hatten sie auch gemeinsame Indikatoren (Spruchschlüssel) und Grundstellungen an der ENIGMA.

Im September 1938 wurden zwischen Grossbritannien und Frankreich die Frequenzen des Marinefunkverkehrs ausgetauscht, eine weitere gegenseitige Unterrichtung über Rufzeichen und Funkpeilungsergebnisse wurde vereinbart.
Weiter wurden die Franzosen gebeten, Informationen zu geben über

a) Details zu den maschinellen Unterschieden der einzelnen Enigma-Modelle
b) Die bei der deutschen Wehrmacht gängigen Verfahren zu
  1) Evtl. neue Chiffrierwalzen
  2) Reihenfolge der Walzen
  3) Einstellung der Ringe
  4) Länge der Periode der Gültigkeit von 1) bzw. 2)
c) Wer bestimmt die Nrn.1) bzw. 2) ?
d) In den militärischen Sprüchen ist eine Buchstabengruppe bei wechselnden Positionen beobachtet worden. Hat sie ausser der Unterscheidung der Funklinien noch eine andere Aufgabe ?
Gibt es Informationen über Schlüssel unterer Wehrmachteinheiten ?

[4]Schreiben des Armeekommandos der schweizerischen Armee vom 20.1.40, Schweizerisches Bundesarchiv
[5]Zum Begriff GC&CS siehe Kap.6.2.1
[6]DENNISTON leitete die GC&CS seit ihrer Gründung am 24.10.1919, bis er im Frühjahr 1942 auf einen weniger einflussreichen Posten befördert wurde (WEST, S. 73)
[7]FOSS a), s. 5)

Zu dieser Zeit waren 34 Frequenzen der Luftwaffe bekannt. Es wurden aber noch mehr Einzelheiten zum Funkverhalten der Wehrmacht benötigt[8].

Im November 1938 fand in London ein Treffen zwischen Franzosen und Briten statt. Ausgetauscht wurden Berichte über gefundene Tagesschlüssel bzw. Spruchschlüssel bis zum 15. 9. 1938. GC&CS wartete noch immer auf weitere Abhörprotokolle (beschränke Abhörmöglichkeiten in Grossbritannien) für die Zeit bis September 1938, die über die etwa 100 Dokumente verschiedener Wichtigkeit hinausgingen. BERTRAND lieferte allerdings vier Heeressprüche mit Klartext, Steckerlage und Walzenlage (I, II, III). Andere Quellen, z.B. FOSS, behaupten, es habe sich um künstliche Sprüche von Agenten mit Zugang zur ENIGMA ohne Stecker, mit Ringstellung `AAA` gehandelt, ausserdem Angaben über deutsche Heeresfunknetze, ausserdem Fotos und Diagramme, die die Rolle der Stecker zeigten. Erst zu diesem Zeitpunkt sollen die Briten Kenntnis der Dienstvorschriften zu ENIGMA erhalten haben.

BERTRAND liess darüber hinaus noch die Chiffrate der 26 Buchstaben des Tastenfeldes für gewisse Walzenlagen an die Briten übergeben.

Eine Liste von Material wurde aufgestellt, das von Agenten beschafft werden sollte:

> Für etwa 1000 Buchstaben die Klartext-Geheimtext-Paare
> Monatliche Schlüsseltafeln.

Am 9. und 10. Januar 1939 fand in Paris ein Treffen der Chefs der britischen, französischen und polnischen Dienste statt. Dabei erläuterte KNOX seine aufwendige, wie sich später hersusstellte, der der Polen ähnliche Methode («SAGA», s.u.), ähnlich der REJEWSKIs für die ersten drei Walzen und die Umkehrwalze und bat BERTRAND um 16 Geheimtexte für bestimmte Stellungen, falls er nicht die Verdrahtungen der Walzen selbst liefern könnte. Dafür wurde für Agenten eine genaue Anweisung der Vorgehensweise entwickelt, um die Alphabete zu den Walzenstellungen

```
AAA, AAB, AAC, AAD
ABA, ABB, ABC, ABD
ACA, ACB, ACC, ACD
ADA, BAA, CAA, DAA
```

zu beschaffen. Der Vergleich mit Kap. 3.1.1 zeigt, wie zielgenau diese Alphabete ausgewählt worden waren. Weiter sollten die Walzenschaltungen beschafft werden. KNOX meinte dazu, die Agenten sollten zunächst an kommerziellen ENIGMAs „üben“ Es sollten weiter Anstrengungen unternommen werden, Sprüche aus der Zeit vor dem 15.9.1938 zu lesen, um damit u.U. genügend viele isomorphe Geheimtexte zu finden, damit für die Zeit nach dem 15.9. evtl. Erkenntnisse verwertet werden könnten.

Die polnischen Vertreter zeigten Erfolge bei der Identifikation der Indikatoren und Lösungen der Schlüssel mit doppeltem Transposition. Die Franzosen zeigten sehr umständliche Verfahren, im übrigen aber weder Kenntnis noch Interesse an der ENIGMA K, bzw. ENIGMA D, der Italiener und Spanier. Sie hatten auch den groben Fehler der Italiener, mehrere Sprüche mit denselben Schlüsseln zu senden, nicht ausnutzen können. Die Briten erläuterten ihr System, das später bei TURING als «SAGA»bekannt wurde. (Vgl. Kap. 3.1.1) Ansonsten liess keiner der Anwesenden seine Erfolge durchblicken. Die polnischen Vertreter waren nicht autorisiert, über ihre Erfolge im Zusammenhang mit der ENIGMA zu berichten. Es waren vom polnischen Geheimdienst bislang auch noch keine dechiffrierten ENIGMA-Sprüche an die verbündeten Dienste geliefert worden. Man stellte nur gemeinsam fest, dass ohne weiteres Agentenmaterial wohl kein

[8] Die Angaben in den letzten drei Absätzen beruhen auf FOSS a)

Fortschritt möglich wäre. Immerhin sollten zwischen Frankreich und Grossbritannien Verbindungsoffiziere ausgetauscht und eine Fernschreibverbindung eingerichtet werden.

5.1.1 PYRY.

Anfang Juli 1939 wurden auf Anordnung des polnischen Generalstabschefs, General STACHIEWICZ, wegen der drohenden Kriegsgefahr die Vertreter der britischen und französischen Dienste für Mitte Juli zu einem geheimen Treffen in PYRY bei Warschau eingeladen.
Teilnehmer waren die drei polnischen Kryptologen REJEWSKI, RÓŻYCKI und ZYGALSKI, dazu die Offiziere LANGER und CIECZKI, aus Frankreich BERTRAND und BRAQUENIQUE, schliesslich aus Grossbritannien der Kryptologe Alastair DENNISTON,Alfred Dillwyn KNOX und Commander Humphrey SANDWITH, ein Spezialist für den Abhördienst der Royal Navy.

Auf dieser am 24. Juli begonnenen Konferenz eröffneten die Polen den überraschten Gästen ihre Erfolge im Entziffern der ENIGMA. Major CIEZKI erläuterte die Methode, aus den Indikatoren (bis 15.9.38) den Spruchschlüssel zu bekommen. Der britische Bericht über PYRY zeigt, dass KNOX inzwischen erkannt hatte, dass man beim neuen System (ab 15.9.1938) die Schlüssel mit Hilfe der «females»erhalten könnte. Er schlug vor, wenn die Verdrahtungen bekannt wären, die female-Positionen auf Film zu registrieren, sah aber die polnischen Lochblätter als praktikabler an. Neu für die Briten war die Verwendung von drei «females»mit gleichen Buchstaben. Ihr „Fehler“ bei ihnen war, dass sie die Eingangswalze falsch eingeschätzt hatten (Tastenfeld statt Alphabet).

In PYRY erfuhren die Briten offenbar nicht, woher die Polen Hilfe erhalten hatten (BERTRAND). Es wurde vereinbart, dass in GC&CS die ENIGMA - Sprüche von Heer und Luftwaffe bearbeitet werden sollten, die Polen sollten die Sprüche der SS behandeln und weiter theoretische Forschung betreiben, während den Franzosen die Sprüche der Marine vorbehalten bleiben sollten.
KNOX glaubte allerdings, dass die Polen nur lügen würden über ihre Erfolge[9]. DENNISTON äusserte sich BERTAND gegenüber sehr kritisch über KNOX, der eine Zusammenarbeit durch mangelnde Teamfähigkeit erheblich erschwere. DENNISTON beklagte sich nach dem Treffen in PYRY, dass das Treffen von englischer Sicht aus ein Flop gewesen sei. Die Rolle BERTRANDs sei überaus undurchsichtig. Erst am zweiten Tage seien von den Polen ihre Methoden genauer erklärt worden. Dabei hätte es sich gezeigt, dass sie genau dort erfolgreich gewesen wären, wo die Engländer versagt hätten. Da auf der Rückfahrt durch Deutschland keine schriftlichen Aufzeichnungen mitgenommen werden konnten, rief KNOX nach der Ankunft in London seinen Mitarbeiter TWINN an und sagte ihm nur, dass QWERTZ... ABCD... sei. Als Resumee war aber erkannt worden, dass die Polen die Unsicherheit der ENIGMA ausgenutzt hätten. Man solle die jungen polnischen Kryptologen nach England holen.
Die Polen liessen den Briten und den Franzosen je eine (nachgebaute) ENIGMA zukommen, zusammen mit der Beschreibung ihres Dechiffrierverfahrens und der ZYGALSKI-Blätter.
Nach Kriegsbeginn zerstörten sie alle Unterlagen und Maschinen, damit den deutschen Truppen keine Spuren der gelungenen Entzifferungen in die Hände fallen sollten. Das Dechiffrierpersonal setzte sich auf Umwegen nach Frankreich ab und baute dort, zusammen mit den Franzosen, eine neue Dechiffrierzentrale auf. (Siehe Kap. 6)

Nach PYRY gaben die Briten den Polen aufgefangene Marine-Sprüche von 1937, diese

[9]FOSS a), handschr. Notizen: «... assuming that no one understoode English raged and roared that they were lying to us as in Paris. The whole thing was a pinch he kept on repeating they never worked it out, they pinched it years ago ...»

dechiffrierten etwa 100 Sprüche aus den ersten acht Tagen von Mai 1937. Sogar nach PYRY war, zumindest bei Teilen der Mitarbeiter in der GC&CS zunächst noch Skepsis vorherrschend, ob sich die deutschen Geheimtexte brechen liessen.

Am 16.8.1939 lieferte BERTRAND das für Grossbritannien bestimmte Exemplar der in Polen nachgebauten ENIGMA in London ab.

Im Vorfeld hatten die Franzosen erwogen, im Falle von Kriegsgefahr die deutschen Geheimdienste wissen zu lassen, dass die ENIGMA gebrochen sei (wozu ein Klartext, durch Agent besorgt, nötig wäre), um so den deutschen geheimen Funkverkehr für gewisse Zeit auszuhebeln. Es war aber doch für klüger angesehen worden, die Tatsache geheimzuhalten, dass Teile des ENIGMA-Verkehrs gelesen worden waren.

In Bletchley Park begannen die Briten Mitte November 1939 mit der Herstellung neuer Lochblätter, die dort «JEFFREY's sheets» genannt wurden. Sie stellten eine andere Form eines Kataloges dar als die ZYGALSKI-Blätter und realisierten die Wirkung von je zwei Chiffrierwalzen und der Umkehrwalze. Es gab eine Verzögerung, weil erst eine Maschine hergestellt wurde, die die Berechnung der Lochkoordinaten schneller ausführen sollte.
Mit diesen neuen Blättern wurden zunächst keine Ergebnisse erzielt, was den Verdacht nährte, das Schlüsselverfahren der ENIGMA wäre mir Kriegsbeginn verändert worden. Es stellte sich jedoch heraus, dass bei dem von Polen an die Engländer übergebenen Material die Positionen der zum Weiterschalten nötigen Aussparungen in der Sperrscheibe bei den Walzen IV und V vertauscht worden waren.

Eine Stellungnahme vom Dezember 1939 sagte, dass die «JEFFREYïs sheets» besser seien als die Zyklometer-Methode. An TURING erging der Auftrag, sich um eine schnellere «Bombe» zu bemühen.

KNOX hatte bemerkt, dass in vielen Fällen Sprüche dort begannen, wo der jeweils vorhergehende geendet hatte. Durch eine Art Subtraktion war es in diesen Fällen oft möglich, zwei der drei Walzen zu identifizieren, was eine erhebliche Erleichterung bei der Anwendung der Lochblätter bedeutete.[10]

[10] P.R.O. HW25/12 Nr. 83440, H.R. FOSS: Reminiscences of the Enigma

Kapitel 6

Alliierte Erfolge ab 1939.

6.1 In Frankreich.

Als die deutschen Truppen im September 1939 in Polen rasch vorrückten, verliess das mit Kryptologie befasste Personal am 6.9.1939 PYRY mit dem Ziel Rumänien (nicht ohne vorher die Anlagen so zu zerstören, dass ihr Verwendungszweck nicht mehr zu erkennen war). In Bukarest boten REJEWSKI, RÓŻYCKI und ZYGALSKI bei der britischen Botschaft ihre Zusammenarbeit an, wurden aber zurückhaltend beschieden. Schliesslich erreichten sie durch Vermittlung der französischen Botschaft Ende September Paris.

Dort warteten sie, bis LANGER und CIEZKI aus einem rumänischen Flüchtlingslager entlassen waren und, zusammen mit zwei ENIGMA-Nachbauten, ebenfalls in Frankreich eintrafen. Der französische geheime Funkaufklärung- und Dechiffrierdienst stand unter der Leitung von Gustave BERTRAND und war unter dem Decknamen P.C. BRUNO im Chateau de Vignolles in der Nähe von Gretz-Armainvillers untergebracht. Dort wurde das polnische Personal mit integriert (die sog. Gruppe „Z“).

Allerdings konnte die Dechiffrierarbeit nicht sofort beginnen, obwohl die Franzosen noch mehr ENIGMA-Nachbauten erstellen liessen. Es fehlten die nötigen Lochblätter.

P.C. BRUNO bestand aus etwa 70 Personen. Das polnische Personal war im wesentlichen für Arbeiten an der ENIGMA vorgesehen. Ende Oktober umfasste diese Gruppe 15 Personen. „Z“ stand unter dem Kommando des polnischen Oberstleutnants LANGER. Eine Personalliste findet sich bei KAPERA[1]. Die Engländer hatten den Franzosen ein gemeinsames Dechiffrierzentrum vorgeschlagen, das von diesen jedoch abgelehnt wurde. Immerhin wurde zwischen BRUNO und dem britischen Kryptologiezentrum in Bletchley Park eine Fernschreibverbindung installiert, und ein britischer Verbindungsoffizier, Captain MACFARLAN, wurde nach BRUNO abgestellt. Das polnische Personal durfte diese direkte Verbindung mit London allerdings nicht benutzen. Ausserdem wurde vereinbart, dass bei BRUNO von der polnischen Gruppe im wesentlichen Forschung betrieben werden sollte, während in Grossbritannien mehr Gewicht auf der eigentlichen Entzifferungsarbeit liegen sollte.

Die Tätigkeit in P.C. BRUNO bzgl. ENIGMA beschränkte sich zunächst auf das Sammeln von Funksprüchen und den Versuch, die einzelnen Funkkreise zu identifizieren. Der britische Abhördienst (Y-Service), der im Gegensatz zum französischen zentral organisiert war, war zu dieser Zeit noch nicht mit hinreichend weit reichenden Empfängern ausgestattet.[2] Die erste Teillieferung der in Grossbritannien gefertigten Lochblätter (24 der nötigen 60 Sätze) wurde am 28.12.1939 für BRUNO bereitgestellt und,

[1] KAPERA, Bericht LANGER, S. 24/25

[2] RIBADEAU-DUMAS, 4 - 4 und WELCHMAN b), S. 103/104

offenbar vom britischen Verbindungsoffizier, am 3.1.1940 dort abgeliefert. Der Rest der Sätze war am 7.1.1940 fertiggestellt und wurde am 17.1.1940 BRUNO zugestellt. (Ob von D. KNOX persönlich[3] oder von A. TURING[4] ist nicht zu klären).

In BRUNO begann „Z“ unverzüglich mit dem Aufarbeiten der angesammelten Funksprüche. Ein Erfolg stellte sich bald ein: Am 17.1.1940 wurde ein Tagesschlüssel vom 28.10.1939 gefunden, der zum Schlüsselkreis für den Verkehr der 20 deutschen Militärbezirke untereinander gehörte. Das war der erste von den Alliierten gelesene ENIGMA-Spruch des Krieges.

Bei einem Besuch LANGERs in London im Dezember 1939 war die Zusammenarbeit zwischen BRUNO und Bletchley Park dahingehend präzisiert worden, dass in BRUNO auch Sprüche bearbeitet werden sollten, für die die Briten den Tagesschlüssel lieferten. Es stand allerdings in BRUNO dafür nur eine einzige ENIGMA zur Verfügung, da eine als Muster für einen Nachbau auseinandergenommen worden war, die zweite für die Forschung reserviert war.

Die ersten Schlüsselkreise erhielten Farbnamen, nach der Farbe des Stifts, mit dem sie in Bletchley Park markiert wurden. Später wurden auch andere Namen verwendet. Der am 17. 1. 1940 erkannte Kreis erhielt den Namen. «Green» . Fast gleichzeitig mit BRUNO ermittelte Bletchley Park den Tageschlüssel für «Green» für den 25. 10. 1939. Mit diesen beiden Erfolgen war auch erwiesen, dass mit Kriegsbeginn auf deutscher Seite keine Änderung des Chiffrierverfahrens vorgenommen worden war.

Vom 17.1.1940 bis Ende März 1940 wurden ausser «Green» noch zwei Schlüsselkreise erkannt:

> «Blue» : Übungsverkehr der Luftwaffe
> «Red» : Allgemeiner Luftwaffenschlüssel, auch zur Verbindung zwischen Heer und Luftwaffe.

«Blue» war relativ uninteressant, «Green» selten gebrochen (wahrscheinlich wegen zu geringer Anzahl von Sprüchen), daher konzentrierte sich die Aufmerksamkeit auf «Red». Ende April waren in diesem Schlüssel die Erfolge vielversprechend. Als erster Tagesschlüssel von «Red» wurde der vom 6.1.1940 gefunden.

Auch aus Gründen der Lage der Abhörstationen lag das Schwergewicht in Grossbritannien bei «Red», in BRUNO bei «Green». Von diesen drei Kreisen wurden in der angegebenen Zeit etwa 50 Tageschlüssel herausgefunden.

Diese ersten Durchbrüche waren nicht sehr ertragreich (im wesentlichen Verwaltungsangelegenheiten) und mit dreimonatiger Verzögerung. Aber die Dinge besserten sich. Das Journal de Marche des Colonel RIVET (Chef des 5ième Bureau SR-SCR[5]) erwähnt am 6.3.1940, dass nunmehr die taktische Auswertung der Dechiffrierungen möglich würde.[6]

Die Verzögerung vom Auffangen von Sprüchen (an 10 Tagen) bis zur Ermittlung des zugehörigen Tagesschlüssels betrug für Januar 1940 zwischen 5 und 43 Tage, für Sprüche im Februar (12 Tage) im Mittel 13 Tage, für März (17 Tage) 8 Tage und schliesslich für April (23 Tage) reichlich 1 Tag. Listen der einzelnen Tage mit den Verzögerungen in den Dechiffrierungen der Sprüche dieser Tage sind bei WELCHMAN und bei LANGER zu finden[7].

Für Sprüche, die in der Zeit vom 5.1.1940 bis 16.6.1940 aufgefangen wurden, wurden für insgesamt 110 Tage 126 Tagesschlüssel bestimmt (d.h. an manchen Tagen für mehr als einen Schlüsselkreis), davon in BRUNO 21. Allerdings sagt der Bericht von LANGER[8]

[3] BLOCH d), E - 13
[4] WELCHMAN b), S. 96
[5] Service de Renseignements et de Centre-Espionage
[6] PAILLOLE, S. 181
[7] WELCHMAN b), S. 105; KAPERA, Bericht LANGER, S. 25 - 29
[8] KAPERA, Bericht LANGER

nicht, welche Sprüche in Frankreich bzw. in Grossbritannien gelesen wurden, mit einer Ausnahme: Der oben erwähnte Spruch vom 28.10.1939. Die Anzahl der dechiffrierten Sprüche lag nach Angaben bei BLOCH[9] bei über 8000, viele mehrteilig, wobei diese Zahl offenbar nur ENIGMA-chiffrierte Sprüche umfassen dürfte. Bei BERTRAND findet man Beispiele für dechiffrierte Sprüche. Die Nachrichtenverbindungen zwischen den Dechiffrierstellen und den alliierten Truppenführungen waren noch nicht auf dem erwünschten Stand, sodass eine operative Nutzung der dechiffrierten deutschen Funksprüche durch die alliierten Stäbe noch nicht erfolgen konnte.[10] Besonders drastisch ist das am „Unternehmen Paula" (Luftangriff auf Paris) zu sehen, wo die meisten Sprüche gelesen werden konnten, jedoch keine Folgerungen bzgl. Abwehr oder dgl. erfolgten.[11]

Da in BRUNO die Lochblätter wesentliches Hilfsmittel zur Bestimmung von Tagesschlüsseln waren, musste die Arbeit mit diesen eigentlich am 1.5.1940 zum Stillstand kommen, als die doppelte Chiffrierung des Spruchschlüssels fallengelassen wurde.[12] (Siehe Kap. 1.3.1) Allerdings war am 10.4. ein neuer Schlüsselkreis aufgetreten («Yellow»), der während der Operationen in Norwegen und Dänemark für die Verbindung Heer - Luftwaffe eingerichtet worden war. In diesem Kreis wurde die in den anderen Kreisen am 1.5.1940 eingerichtete Veränderung der Chiffrierung nicht mit vollzogen, sodass für diesen Kreis die Lochblätter noch verwendet werden konnten. Die Tagesschlüssel dieses Kreises wurden täglich ermittelt bis zum 15. Mai, als der Schlüsselbereich zu bestehen aufhörte. Nach anderen Quellen bestand der Schlüsselkreis «Yellow» bis Juli.[13]

Bei «Yellow» wurden Erfahrungen gesammelt über Funkverkehr deutscher Verbände im Kampfeinsatz, bei Einheiten in Bewegung, z.B. Einsatzbefehle, Regelmeldungen, Funknetzabstimmungen kurz nach Mitternacht usw. Bevorzugt wurden dabei als besonders „schwatzhaft" bekannte Stationen.

In BRUNO wurde man während des Norwegenfeldzuges drauaf aufmerksam, dass beim Wetterschlüssel der Luftwaffe jede Codegruppe mit einer involutorischen Substitution der Buchstaben der jeweiligen Steckerverbindung chiffriert wurde.[14] WELCHMAN schreibt, die Ausnutzung dieses Sachverhalts sei neben der Anwendung der «HERIVEL-Tips» eine der sog. KNOX-Methoden gewesen.[15]

Bei der Annäherung der in Frankreich im Mai 1940 vorrückenden deutschen Truppen an den Standort von BRUNO setzte sich das polnische Team auf dem Umweg über Algerien nach Südfrankreich ab zum Chateau des Fouzes nahe Uzes (Tarnname P.C. CADIX) und bearbeitete dort ab Oktober 1940 Sprüche, die vom französischen Funkhorch- und Peildienst der Vichy-Regierung (zweckentfremdet) sowie von vier eigenen Stationen aufgenommen worden waren. CADIX stand in Verbindung mit der Zentrale des polnischen Geheimdienstes in Marseille und der Londoner Zentrale des polnischen militärischen Aufklärungsdienstes. Im Juni 1941 wurde eine weitere „Filiale" in Algier eingerichtet (RYGOR).

Neben verschiedenen Sorten von Handschlüsseln wurden bei CADIX auch ENIGMA-Sprüche gelesen, unabhängig von aus Grossbritannien gelieferten Tagesschlüsseln. Wie sich 1945 herausstellte, besassen REJEWSKI und ZYGALSKI deutsche Schlüsselunterlagen für hochrangige Heereseinheiten, zumindest für eine Zeitspanne im Jahre 1941[16], die vermutlich von Agenten beschafft worden waren.

[9] BLOCH d), E - 7
[10] BLOCH c), S. 182
[11] Die gesammelten Sprüche bei BERTRAND, S. 91 - 96
[12] BLOCH e) hat, erstmals unter Hinweis auf die Deckblätter Nr. 1 - 8 zur H.Dv. Nr. 14 die Kontroverse um den genauen Termin beendet. Seine Aussagen decken sich mit einem Bericht von PAILLOLE, S. 183
[13] HINSLEY II, App. 4, S. 662
[14] KOZACZUK a), S. 117, Note 11
[15] WELCHMAN a), S. 97
[16] KOZACZUK b), S. 233

Am 9.11.1942 musste CADIX evakuiert werden. REJEWSKI, ZYGALSKI und andere Mitarbeiter erreichten im August 1943 auf dem Umweg über Spanien schliesslich Grossbritannien, wo sie aber nicht an der Militär-ENIGMA arbeiten durften. Sie wurden im wesentlichen mit den Handschlüsseln der SS, des SD, der Gestapo und der Polizei beschäftigt, wobei sie über 3000 Sprüche entzifferten.

Ab Mitte November 1940 war „Z“ noch mit anderen ENIGMA-Sprüchen konfrontiert. Peilungen ergaben, dass sie aus der Schweiz stammten. Ihre Besonderheit war: Alle Sprüche eines Tages begannen mit derselben Maschineneinstellung. Das bedeutete, dass alle ersten Buchstaben der Sprüche eines Tages einem einzigen Substitutionsalphabet angehörten, alle zweiten Buchstaben einem zweiten usw.[17] Da diese Maschinen keine Stecker enthielten, war die Bestimmung der Verdrahtung der Eingangswalze und damit auch der anderen Walzen ohne weiteres möglich. Die in Spanien benutzten Methoden zum Finden der Schlüssel konnten wieder verwendet werden. 1941 hat das Chiffrebüro der Abt. f. Nachrichten- und Sicherheitsdienst des schweizerischen Armeekommandos eine „Feststellung zur Verwendung der ENIGMA-Maschine bei der Fliegertruppe“ verfasst. Darin wurde festgestellt, dass durchschnittlich 35 Sprüche mit durchschnittlich 30 Gruppen (zu fünf Buchstaben) mit demselben Schlüssel, der in der Regel 14 Tage verwendet worden war, chiffriert worden wären.[18]

LANGER übt in seinem Bericht Kritik an der Organisation und den Methoden in BRUNO. Die Möglichkeiten der Erfahrung und des Materials der polnischen Mannschaft seien nicht ausgenutzt worden. Britische Autoren haben diese Kritik zurückgewiesen.

6.2 Grossbritannien und USA.

6.2.1 Organisation.

In Deutschland waren die kryptanalytischen Dienste weitgehend zersplittert: Chiffrierabteilung des OKW, Abt. Pers - Z des Auswärtigen Amtes, Forschungsamt, Amt des Sicherheitsdienstes (SD), dazu die einzelnen Dienste der Marine, des Heeres und der Luftwaffe. Obwohl es zwischen ihnen verschiedentlich Zusammenarbeit gab, kann eine zu grosse Zersplitterung, häufige Doppelarbeit mit entsprechendem Mangel an Gesamtübersicht nicht geleugnet werden.

6.2.1.1 GC&CS.

Auf Grund der Erfahrungen mit der Auswertung der Erkenntnisse aus deutschen Funksprüchen u. dgl. im Ersten Weltkrieg wurde 1919 die Government Code and Cipher School (GC&CS) geschaffen, die allerdings zunächst nur mit geringer Effektivität arbeitete. Auf Grund der sehr geringen Erfolge des Dienstes während des Abessinienkrieges wurde 1937 eine Zentrale für den Marine–Nachrichtendienst geschaffen, die sich auf GC&CS stützte, das seinerseits dem Aussenministerium unterstand. Zwar wurden im Spanienkrieg erste Erfolge erzielt, was Verkehrsanalysen und Entzifferungen angeht, aber ein zugehöriger Peildienst fehlte.

6.2.1.2 BP.

Im Gegensatz zur deutschen Zersplitterung wurden, gegen anfänglichen Widerstand einzelner Abteilungen, in Grossbritannien alle Bestandteile der durch Funk zu erlangenden Erkenntnisse (Verkehrsanalysen, Peilungen, Schlüsselermittlungen, inhaltliche Auswertung) in einem Zentrum zusammengeführt (Ergebnisse der Photoaufklärung kamen später ebenfalls dazu). Die aus den Erkenntnissen an die Streitkräfte weiterzugebenden Mitteilungen wurden ebenfalls von diesem Zentrum gesteuert. Es wurde

[17] KOZACZUK b), S. 143

[18] Schreiben des Armeekommandos der schweizerischen Armee vom 25.4.41, (schweizerisches Bundesarchiv)

aus GC&CS die schon vorhandene Marinesektion und die das Schwergewicht bildende Diplomatenfunk-Abteilung 1930 um die Army Section und 1936 um die Air Force Section erweitert. Sie zog im Juli 1939 nach Bletchley Park, zwischen Oxford und Cambridge gelegen (Im folgenden abgekürzt BP). Anfangs arbeiteten dort nur 30 Personen, am Ende des Kreiges waren es etwa 10000.

Bei der Royal Navy wurde das „Operational Intelligence Centre“ (O.I.C.) 1936/1937 von DENNING als Bestandteil der „Naval Intelligence Division“ (N.I.D.) gegründet. Im O.I.C. entstanden nach und nach u.a. Sektionen für Überwasserschiffe, U-Boote, Minenwesen, Hilfskreuzer, Peilwesen usw.[19]

Die Admiralität, die im Gegensatz zu den anderen britischen Teilstreitkräften auch operative Funktionen ausübte, musste darauf bestehen, dass BP alle dechiffrierten Sprüche, die die Marine betrafen, unmittelbar an das O.I.C. leitete. Dort wurden sie in den betroffenen Sektionen ausgewertet und die Resultate an alle Stellen, bei denen die Notwendigkeit der Kenntnisnahme bestand, weitergeleitet. Bei Kriegsausbruch bestand das O.I.C. darauf, dass die Anzahl der Horch- und Peilstationen erheblich vermehrt würde. Es waren zunächst nur drei gewesen: Scarborough, Flowerdown und Malta. Im Laufe des Krieges nahm die Anzahl der Stationen erheblich zu. (1943 arbeiteten 350 landgebundene Stationen , sodass praktisch die Nordsee und der gesamte Atlantik überwacht werden konnten.) Hinzu traten später über hundert Peileinrichtungen auf Schiffen (HF/DF ,«Huff-Duff»), die für die U-Boot-Bekämpfung zunehmend Bedeutung erlangten. Auch die Nachrichtenlinien für den sicheren Austausch von zu schützenden Sprüchen zwischen eigenen Stellen wurden vermehrt.[20]

Die Mitarbeiter der GC&CS wurden, beginnend 1937, meist nach dem Prinzip „Wer kennt wen, der geeignet erscheint ?“ ausgesucht, wobei sich mit der Zeit die entstehenden „Seilschaften“ aus den verschiedensten Berufsrichtungen ergaben. Darunter waren z.T. noch sehr junge Studenten der beiden grossen Universitäten, alle höchst intelligent und hochmotiviert.

Zunächst wurde die vorsorgliche Rekrutierung im wesentlichen im geisteswissenschaftlichen Bereich betrieben, ab 1938 aber auch Mathematiker, obwohl man zunächst Zweifel hegte, ob diese manchmal als seltsame Vögel angesehenen Menschen für die vorgesehenen Aufgaben taugen würden. Bei Kriegsbeginn waren also im wesentlichen Sprachwissenschaftler, Altsprachler und Historiker eingebunden. Dann traten neben anderen auch zwei der wesentlichen mathematischen Spitzenbegabungen in das Team ein: TURING und WELCHMAN. Auf diese Weise entstand eine Mannschaft, die die unterschiedlichsten Altersgruppen, Berufsrichtungen und Charaktere (bis hin zu den exzentrischsten) vereinte. Ohne Rücksicht auf Rangordnung oder Hierarchien, manchmal chaotisch, aber stets innovativ, arbeiteten sie an dem einzigen Ziel: Die vorgegebenen Quellen bis zum letzten auszuschöpfen. CHURCHILL war der Meinung, dass Spezialisten, auch anderer Disziplinen, auf dem Gebiet der Nachrichtendienste (intelligence) (ND) besser geeignet seien als Militärs. Dieses System der Rekrutierung von Zivilisten wurde auch von der Admiralität übernommen, wo z.B. das zentrale O.I.C. im wesentlichen aus Zivilisten bestand. Der Wirkungsgrad des Systems wäre sicher unter militärischer Disziplin oder starrer Routine eines Öffentlichen Dienstes geringer gewesen.

WELCHMAN erkannte frühzeitig, dass bei der nötigen Zunahme von Personal eine klare Organisation nötig war, um die Menge des zu verarbeitenden Materials möglichst reibungsfrei zu gewährleisten. Er schlug seinem Vorgesetzten TRAVIS die folgende Gliederung vor, die so auch realisiert und im wesentlichen durch die Dauer des Krieges beibehalten wurde:

[19] BEESLY a), S. 149
[20] BEESLY a), S. 149

Dechiffrierung für Heer/Luftwaffe: Hut 6
Dechiffrierung für Marine: Hut 8
Auswertung der Erkenntnisse Heer/Luftwaffe: Hut 3
Auswertung der Erkenntnisse Marine: Hut 4

6.2.1.3 Y-Stationen.

Die Reihenfolge der Bearbeitung begann in den Y-Stationen genannten Funkhorch-Stationen. Damit verbunden war bereits eine erste Analyse des deutschen Funkverkehrs.

In den Abteilungen für die Dechiffrierungwurde nach der Registrierung der Funksprüche und einer intensiven Funkverkehrsanalyse u.U. Rückmeldung an die Horchstationen gegeben, welche Frequenzen besonders zu beachten seien.

Die nächste Aufgabe war die Untersuchung des vorliegenden Materials auf mögliche Klartexte, sodass damit die Menus für die Bomben entwickelt werden konnten (Siehe Kap. 6.2.1.10). Wenn diese erfolgreich die Schlüssel lieferten, wurden die Sprüche dechiffriert.

In den weiteren Abteilungen Hut 3 und Hut 4 wurden die Sprüche übersetzt und die gewonnene Information registriert. Für die Weitergabe der Erkenntnisse mussten die Inhalte allerdings paraphrasiert werden, damit die Quelle - deutsche Funksprüche - nicht erkannt werden konnte. Weiter wurde der umfangreiche Kartenindex mit jeder möglichen cross-reference ergänzt, sodass das Wissen um die deutschen Streitkräfte jederzeit auf dem neuesten Stand blieb.

Unter dem Begriff SIGINT (Signals Intelligence) wurden zusammengefasst: Abhördienst, Kryptanalyse, Verkehrsanalyse und die daraus resultierende Auswertung. Für den Abhördienst war der „Y - Service“ geschaffen worden, der auch für Peildienste und Dechiffrierungen von taktischen Handschlüsseln vorgesehen war. Die RAF operierte 1940 mit den Abhörstationen in Cheadle und Kingsdown, die Army in Chatham. Cheadle wurde 1941 nach Chicksands verlegt, hinzu kamen 1942 Shaftesbury und schliesslich 1943 Trowbridge, Beaumanor, Forest Moor, Knockholt, Heliopolis und Malta.[21] Eine Karte der Abhörstationen ist bei WEST zu finden.[22] Beaumanors Zentrale hatte eine direkte Fernschreibleitung nach BP. Die einzelnen Abhörstationen lieferten ihre Ergebnisse durch Meldefahrer an diese Zentrale. Chicksands entwickelte sich zum Schwerpunkt für das Abhören schwacher Signale aus Afrika, vom Balkan und von der Russischen Front. Weitere Stationen mit sehr empfindlichen Empfängern traten hinzu, sodass fast alle Frequenzen nahezu dauernd und über sehr grosse Entfernungen (z.B. von der Russlandfront) überwacht werden konnten. 1942 waren bereits über 100 Empfänger in Betrieb. Mit der Zeit traten noch mehr Empfangsstationen hinzu, die z.T. mit denen in Kingsdown vernetzt waren. Ausserdem wurden weitere Abhörzentren in Malta, Sidi Barani, Palästina und Bagdad eingerichtet, sodass praktisch der Funkverkehr aus ganz Europa abgehört werden konnte. Einen Katalog der Horch- und Peilstationen im Mittelmeer-Raum gibt CLAYTON.[23] Die typischen Aufgaben von Aussenstellen gibt SKILLEN am Beispiel Heliopolis:[24]

a) ENIGMA-Sprüche an BP weiterleiten
b) andere deutsche u. italienische Sprüche selbst bearbeiten
c) Verkehrsanalyse erstellen, Peilungen registrieren, Katalog von Präambeln, Rufzeichen usw. erstellen.

[21] SKILLEN a), S. 93
[22] WEST a), S. 147
[23] CLAYTON, Appendix
[24] SKILLEN b), S. 146

Für Heer und Luftwaffe standen 1943 357 Abhörstationen im Einsatz, 1944 waren es 609.[25] Für die Zeit der Invasion 1944 wurden sogar in BP selbst Antennenanlagen errichtet, um die Zeitspanne zwischen Spruchaufnahme und Bearbeitung in BP so kurz wie möglich zu halten.[26] In einem Falle wurde dadurch die Übersetzung eines abgehörten und dechiffrierten Spruches bereits 12 Minuten nach seiner Aufnahme an die Admiralität weitergeleitet.[27]

6.2.1.4 RSS.

Zusätzlich wurde 1939 der Radio Security Service (RSS) gegründet, in dem Amateurfunker in Grossbritannien zur Funküberwachung herangezogen wurden, zunächst zur Aufdeckung von illegalen Agentensendern[28]. Die Abhörberichte liefen in Arkley in Middlesex zusammen. Es stellte sich schon Mitte März 1940 heraus, dass alle aufgenommenen Sprüche von deutschen Stellen vom Kontinent stammten. An manchen Tagen wurden 300 Abhörprotokolle (sog. „logs") an die Zentrale geliefert. Mehr und mehr gewann die Beobachtung der chiffrierten Sprüche der deutschen Abwehr an Gewicht, zumal es auf der Insel kaum noch illegale Sender zu entdecken gab. Die Ergebnisse (es handelte sich fast nur um Handschlüssel) führten oft zu Erkenntnissen, die als Grundlage für spätere Einbrüche in ENIGMA-Schlüssel dienten. (U.a. wurde Anfang 1940 eine Relais-Funkstation auf einem Schiff vor der norwegischen Küste ausgemacht, die die Funksprüche des britischen Agenten SNOW - „umgedrehter" deutscher Agent OWENS - in ENIGMA-Sprüche „übersetzte".)[29] Die Abhörprotokolle wurden an Hut 6 (s.u.) geliefert.

In BP liefen alle Stränge der Informationsbeschaffung zusammen. Alle Sprüche wurden zentral erfasst, bearbeitet, ausgewertet und an die zu informierenden Stellen weitergeleitet. Zunächst waren die einzelnen nach dem Prinzip «need to know» voneinander abgeschotteten Abteilungen in einer Art Baracken untergebracht, woher die Abteilungen ihre Namen herleiteten (z.B. Hut 6), den sie auch beibehielten, als sie in grössere, feste Häuser umzogen.

In Hut 2 wurde das militärisch-wissenschaftliche Vokabular beobachtet, gedeutet und verfolgt. Von hier wurde auch beim Auftreten von neuen Begriffen die Aufmerksamkeit der anderen Abteilungen auf die betreffenden Schlüsselkreise gelenkt.

6.2.1.5 SLUs.

Die Weitergabe der Erkenntnisse an die (ausserordentlich wenigen) autorisierten Empfänger war bei Heer/Luftwaffe und Marine verschieden:
Bei der Marine wurden die Ergebnisse direkt im Wortlaut der Übersetzung an das O.I.C. geliefert, weil die Admiralität auch operative Zentrale für die Marine war. Bei der Marine wurden die weiterzugebenden Nachrichten mit zwei Skalen versehen : A bis E für Verlässlichkeit der Quelle, 1 bis 5 für Gültigkeit der Information.

Bei Heer und Luftwaffe wurden die Erkenntnisse mit einem als solchen kenntlich gemachten Kommentar versehen, paraphrasiert und nach der Dringlichkeit eingestuft (Z = niedrig, ZZZZZ = höchst wichtig). Dann wurden sie an spezielle Verbindungseinheiten (Special Liaison Units = SLUs), die bei den autorisierten Empfängern eingerichtet waren, weitergegeben, die ihrerseits die allein dazu autorisierten Empfänger informierten. Alle Meldungen wurden sofort, nachdem sie von den Empfängern gelesen und verstanden waren, vernichtet. Jede auf Grund dieser Informationen vorgenommene Massnahme durfte keinen Rückschliss auf die Quelle erlauben[30]. Die Empfänger von

[25] HINSLEY III/2, App. 6, S. 777
[26] HINSLEY III/2, App. 6, S. 784
[27] NARA Dokument Box ZEMA44, Nr. 4685«The History of Hut Eight 1939 - 1945», S.10
[28] WEST, S. 120
[29] ALLASON, S. 152 - 155
[30] Lewin, S. 166

Ultra-Meldungen durften diese weder weitersenden, wiederholen oder in irgendeiner Form darauf Bezug nehmen. Der autorisierte Empfänger durfte sich auch keinesfalls so bewegen, dass die Gefahr der Gefangennahme durch deutsche oder italienische Truppen bestehen könnte. Die Geheimhaltung der Ultra-Quellen und somit der Tatsache, dass die ENIGMA - Sprüche entziffert werden konnten, war eins der bestgehüteten Geheimnisse der Alliierten bis in die 70er Jahre.

Beispiele:[31]

> 1) KV 3281 ZZZZ, vom 9.5.1944, 13.34 Uhr: Kommentar zu einem Bericht der Luftflotte 3 vom 8.5., worin sie die Meinung vertritt, dass die Hauptrichtung eines zu erwartenden alliierten Landungsversuchs im Bereich Le Havre - Cherbourg liegen dürfte.
> 2) XL 4795 ZZZZZ, vom 5.8.1944, 10.40 Uhr: Flivo-Spruch vom 5.8. 05.30 Uhr, die 1. SS-Division wird während der Nacht herausgezogen.
> (Flivo = Flieger-Verbindungsoffizier)

Die Geheimhaltungsstufe war Ultra Secret, woher die spätere Kurzbezeichnung Ultra stammte. Zunächst waren die Meldungen mit dem Stichwort PECKSNIFF, später mit BONIFACE versehen worden, was die Assoziation wecken sollte, es handle sich um Agentenerkenntnisse.

Zu diesen Zwang zur Geheimhaltung gehörte vor allem, dass jeglicher Einsatz, der letzten Endes auf Erkenntnissen aus ENIGMA-Sprüchen fusste, durch eine Verschleierungsmassnahme erklärbar gemacht wurde, damit die deutschen Befehlsstellen aus den Massnahmen des Gegners nicht auf den Verdacht der Kompromittierung der Schlüsselmittel kamen.[32] Dies ist auch bis auf wenige Ausnahmen gelungen, die erhebliche Aufregung im alliierten Lager hervorriefen.[33]

In Hut 11 wurde am 18. 3. 1940 die erste «Bombe» (s.u.) installiert[34], nach einem Jahr waren es etwa 12, wovon einige in Adstock, etwa 15 km westlich Bletchley standen. Später kamen noch Standorte in Wavendon, etwa 5 km nördlich von Bletchley und in Gayhurst, 12 km nördlich von Bletchley dazu, weitere dann in Stanmore und Eastcote, zusammen waren bei Kriegsende rund 200 «Bombes» im Einsatz.

Im Frühjahr 1942 verarbeiteten ca. 1500 Menschen im Monat etwa 25000 Sprüche von Heer und Luftwaffe und etwa 14000 Sprüche der Marine. Im Juni 1943 waren es etwas über 5000, wovon 500 allein mit Handschlüsseln befasst waren. Gegen Kriegsende waren in BP rund 10000 Menschen beschäftigt.

Ende 1942 traf eine Gruppe der amerikanischen Armee in Grossbritannien ein, um sich in BP einzuarbeiten, nachdem 1941 bereits vier Amerikaner in BP das System kennengelernt hatten. Die Dechiffriergruppen, die in den Vereinigten Staaten ihre Arbeit aufgenommen hatten, hielten engen Kontakt mit Hut 8 in BP. Zwar wurde nicht die Elite der Kryptografen mit dem Hauptproblem „Triton" befasst, dafür aber höchst intelligentes kryptografisch vorgebildetes Personal mit glänzenden Organisationsideen. So sind z.B. die Regeln für die Walzenpositionen im Mai 1944 bei Op–20–G entdeckt (siehe Kap. 6.2.3.3 zur Marine-ENIGMA) worden.

In den USA wurde im Mai 1943 zur Bekämpfung der U-Boote die Zehnte Flotte gebildet, eine reine Behörde ohne Schiffe. Dort wurden, wie im O.I.C., in einem «tracking

[31] Quelle: Ultra Reel Inventory, October 15,1987; in: Bibl. f. Zeitgeschichte, Stuttgart, A 11

[32] Bei der Versenkung von Nachschub-Schiffen für das Afrika-Korps mit Benzin bzw. Panzern wurden stets ein oder zwei Schiffe unbehelligt gelassen, um den Verdacht nicht auf die Möglichkeit der Kompromittierung der Schlüssel zu lenken (HANDEL, S. 449)

[33] Im März 1943 hatte das britische Middle-East-Kommando eine realistische „Entdeckung" durch Flugzeuge von zwei Nachschubgeleiten für das Afrika-Korps vor der Versenkung der Schiffe unterlassen, was prompt zum deutschem Verdacht auf Unsicherheit der Schlüssel führte. Churchill schickte ein wütendes Telegramm an das Kommando und drohte mit harten Konsequenzen (JABLONSKI, S. 160)

[34] SEBAG-MONTEFIORE, S.56, Deckname «Agnes»

room» alle Erkenntnisse über Schiffsbewegungen verfolgt und sofort in Karten eingetragen. Eine Kartei hielt, wie in BP, alle Einzelheiten über U-Bootbewegungen fest.

Im Frühjahr 1943 waren die Prototypen von zwei «Bombes» einsatzbereit (»ADAM» und«EVE»), ab September 1943 waren die ersten Maschinen in Washington einsatzbereit, im November 1943 bereits 50 Maschinen im Einsatz.

Anfangs wurden von BP Sprüche mit angenommenen Klartexten in die USA geliefert und dort mit «Bombes» hoher Geschwindigkeiteitet bearbeitet (speziell für den Schlüssel M Form M 4), deren Kapazität je sechs britischen «Bombes» entsprach.

Da für „Triton“ «Shark» kaum noch vernünftige Klartextteile zur Verfügung standen, nützte man in Op–20–G die Meldungen der Boote beim Ein- und Auslaufen, da man die Boote selbst meist kannte. Ab Mitte 1944 übernahmen die USA wegen der grösseren Zahl und der grossen Schnelligkeit ihrer «Bombes» die gesamte Verantwortung für die Schlüssel der deutschen U-Boote. Dabei half eine verhängnisvolle Stereotypie im Bereich des Schlüssels Wetter Biscaya, die trotz einer Rüge durch die deutsche Funküberwachung bis zur Invasion im Juni 1944 andauerte. Darüber hinaus stellten sie BP auch «Bombe» - Laufzeiten für Schlüssel zur Verfügung, die nicht zum Bereich von Hut 8 gehörten.[35]

Die von den Abhörstationen gelieferten Sprüche wurden zunächst mit den Erkenntnissen der «Traffic Research» in die einzelnen Funknetze sortiert. Die Marinesprüche wurden an Hut 8 weitergeleitet, die anderen an Hut 6.

Es gab auch eine Hut F, in der der Mathematiker Max NEWMAN mit seinen Mitarbeitern die sog. «Heath Robinson» entwickelte, die später durch die «Colossi» abgelöst wurde. Diese Maschinen dienten dazu, den geheimen Nachrichtenverkehr mit Fernschreibern und ihren Geheimzusätzen zu dechiffrieren. Hier soll auf diese Arbeiten nicht eingegangen werden.

6.2.1.6 Hut 6.

6.2.1.6.1 blists. In Hut 6, spätestens ab Januar 1940 in Aktion, gingen alle Sprüche von den Abhörstationen, die Heer oder Luftwaffe betrafen, im Registration Room ein, wurden dort registriert und sortiert nach Frequenzen, Rufzeichen, Indikatoren und Spruchtarten (ENIGMA, nicht-ENIGMA, Italienische) und in Listen, sog. «blists» eingetragen.

Das Verzichten auf die Kenngruppen ab Herbst 1943 erschwerte das Sortieren der Sprüche nach Funkbereichen erheblich. Da bei der Einführung der UD die Kenngruppen wieder eingeführt werden mussten, wurde für Hut 6 trotz der Erschwerung der Arbeit durch die neue Umkehrwalze das Sortieren der Sprüche wieder erleichtert.

6.2.1.6.2 FOSS-sheets. Aus den «blists» wurden die Sprüche in sog. «FOSS–sheets» übertragen. Diese Bögen bestanden aus je 676 Zellen, wobei als Koordinaten die 1. und 2. Buchstaben des jeweiligen Indikators dienten. In die einzelnen Zellen wurde die 3. Buchstaben mit der «blist» Nummer eingeschrieben. Das Ziel dieser Registrierung war es, auffällige Häufungen bei den Zelleninhalten zu entdecken.(«nearness»und «giveaways»[36]). «nearness» ist unter HERIVEL–Tips (Kap. 6.2.3.1.3, S. 149) zu finden.

Das war bei rund 70 Netzen bei Heer und Luftwaffe nicht einfach. Die Diskriminanten in den Sprüchen, die die Zuordnung zu einem Netz festlegten, bestanden aus einem Trigramm, das aus vier möglichen pro Netz und Tag ausgewählt wurde und permutiert in den Spruch eingesetzt wurde. Hier half aber wieder deutsche Systematik. Offenbar gab es etwa 250 Karten mit je 31 Zeilen (entsprechend den Monatstagen) mit je vier

[35] ERSKINE b), S. 504

[36] «giveaways»: Angaben zum Schlüssel in Klartext; SMITH u. ERSKINE, S.64

Diskriminanten. Für jeden Monat wurde eine Karte einem Funknetz zugeordnet. Da die Frequenzen der einzelnen Netze festlagen, war das Erkennen der dem Netz zugeordneten Karte nur am Monatsanfang schwierig. Bei der Luftwaffe war das System etwas anders, da wurde für ein Netz ein beliebiger Tag (= Zeile) auf 30 oder 31 Karten ausgewählt, dieser Tag blieb ungeändert für einen Monat.

Am Monatsanfang war zunächst zu erkennen, zu welchem Typ Netz die Sprüche gehörten: Linie, Stern, Kreis oder Netz. Bei letzterem war die Zuordnung am schwierigsten, weil da jede Station zwar eine feste Empfangsfrequenz, aber so viele Sendefrequenzen hatte, wie Stationen im Netz waren. Hier musste die Funkpeilung Hilfestellung zur Identifikation leisten.

Eine weitere Aufgabe bestand darin, die Zuordnung der Rufzeichen nach den Vorgaben des B-Buches («Bird book») bei der Luftwaffe oder des E-Buches («Elephant book») beim Heer. Jedes dieser Bücher enthielt 200 Seiten mit je 200 Rufzeichen. Die deutschen Truppen in Europa waren in „Funkverkehrsbereiche“ eingeteilt. Jeder Einheit war für eine längere Zeitspanne eine bestimmte Zeile im Buch und eine Folge von zufallsverteilten Spalten für 365 Tage zugeteilt (Zyklennummer). Diese Zyklennummer bestimmte in der Monatsspalte (links im Zuweisungsplan) die Zeile, in der rechts im Zuweisungsplan unter dem Datum die Spalte in der zugewiesenen Zeile im Buch das Tagesrufzeichen zu finden war.[37]

J	F	M	...	O	N	D	1	2	3	...	30	31
1	9	18	...	78	87	96	85	172	13	...	73	28
2	10	19	...	79	88	97	16	43	127	...	3	67
3	11	20	...	80	89	98	131	26	39	...	122	91
150	8	17	...	77	86	95	22	101	15	...	43	1

Die alliierten Dienste hatten beide Bücher weitgehend rekonstruiert, nicht zuletzt, weil die versteckte Systematik der nur scheinbaren Zufälligkeit erkannt werden konnte.

In der «Intercept Control» wurden die Frequenzen bestimmt, denen besondere Aufmersamkeit zu widmen war, bzw. welche Frequenzen von mehreren Abhörstationen überwacht werden sollten, um Hörfehler möglichst auszuschalten.

Damit war schon eine grobe Einteilung nach Schlüsselkreisen erreicht. Diese Register enthielten von jedem aufgenommenen Spruch die Präambel und die ersten sechs Buchstaben. Sie wurden dreifach erstellt, einmal zum Eintragen in die Verkehrsregisterkartei, einmal für die Kryptologen, die danach entschieden, welche Sprüche sich zur Bearbeitung eignen könnten (in welchen sich erfahrungsgemäss ein bekannter Klartext befinden könnte), schliesslich erhielt auch der Koordinator für die Abhörstationen ein Exemplar. Er gab u.U. Hinweise, welche Stationen bzw. Frequenzen von den Abhörstationen besonders genau beobachtet werden sollten. Die Registerkartei machte sich nach etwa 18 Monaten bezahlt. Es wurde mehr und mehr möglich, Strukturen des Funkbildes der deutschen Wehrmacht zu erkennen.[38] In Hut 6 wurde auch die eigentliche Dechiffrierarbeit geleistet. Eine Gruppe von Mitarbeitern suchte nach dem, was intern «kiss» genannt wurde : Ein und dieselbe Nachricht in verschiedenen Schlüsselkreisen und somit unter verschiedenen Schlüsseln. Ausserdem wurden hier entsprechend den erkannten Schlüsselkreisen Klartexte formuliert. Daraus wurden die Menus für die Bomben entwickelt und an die Bomben-Einheiten abgegeben.

Von dort kamen die vermuteten möglichen ENIGMA-Stellungen zurück und wurden überprüft, ob es sich um die richtige Stellung handelte. Wenn das der Fall war, erhielt

[37] Diese Daten sind dem NARA-Dokument Box CBTE28, Nr. 3620«E-Operations of the GC&CS», S. 15, entnommen

[38] WEST a), S. 161

der Dechiffrierraum die Stellungen und erstellte mit umgebauten TypeX-Maschinen den deutschen Klartext.

Im Bericht F-121 vom 29.11.1944[39] wird die seit dem 1. November aufgetretene Chiffrierung von Frequenzen und Rufzeichen beschrieben. Diese neue Verschleierung trat zuerst bei der Luftwaffe auf, danach auch beim Heer. Das Sortieren der Sprüche nach Rufzeichen bzw. Frequenzen war somit kaum noch möglich. Das Verfahren benutzte zwei Zahlenkästen und drei Chiffrieralphabete, täglich wechselnd. Vertikal ist jeweils die erste Ziffer aufgetragen, horizontal die zweite.

Kasten A

	0	1	2	3	4	5	6	7	8	9
0	76	80	26	34	53	99	08	64	58	48
1	12	14	93	25	84	30	36	02	73	41
2	05	97	82	35	94	51	42	17	61	03
3	55	23	66	07	86	42	29	70	63	39
4	11	95	00	81	18	59	32	91	40	85
5	69	28	79	33	72	04	60	37	13	74
6	22	88	90	46	65	50	09	54	96	31
7	01	92	43	62	47	83	87	16	10	98
8	15	38	06	67	89	19	56	45	49	20
9	52	24	57	21	78	27	77	68	75	71

Kasten B

0	1	2	3	4	5	6	7	8	9
88	30	35	76	10	06	57	42	63	27
90	61	99	55	31	23	84	58	37	03
33	45	87	65	39	13	13	71	04	21
26	69	50	44	82	48	60	34	73	00
14	41	80	07	75	11	22	86	29	09
40	15	53	32	08	79	47	28	89	98
70	04	92	36	01	62	49	96	52	91
20	81	17	85	02	51	16	83	25	93
56	64	95	66	74	68	54	05	18	72
78	43	77	46	19	59	38	12	24	97

Schlüsselalphabete:

```
*  A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0 1 2 3 4 5 6 7 8 9
1  P 6 U Q 3 H W M 9 F C K N Y 2 I D E O R X L G 7 4 O T J V B 5 S 8 Z 1 A
2  W O P C 6 X M 9 Z G L A U O Y D 4 N V B S Q 7 H 8 F I 3 J 5 R E 2 T I K
3  L Q H U O T 4 Z F 7 I 6 9 B K X A 2 N O R E 5 1 W S 8 J D P Y 3 C V G M
```

Angenommen, das Rufzeichen sei primär in Zeile 35 und Spalte 367 des F-Buchs festgelegt. Die erste Chiffrierung ändert die Position im F-Buch zu Zeile 42 und Spalte 396. Wenn dort das Rufzeichen `P3S` zu finden ist, wird dieses im zweiten Schritt über die Schlüsselalphabete in `I5N` umgewandelt. BABBAGE, einer der führenden Kryptologen von Hut 6 war der Meinung, dass dieses System der Rufzeichenchiffrierung nicht gebrochen werden könnte.

Wenn ein Spruch dechiffriert vorlag, wurde er an Hut 3 abgegeben. Vorher wurde er noch daraufhin geprüft, ob Teile davon möglicherweise für andere Sprüche als Klartext zu verwenden wären. Es gab auch noch Teams, die sich nur mit Handschlüsseln befassten, bzw. mit solchen Maschinenschlüsseln, zu denen noch kein Zugang gefunden war.[40]

Analoge Tätigkeiten für den Bereich der Marine waren in Hut 8 zusammengefasst.

6.2.1.7 Hut 3

Die weitere Verarbeitung der dechiffrierten Sprüche in Hut 3 bestand aus der Übersetzung (u.U. Ausbesserung von lücken- oder fehlerbehafteten Texten), der Bewertung des Inhalts und der Auswertung und Verteilung. Zur Auswertung gehörte eine grosse Index-Kartei, in der auf vielen tausend Karteikarten alle wesentlichen Erkenntnisse (Namen, Truppenteile, militärische Fachbegriffe, Beförderungen, Versetzungen usw.) mit ausführlichen Querverweisen festgehalten wurden. Ein Doppel dieser Kartei wurde

[39] NARA Dokument Box CBMH15, Nr.1238A «Capt. W. Fried Reports»
[40] KOZACZUK b), S. 110

aus Sicherheitsgründen nach Oxford ausgelagert. In den Karteien für das Heer bzw. die Luftwaffe wurden die Truppenteile bis unterhalb der Regimenter erfasst, Personalien bis hinunter zu Unteroffizieren. Die Kartei der Luftwaffe z.B. umfasste rd. 15000 Karten. Bei der Marine umfasste die Kartei rd 200000 Karten, gegliedert in ZTPI (Italienische Marine–Hagelin), ZTPG (Deutsche Marine), ZTPGM (Deutsche Marine–ENIGMA), ZTPGU (Deutsche U-Boot–ENIGMA), ZTPS (Spanischer Marine–Handschlüssel) und STPG (Handschlüssel der deutschen Marine).

Etwa 1000 Sprüche erhielt Hut 3 täglich zur weiteren Bearbeitung. Schliesslich wurden die Inhalte im Wortlaut so verändert, dass ihr Ursprung aus ENIGMA-Sprüchen nicht mehr erkennbar war. Es wurden dabei z.T. Spione oder Agenten als Quellen zur Tarnung der Herkunft erfunden. Damit wurde auch die Arbeit der SLUs gesteuert.

Schliesslich wurden im «German Book Room» alle deutschen Sprüche u.a. mit Frequenz, Sendezeit, Rufzeichen, Indikator und vollem deutschen Wortlaut festgehalten.

Die Zusammenarbeit zwischen Hut 6 und Hut 3 bestand auch darin, Schwerpunkte für die Auswertung zu setzen und u.U. spezielle Frequenzen besonders aufmerksam beobachten zu lassen. In Hut 3 waren etwa 200 Experten rund um die Uhr in vier Schichten tätig.

Hut 4 leistete die der Hut 3 entsprechende Arbeit für Hut 8, u.a. die Bearbeitung des Werftschlüssels, der ab Mai 1941 laufend gelesen wurde.

In Hut 10 war u.a. die Dechiffrierung des Wetterschlüssels der Marine konzentriert, der schliesslich im Februar 1941 gebrochen wurde. Zusammen mit der Kenntnis des Wetterkurzschlüssels der U-Boote hatte man hier die Möglichkeit, Klartextteile zu gewinnen und so immer wieder in den U-Boot-Schlüssel einzubrechen.[41]

6.2.1.8 Hut 8

Die Organisation hat sich im Laufe der Jahre den wachsenden Erfordernissen entsprechend immer wieder verändert, eine Art Leitlinie, die Trennung der Bearbeitung von Sprüchen des Heeres bzw. der Luftwaffe von denen der Marine, ist jedoch erhalten geblieben. Am Beispiel der Verarbeitung eines abgehörten Spruches in der Abteilung, die als «HUT 8» von TURING geschaffen und zunächst auch von ihm geleitet worden war, soll sie verdeutlicht werden.

Die Sprüche kamen im wesentlichen von der Abhörstation Scarborough, z.T. auch von Murmansk (Norwegen-Verkehr) und von Alexandria (Mittelmeer). Die durchschnittliche tägliche Zahl von anfallenden Sprüchen betrug[42]

1941	465
1942	458
1943	981
1944	1560
1945	1790

Ein Spruch wurde von der Abhörstation geliefert und zweifach der Registratur zugestellt (u.U. noch ein drittes Exemplar für die USA). Die Sprüche wurden grob sortiert nach Schlüsselverfahren (K-Buch und Bigrammtafeln bzw. Doppelindikator) und geografisch.

Hierbei wurde bereits die Aufmerksamkeit intensiv darauf gerichtet, ob etwa Wiederholungschiffrierungen vorliegen könnten. Die einzelnen Sachbearbeiter mussten über ihren Bereich bzgl. der Funknetze einen sicheren Überblick haben und jede Abweichung vom Bisherigen sofort erkennen können.

[41] KAHN a), S. 189

[42] NARA Dokument Box ZEMA44, No.4685«The History of Hut Eight 1939 - 1945», S.7

Intensive Zusammenarbeit mit den Leuten der Verkehrsanalyse war deshalb vonnnöten. Da selbstverständlich jeweils nur ein Teil des tatsächlichen Funkverkehrs abgehört werden konnte, konnten aus Quittierungen von (nicht abgehörten) Funksprüchen Rückschlüsse gezogen werden auf das nicht erfasste Funkgeschehen. Hier kam es auch hin und wieder vor, dass bei Missverständnissen zwischen den Funkstellen Walzenlagen oder Steckerpositionen offen zu erkennen waren.

Die weitere Arbeit übernahmen zwei Abteilungen mit zwei völlig getrennten Aufgabenzielen, erstens die für die Kryptanalyse, zweitens die, die sich damit befasste, die Ergebnisse der ersten Abteilung zur Lösung zu bringen und die Sprüche zu lesen, aber auch Rückmeldungen an die erste Abteilung, die für deren Arbeit nützlich bzw. notwendig war. Hierzu gehörte es, mit Hilfe von K-Buch und Bigrammlisten die für den Banburismus (s. Kap. 6.2.3.1.6) nötigen Trigramme bereitzustellen und sie nach Schlüsselgebieten und Diskriminanten zu überprüfen. Weiter musste hier das Materials für die Bearbeitung mit den Bomben vorbereitet werden und die Ergebnisse, wie sie von den Bomben geliefert wurden ausgetestet werden. Wenn die Bombe diese eine richtige Lösung mit Walzenlage und Steckerstellungen geliefert hatte, ging der Vorgang zurück zu den Kryptanalysten, damit dort die Ringstellungen und die Grundstellung gesucht werden konnte.

Das vollständige Lesen, die Vervollständigung der Lösungen mit Hilfe der Informationen aus der ersten Abteilung und die ausführliche Listenführung ergänzten diesen Aufgabenbereich.

In der ersten Abteilung wurden mit zunehmendem Erfolg die Bigrammtafeln rekonstruiert, mit deren Hilfe dann mit dem Banburismus die jeweils verwendeten Walzen identifiziert werden konnten. Hier wurden Klartextstellen gesucht und weitere Methoden angewendet, die für die Anwendung der Bombe Erleichterung brachten.

Mit zunehmender Anzahl der verfügbaren Bomben nahm die Notwendigkeit des Banburismus ab, dafür wuchs die Bedeutung von passenden angenomenen Klartexten. Das hiess, dass sehr viel mehr Registraturarbeit und Vergleich von Sprüchen notwendig wurde.

Gleichzeitig wurden die Sprüche mit früheren verglichen, ob sie sich so anordnen liessen, dass sie zumindest teilweise mit derselben Maschinenstellung chiffriert waren und so evtl. Klartextabschnitte ermitteln weren könnten.

6.2.2 Dechiffriermethoden und -Geräte.

6.2.2.1 Transpositionsverfahren („Versatzverfahren“).

6.2.2.1.1 „Doppelwürfelverfahren“. Die bei einer reinen Transposition, dem Doppelwürfelverfahren, anzuwendende Anagramm-Methode ging davon aus, dass bei regem Funkverkehr sicher einige Sprüche gleicher Länge auftreten würden. Da diese wegen ihrer gleichen Länge der gleichen Permutation beim Chiffrieren unterworfen waren, konnte man sie untereinander schreiben und in Spalten zerschneiden. Alle Buchstaben einer Spalte hatten bei der doppelten Spaltentransposition die gleichen Platzwechsel erfahren. Die Kunst (oder das Glück) bestand darin, die Spalten so zu kombinieren, dass sich wenigstens in einer Zeile ein sinnvolles Bigramm oder Trigramm ergab. Anlegen von sinnvoll ergänzenden Spalten an diesen Kern rechts und links führte dann u.U. zum Klartext dieser Sprüche. Damit waren aber die Schlüssel a bzw. b (Siehe Kap. 1.4.1.2) noch nicht bekannt. Bei GAINES[43] und KOZACZUK[44] sind die weiteren Schritte erklärt, die anschliessend an einem Beispiel erläutert werden. Im Beispiel ist aber, abweichend vom militärischen Sprachgebrauch, `CH` nicht durch `Q` ersetzt, um das

[43] GAINES, S. 56
[44] KOZACZUK b), Anhang B, S. 291

Verfahren durchsichtiger zu machen. So ist z.B. im ersten Spruch die Häufung dieser Buchstaben `C` und `H` auffällig. Das führt dazu, den Einstieg mit der Kombination `CH` zu versuchen. Mit Geduld und Sprachgefühl kann man die im Beispiel gezeigte Lösung für den Spruch 3 (zugleich natürlich auch die Lösungen für die anderen drei Sprüche) erhalten.

Beispiel zum Doppelwürfel-Schlüssel
Vorgegeben seien die Schlüssel

a : 5 9 14 1 12 8 17 15 19 2 10 4 13 18 6 1 16 3 7
b : 2 12 16 1 8 17 14 4 11 7 20 3 13 19 5 22 10 15 6 9 21 18 23

Unter diesem (noch unbekannt gedachten) Schlüssel werden 4 Sprüche gleicher Länge gehört:

```
   00000000011111111112222222222333333333344444444445
   12345678901234567890123456789012345678901234567890

1: NAXWCEEXANEERDCLEIEXSTADEMICOXASNXDASXSRIHHHOXNMHX
2: XDETSRMTESEINSXREHXXGBEUEVMAXXENRANNNSIAXTSGXEOIBK
3: RENGHMMRRNNWNIXEIXDXSIXSEDIEBEETLUNEDWOLSANIXXXSAI
4: NGTUXXTEXMCOXRESAHMLARXMITHSXFEAXOBXAUREMSXRMENRTI
```

In der ersten Zeile wären mögliche Kandidaten für eine Kombination die Spalten 5, 18, 28 mit den Spalten 42, 43, 44 und 49, wobei die Kombination (5,43) wegen des auftretenden `XX` in der vierten Zeile (wahrscheinlich) wegfällt. In der vierten Zeile wäre die Spalte 11 mit den Spalten 18 und 27 zu kombinieren:

```
11  18    11  27
 E   I     E   I
 E   H     E   M
 N   X     N   I
 C   H     C   H
```

Da die Silbe, bzw. das Wort, /ein/ im Deutschen sehr häufig ist, kann ein Versuch gemacht werden die Spalten 10, 33 oder 47 rechts anzufügen:

```
11 18 10  11 18 33  11 18 47  11 27 10  11 27 33  11 27 47
 E I N     E I N     E I N     E I N     E I N     E I N
 E H S     E H R     E H O     E M S     E M R     E M O
 N X N     N X L     N X X     N I N     N I L     N I X
 C H M     C H X     C H N     C H M     C H X     C H N
```

Die Spalte 47 liefert relativ unwahrscheinliche dritte Zeilen, die beiden Kombinationen können also (zunächst) weggelassen werden. Mit der Annahme, /ein/ sei ein Wort, können vorn bzw hinten eine der Spalten 3, 8, 20, 30, 34, 38, 46, oder 50 angefügt werden. Mit Spalte 50 (links) und Spalte 30 (rechts) ergibt sich der Verdacht auf das Wort /verkehr/ in der zweiten Zeile, dieser Verdacht erhärtet sich und führt schliesslich zum Lösungsansatz.

1	26	23	16	50	11	18	33	30	21	28	49	29	25	10	19
N	M	A	L	X	E	I	N	X	S	C	H	O	E	N	E
X	V	E	R	K	E	H	R	X	G	A	B	X	E	S	X
R	D	X	E	I	N	X	L	E	S	E	A	B	E	N	D
N	T	X	S	I	C	H	X	F	A	S	T	X	I	M	M

Die Lösung für Spruch 3 lautet:

morgenxwirdxeinxleseabendxseinximxwirtshausxlinden Bei der Lösung liegen die Streifen in der Reihenfolge

<u>7</u> 39 <u>8</u> 4 31 *13* 20 12 **27** 1 **26** 23 16 *50* 11 18 33 30 21 <u>28</u> 49 <u>29</u> 25 10 *19*
46 48 **36** 17 **35** 15 44 *6* 47 38 14 9 32 <u>41</u> 5 <u>42</u> 34 24 45 40 22 **3** 37 **2** 43

Auffällig sind Paare von Streifennummern mit gleichen numerischen Abständen (unterstrichen, kursiv bzw. fett). Die horizontalen Abstände dieser gleichartigen Paare sind gleich und zwar gleich 19. Der Schlüsselteil a hat also die Länge 19, d.h. die Spaltenzahl von a ist 19. Es liegt also nahe, die Streifennummern der Lösung in Zeilen mit der Länge 19 zu schreiben.

7	39	8	4	31	13	20	12	27	1	26	23	16	50	11	18	33	30	21
28	49	29	25	10	19	46	48	36	17	35	15	44	6	47	38	14	9	32
41	5	42	34	24	45	40	22	3	37	2	43							

Schreibt man die ersten Spalten des obigen Schemas als Zeilengruppen:

7	28	41	39	49	5	8	29	42	4	25	34	31	10	24
20	46	40	12	48	22	27	36	3	1	17	37	26	35	2
16	44			50	6		11	47		18	38		33	14
21	32													
						13	19	45						
						23	15	43						
						30	9							

und arrangiert die Zeilengruppen so, dass in den Spalten fortlaufende Zahlen von oben nach unten stehen.

Zwei Lösungen sind möglich:

(1)

4	25	34	1	17	37	7	28	41	30	9	23	15	43	11	47	21	32	13	19
5	26	35	2	18	38	8	29	42	31	10	24	16	44	12	48	22	33	14	20
6	27	36	3																
								45	39	49									
								46	40	50									

(2)

4	25	34	1	17	37	30	9	23	15	43	7	28	41	11	47	21	32	13	19
5	26	35	2	18	38	31	10	24	16	44	8	29	42	12	48	22	33	14	20
6	27	36	3																
								45	40	50									
								46	40	50									

Die Lösung (2) führt weiter.
Die Länge des Schlüsselteils b ist 23, man erhält ihn durch fortlaufende Numerierung der Spalten in Lösungsansatz 2.
Das Ergebnis:

2 12 16 1 8 17 14 4 11 7 20 3 13 19 5 22 10 15 6 9 21 18 23

Nun ordnet man den Spalten in Schema a ihre Position in der Folge der Zeilengruppen in (2) zu und erhält so

5 9 14 1 12 8 17 15 19 2 10 4 13 18 6 11 16 3 7

6.2.2.2 Substitutionsverfahren, („Ersatzverfahren“).

6.2.2.2.1 Doppelkastenschlüssel, («Double Cascet») In Deutschland wurde dieser Schlüssel bei SS, SD, Polizei, Heer und Luftwaffe benutzt. Das Aufkommen an Sprüchen war so gross, dass ein Teil davon als Schulungsmaterial und zum Training für den Nachwuchs des kryptologischen Personals benutzt wurde.

Auffällig ist, dass nur zwei Autoren das volle Doppelkastenverfahren, eigentlich ursprünglich Doppel-Kassetten-Verfahren, mit zweistufiger Chiffrierung beschreiben. Alle anderen sprechen nur von einem einstufigen Verfahren, wobei - natürlich - aus dem Gedächtnis auch Ungenauigkeiten auftreten können.

Dort, wo in deutschen Funkkreisen nur einstufig chiffriert wurde, war der Einbruch relativ einfach: 1941 und bis zur drastischen Kürzung der Zeit der Gültigkeit eines Schlüssels 1942 war die Spruchmenge relativ gross. Durch während des Tages fortlaufendes Mitzählen der Bigramme schälten sich bald die Frequenzen der häufigsten Buchstaben-Kombinationen heraus. Da i.a. die Absender bzw. Empfänger bekannt waren, liessen sich Klartextteile bilden, die dann die Konstruktionen der beiden Schlüsselquadrate ermöglichte. Hierbei waren wieder stereotype Meldungen (z.B. Bestandsmeldungen jeden Freitag um 18 Uhr) besonders aufschlussreich, da sie auch meist im selben Wortlaut abgefasst waren. Die Rekonstruktion der Quadrate für diesen einfachen Fall ist modellhaft bei CURRER-BRIGGS erläutert.[45]

Nach der Verkürzung der Gültigkeitsspanne der einzelnen Schlüssel auf drei Stunden im November 1942 wurden die Sprüche zunächst nicht mehr gelesen, noch dazu, wenn, wie in Afrika, Sender und Gegenstelle auf verschiedenen Frequenzen arbeiteten.

Durch die alliierte Aktion gegen die deutsche Nachrichten-Fernaufklärungs-Kompanie unter Hauptmann Seebohm bei Tel el Eisa in Nordafrika am 10. Juli 1942 gelangten die Alliierten in den Besitz der vollen Ausrüstung und fast aller Chiffrier-Unterlagen, auch Einzelheiten zum neusten Stand des Doppelkastenschlüssels.

Nach SCHICK[46] wurden auch die einzelnen Sprüche bei vollem, zweistufigen Schlüsselverfahren und Gültigkeit von nur drei Stunden dechiffriert, allerdings wurden die Kästen nicht rekonstruiert, was auch wegen der unbekannten Zwischenstufe einen erheblichen Aufwand bedeutet hätte. Praktikabler war es da, eine Bigrammtafel aufzubauen, wie sie in Tabelle 1.26 gezeigt ist. (1943 im Hauptquartier des 849th Signal Intelligence Service in Hammun-Melouane in Nordafrika, das später nach Sizilien und weiter in die Nähe von Caserta verlegte.)[47]

6.2.2.2.2 Übungsfunk. DAVID beschreibt ausführlich seine Erfahrungen bei der 12th Army Group (General Omar Bradley) mit dem Brechen dieses Schlüssels und sogar der Rekonstruktion der Kästen ab 1944. Vor der Invasion waren deutsche Funkstellen mit Übungsfunk beschäftigt, der aus persönlichen Mitteilungen, Zeitungsartikeln, Kinderversen u. dgl. bestand. Diese Phase half, das Ermitteln der Schlüssel zu üben. Die Zeilenlänge war zu dieser Zeit 21 Buchstaben lang gewesen. Die genaue Verkehrsanalyse und Peilung der Funkstellen half, die aufgenommenen Sprüche den Einheiten und damit dem jeweiligen Schlüssel zuzuordnen.

Nach DAVID wurden die zu einem Schlüssel gehörigen Sprüche auf die Häufigkeit der Bigramme hin untersucht. Ein Beispiel zeigt das Vorgehen:

[45] CURRER-BRIGGS, S. 285
[46] SCHICK, S. 33
[47] SCHICK, S. 33

```
 1  -  VDLVVKXRKCXVRBXABASKD
       DFXEGKMNZIWBTAWPFYOKE
 2  -  GKSQAVISKSNUTEKOCKCGF
       VUAZNRIMZRWIFGKKKLTTD
 3  -  WPNMYYKGCCDYMWOKFISMQ
       TDQYCXKDYPOPISZFLSOAE
 4  -  UQDOUNKINDHGOYPHMKNYB
       IQMQYDKBFAGQDMDAAIOYF
 5  -  DOERFBPVPU
       LKDIOREMQO
 6  -  MUMVIBVO
       PQKOIWDU
 7  -  KLOAZWSEZUCKSPKOTXCYU
       KSLFQMFDXDPZQXNMOVKDS
 8  -  CXSZOKW
       KCACMKP
 9  -  KNDCVMKSANILYSMCAPWBQ
       KSUPOKZKAQIKCLSKWSXCG
10  -  YKCSIUTOSGMDOGKKCKOOH
       WLDMZZPKASYARZKQMKVZB
11  -  NCFYKF
       LUTTZA
12  -  KUGYXKWSKRMKAUOVHKKNC
       KKBWWZHMMZUKEBKBGKFIP
13  -  VCGDSOLCKOKIWASVKFSUA
       BQQOVSRPLKQIBFRMKSXIN
14  -  TCKU
       NUKO
15  -  VDLVVKBUOUSHWVDYEBQOG
       DFXEGKZWZKAZXDFPDOAZQ
16  -  KFUKYLKUGOKIXWZLOXFKC
       KPDKEWIDVKTMMXCSNRXBP
```

Die Schwierigkeit beim zweistufigen Verfahren lag darin, dass nicht die Häufigkeit der Bigramme zu erkennen war, sondern, dass die individuellen Häufigkeiten der Einzelbuchstaben in den Paaren zum Tragen kam. Dazu kam die Erschwernis, dass jede Division ihre eigenen Verchlüsselungsmatrizen hatte, deren Kombination alle drei Stunden geändert wurde. (Vgl. Kap. 1.4.1.1)

Im Beispiel fällt auf, dass das Bigramm `KK` bei weitem am häufigsten auftritt. Daher ist der (vorläufige) Schluss erlaubt, dass es sich dabei um den Klartext `ee` handelt. Die wesentlichen und häufigsten deutschen kurzen Sprüche von 6 bis 12 Buchstaben Länge waren bekannt. Der sehr kurze Spruch Nr. 14

```
..e.
TCKU
NUKO
..e.
```

konnte als Stereotyp „Wie Lage“ (richtig) angenommen werden. Ein sehr grosser Teil der deutschen Funksprüche begann entweder mit `/An/` oder `/E/` (erbitte, ein, eins, eigene). In Spruch Nr.9 hat auch das Bigramm `KZ` sehr grosse Häufigkeit, sodass der

Versuch erlaubt war, dafür zu setzen

```
erbitte..
KNDCVMKSA
KSUPOKZKA
e........
```

und, folglich in Spruch Nr. 12

```
eigene.....e.
KUGYXKWSKRMKA
KKBWWZHMMZUKE
e............
```

Für Spruch 6 ergab sich

```
bittelag
MUMVIBVO
PQKOIWDU
emeldung
```

und schliesslich im ersten Anlauf für die Sprüche 1 und 15

```
anxroemxeinsxantonfei
VDLVVKXRKCXVRBXABASKD
DFXEGKMNZIWBTANPFYOKE
ndliqe.............e.

anxroemxeinsxantonfei
VDLVVKBUOUSHWVDYEBQOG
DFXEGKZWZKAZXDFPDOAZQ
ndliqe.......nd......
```

Falls in einer Schlüsselperiode genügend viele Bigramme erkannt waren, konnte der Versuch unternommen werden, die Schlüsselquadrate selbst zu entwickeln. Dabei konnte Gebrauch gemacht werden von den Eigenschaften des Chiffrierverfahrens.[48]
DAVID bestätigt, dass auch nur einfache statt doppelte Chiffrierung aufgetreten war.[49]

Diese Schlüssel wurden nicht nur, wie die Beispiele zeigen, „vor Ort“ bearbeitet, auch das Personal in Block F in BP war mit ihnen befasst.

Die Doppelkasten-Sprüche von SS und SD wurden auch von REJEWSKI und seinen polnischen Mitarbeitern nach ihrem Eintreffen in Boxmoor dechiffriert. Aber auch hier halfen unverständliche Fehler dem Kryptologen: Bei einer Division wurde z.B. einmal ein und derselbe Spruch nacheinander gesendet im neuen Schlüssel, im alten Schlüssel und schliesslich sogar noch im Klartext ! Ausserdem, wie oben gesehen, halfen stereotype Wendungen und immer wiederkehrende Abkürzungen als Klartextspuren.[50]

Ihre grösste Bedeutung haben die Hand-Schlüsselverfahren der Marine gefunden, die auf Bigrammtausch beruhten hierbei aus der Sicht der Alliierten vor allem der Werftschlüssel.

[48] DAVID, S. 72
[49] DAVID, S. 74 - 76
[50] KOZACZUK a), S. 209

6.2.2.2.3 Werftschlüssel. Er wurde ab 15. Mai 1940 verwendet. Nach MORRIS ist der Verkehr in diesem Schlüssel offenbar bereits im April 1940 entdeckt worden.[51] Ein Einbruch gelang erst, nachdem ein Beutedokument zu diesem Schlüssel im Frühsommer 1940 vorlag[52] und somit das Verfahren (und auch einige Klartexte) bekannt war. Auch die Tatsache der Selbstreziprozität der Tauschtafel (Wenn `rt` $\mapsto$ `MU`, dann `mu` $\mapsto$ `RT`) half. Unter der Voraussetzung, dass hinreichend viele Sprüche eines Tages vorlagen, konnten mit Bigramm-Frequenz-Analysen der einzelnen Spalten und Klartextstücken stückweise Tauschtafeln der zwei Monate (später: des Monats) rekonstruiert werden. Auch hier halfen unnötige Stereotype ganz erheblich. Eine Schwäche des Werftschlüssels lag auch darin, dass einige Funker die in der M.Dv.Nr. 103 als Füllwörter genannten Beispiele wörtlich übernahmen. Diese Wörter (Wassereimer usw.) hatten aber die Eigenschaft, in den 5er-Gruppen u.U. Bigramme aus häufigen Buchstaben zu bilden, was den Einstieg in die Analyse der Tauschtafeln durchaus erleichtert haben könnte.

Über den Werftschlüssel erfuhren die Alliierten viele Einzelheiten über Schiffsbewegungen, Küstengeleitzüge, Indienststellungen usw., was im einzelnen vielleicht nicht von hoher operativer Bedeutung gewesen sein mochte, es lieferte aber im Gesamtbild wichtige Mosaiksteine. Der Werftschlüssel hatte aber seine immense Bedeutung darin, dass viele Funksprüche sowohl im Werftschlüssel als auch in ENIGMA-Schlüsseln der U-Boote (im wesentlichen „Heimisch“) abgegeben wurden. So war es möglich, dass beide Schlüsselformen gegenseitig Klartexte liefern konnten. (Im Extremfall soll z.B. die Beförderung von DÖNITZ zum Admiral in fast allen Schlüsseln mit gleichem Wortlaut verkündet worden sein.)

Wenn neue Schlüsseltafeln gültig wurden und aus anderen Schlüsseln kein vermuteter Klartext vorlag, halfen sich die Briten, indem sie Funksprüche provozierten (Operation «Gardening»): In geräumte Seewege wurden z.B. Minen abgeworfen, was Sperrnachrichten provozierte. Ein Beispiel für das Ineinanderspielen von ENIGMA- und Werftschlüssel-Sprüchen in einem solchen Falle gibt ERSKINE.[53] MORRIS schreibt[54], dass von März 1941 an täglich etwa 23 Sprüche im Werftschlüssel gelesen wurden.

6.2.2.2.4 Das Reservehandverfahren. Es beruhte ebenfalls auf Bigrammtausch. Wegen der Kompliziertheit des Verfahrens gelang ein erstes Lesen jedoch erst im Juni 1941, nachdem entsprechende Unterlagen erbeutet worden waren.[55] Eine Hilfe zum Einbruch in das R.H.V. war dabei das Kenngruppenbuch mit den dazugehörigen Zuteilungslisten und Tauschtafeln. Dabei wurde bemerkt, dass die Chiffrierer bevorzugt Trigramme aus dem Oberteil der Spalten aus den mittleren Seiten des Kenngruppenbuches verwendeten[56]

Das vor dem Chiffrieren des eigentlichen Spruchtextes liegende Auswählen von Kenngruppen und ihre Chiffrierung mit einem eigenen Verfahren diente letztlich nur zur Festlegung, welche Tauschtafel des R.H.V. für jede der vier Spalten des Spruchtextes angewandt werden sollte. Mit der allen Bigrammtauschtafeln eigenen Reziprozität wurde es bei Vorlage von hinreichend vielen Sprüchen möglich, nicht nur die Einzelsprüche, von denen man Klartextteile hatte, zu lesen, sondern man konnte stückweise auch die Tauschtafeln selbst rekonstruieren.

Ein Beispiel soll das verdeutlichen:

---

[51] MORRIS, S. 112

[52] Diese könnten von U 13 stammen, das im Juni 1940 versenkt wurde. Dem könnte aber widersprechen, dass Front-U-Boote den Werftschlüssel nicht mitführen durften. (Überarbeitung der Dienstvorschrift von 1944)

[53] ERSKINE a), S. 166

[54] MORRIS, S. 232

[55] Von U 110 am 9.5.41 (Tauschtafel „Bach“ , von Gedania am 11.6.41 („Teich“) und von Geier (VP 5904 am 1.1.42 („Ufer“ , „Strom“), ERSKINE b), S. 501

[56] SEBAG-MONTEFIORE, S. 187

```
        1 2 3 4 5 6 7 8 9 0 1 2

 1      v o r h e r s a g e v o     W Y H B R S L F K A C K
 2      n v o n w e w a b e r g     B A H J L V J V X L F U
 3      e n a n f a n g s s u e     E E A V V X C U B B I R
 4      d b i s s u e d o s t v     J M C Z Q G I O Y Q O T
 5      i e r b i s s e c h s i     A K O T W Z Q D R I K P
 6      m s u e d t e i l s i e     N G Q F L O M G X X M Z
 7      b e n b i s a c h t o e     X D O X B T A G A L Q D
 8      r t l i c h n e u n s p     B T K U I V F Q L Y V K
 9      a e t e r r e c h t s d     W I S H U O F I H S D Q
10      r e h e n d b e d e c k     O Z X M B B U E Y A T H
11      t r e g e n t e i l s a     T W E X D S E R S Y A D
12      l s s c h a u e r m i t     O O X C Y J D K M C I B
13      s c h n e e v e r m i s     W J H T O X L M T Q B J
14      c h t m a e s s i g e s     F L S Z N V D L G O D V
15      i c h t s e e f u e n f     D D C H S R S Z Y R Q Q
16      b i s s e c h s a u s s     S B D O F N N P J W F B
17      i c h t e n f u e r m o     A H N W Q M T L J J O X
18      r g e n x x s u e d w e     S T F J P T M J I G U D
19      s t b i s w e s t v i e     Y E H K H H U R V C E F
20      r b i s s e c h s o e r     R Q S Q Z Q U F E K D N
21      t l i c h s i e b e n w     V H Y P V K Z X M O J B
22      e c h s e l n d w o l k     P D I M Y J V B Q K C A
23      i g s c h a u e r o e r     P H C M Q R A A C A D Z
24      t l i c h r e g e n m i     Y J R B S Z G T D O W T
25      s c h n e e g e m i s c     D Q X E N J D S N W C C
26      h t a n f a n g s m a e     V C A Q X B F Q W R L E
27      s s i g e s i c h t s p     M G H P I A U Q C I H T
28      a e t e r s i c h t b e     F W V H P Q X G V N N Y
29      s s e r u n g s e e f u     D Q E U V T W N R T C S
30      e n f b i s s e c h s f     S W H Q X U K Y Q Y N K
```

Zahlenreihe zum Verteilen des Klartextes im „Kasten“:

3 4 11 6 12 2 8 5 10 1 7 9

Geheimtext in senkrechten Bigrammen

```
 1. WBEJ     2. WOTO     3. ASYR     4. DVMF     5. EMKG
    ANXB        WFDS        VPPY        DSYA        DTIZ
 6. WOJT     7. EQHD     8. GWQW     9. OQOK    10.HSCD
    DBHT        HJQC        HHAC        SXEX        NFHS
11.YICR     12.EHBJ     13.XUHM     14.HOWJ     15.MBEQ
    XAHV        VZTF        XCTZ        KQPM        PHUQ
16.RLVQ     17.UBDY     18.QPHZ     19.NXIP     20.XGZO
    WLBI        ONSF        VYQS        VXSV        TVOB
21.SJXV     22.HQKJ     23.AQTU     24.QMAF     25.LDSN
    RNMT        RZJB        LJCI        FUED        TMUU
26.ZVAG     27.WKFV     28.GQIE     29.ZPLJ     30.ATSQ
    DFUX        OUDG        RKML        RFXB        QGNY
31.KXBY     32.HYSM     33.JIVE     34.NWCV     35.BQIX
    RXAL        TGYJ        MQCD        RQAL        LYSA
36.YCQO     37.CKOK     38.INTY     39.KMQV     40.BDQF
    RWJG        AOWR        CFIO        DTAI        UOED
41.JCDW     42.CNKU     43.DKQH     44.QBXD     45.ZTCE
    CLHN        RTPZ        DBJV        FNBA        TYSK
```

Bearbeitung des Materials: Die hier verwendeten Bigramm-Tauschtafeln sind aus Platzgründen nicht angegeben[57].

In der Liste des Geheimtextes in Vierergruppen wurde nach mehrfach auftretenden Bigrammen gesucht.

```
BN 2 130 - BN 2 346 - BN 130 346;  JB 4 172 - JB 4 228 -
                       JB 172 228
QJ 50 178 - QJ 283 339;  SR 16 80 - DD 25 337 - DE 29 45 -
                       MT 34 306
DW 37 205 - HQ 51 139 - QA 59 307 - CH 75 83 - VX 93 149 -
                       XX 146 242
   IS 147 275 - RH 165 245 - RA 173 229 - IF 184 312 -
           QF 185 345  - FD 188 316 - KO 210 290
```

Ihre Position wurde durch den ersten Buchstaben gegeben.

Beispiel: BN in Gruppe 1: $0 \cdot 30 + 2 = 2$ und $4 \cdot 30 + 10 = 130$.

Gesucht waren nun Bigramme, die in Zeile 2 (und 6) und Zeile 10 (und 16) übereinstimmten. Hier ergab sich die Entsprechung BN $\mapsto$ es, also entsprach die Spalte 10 des Klartextes der Spalte 1 des Geheimtextes. Die Gruppe es in Spalte 5 des Klartextes entspricht der Gruppe BN der Spalte 12 des Geheimtextes. Die Buchstaben B sind in obigem Geheimtext unterstrichen.

Bigramm CH: $2 \cdot 30 + 15 = 75$ und $2 \cdot 30 + 23 = 83$. Hier haben die Gruppen den Abstand 8, standen in derselben Spalte der Viergruppen und wurden dementsprechend mit derselben Tafel chiffriert. Es ergab sich CH $\mapsto$ is und damit die Zuordnung der 1. Spalte des Klartextes mit der 3. Spalte des Geheimtextes.

Bigramm JB: $0 \cdot 30 + 4 = 4$ und $5 \cdot 30 + 22 = 172$. Daraus folgt JB $\mapsto$ sn und die Zuordnung der 4. Klartextspalte zur 6. Geheimtextspalte. Weiter JB: $7 \cdot 30 + 18 = 228$, somit gehörte zur 7. Klartextspalte die 8. Geheimtextspalte.

Bigramm HQ: $1 \cdot 30 + 21 = 51$ und $4 \cdot 30 + 19 = 139$ liefern mit HQ $\mapsto$ sc die weiteren Zusammenhänge 6. Klartextspalte mit der 2. Geheimtextspalte und 8. Klartextspalte mit der 5. Geheimtextspalte.

Mit dem Bigramm XX $\mapsto$ ge wurden mit $4 \cdot 30 + 26 = 146$ und $8 \cdot 30 + 2 = 242$ der 12. Klartextspalte die 9. Geheimtextspalte zugeordnet, mit dem Bigramm FD $\mapsto$ si die 11. Klartextspalte der 7. Geheimtextspalte und die 3. Klartextspalte der 11. Geheimtextspalte. Mit dem Bigramm QJ $\mapsto$ re wird der 9. Klartextspalte die 10. Geheimtextspalte zugeordnet. Mit weiteren Bigrammen liessen sich mehr Klargruppen zu den Geheimbigrammen bestimmen und so die benutzten Schlüsseltafeln entweder bestimmen oder rekonstruieren. Der Vergleich mit den obigen Daten zeigt die Übereinstimmung.

Dieses Beispiel wurde von vornherein mit der richtigen Schlüssellänge demonstriert. Wenn diese falsch angenommen wird, ergeben sich Widersprüche.

Auf diese Weise ist es zu verstehen, dass ab Mitte 1941 im Mittel täglich 12 Sprüche in diesem Verfahren gelesen werden konnten. Auch hier war die Verflechtung der Sprüche mit denen anderer Chiffrierverfahren, insbesondere mit ENIGMA - Schlüsseln, nützlich.

[57] Der Klartext ist entnommen aus: «Methods for dealing with RHV - 1942», NARA Dokument No. 4378, ZEMA 190, S. 7

6.2.2.2.5 Wetterschlüssel. Die Bedeutung der Wetterschlüssel, der Wetterkurzschlüssel (WKS), der chiffrierten Wetteraussendungen (SY) der Sender DAN (Norddeich), DDX (Berlin) u.a., letztere bearbeitet in Hut 10, beruhte darauf, dass über diese Schlüssel die Textschlüssel, u.U. die Tagesschlüssel, der U-Boote ermittelt werden konnten. U-Boote gaben ihre Wettermeldungen (auf Anforderung) als Wetterkurzsprüche ab, die mit ENIGMA chiffriert wurden. Die Zentrale strahlte die Inhalte dieser Wettermeldungen als Wettersprüche, strukturiert nach dem International Meteorogical Code (IMC) und chiffriert (s. Kap.1.3.2.6) aus. Die Art der Chiffrierung versuchte, die Zusammenhänge zwischen auftretenden Wiederholungen im IMC und in der SY-Aussendung zu beseitigen, was nicht ganz gelang.

Seit Februar 1941 konnte Hut 10 diese Wetterschlüssel brechen, der Klarinhalt der U-Bootsprüche war also bekannt[58]. Hierbei war allerdings die Schwierigkeit zu überwinden, die Zuordnung von Wetterspruch (SY) und Wetterkurzspruch herzustellen. Einmal im Besitz des Klartextes des Wetterkurzspruchs konnte in Hut 8 aus vorhandenem Klar- und Geheimtext der Schlüssel gefunden werden. [59]

Der Einbruch in den Wetterschlüssel setzte die Kenntnis der Trigramm-Schlüsseltafeln voraus. Es war also nötig, alle Tafeln während der 5-Tage-Periode zu rekonstruieren. Es stellte sich aber heraus, dass diese Tafeln nach etwa einem Monat für fünf bis sechs Tage wiederverwendet wurden. Zwar dauerte es einige Tage, eine neue Tafel zu rekonstruieren, aber wenn eine wiederverwendete Tafel auftauchte, war die Arbeit leicht[60]. Alle Sprüche innerhalb jeder 24-Stunden-Dauer von DAN, DDX, HBP (Wien), PZR (Rom), MBY (Paris), ZJL (Danzig) mussten aufgenommen werden, dazu die Klarsendungen spanischer und portugiesischer Wettersender täglich 0200 Uhr, 0500 Uhr, 1900 Uhr und 2300 Uhr. Diese Klarsendungen wurden lange Zeit von PZR chiffriert wiederholt. Bei der Aufnahme der Sprüche musste genau darauf geachtet werden, dass nur solche jeweils einer einzigen Zeitgruppe gemeinsam betrachtet wurden. Wenn sichergestellt war, dass zur Untersuchung Sprüche nur einer Quelle und nur einer Zeitgruppe vorlagen, konnte das Durchmustern nach wiederholten Trigrammen beginnen. Wenn z.B. mehrere Hundert verschiedener Sprüche von einer einzigen Tafel erfasst worden waren, dann konnten sie mit Hilfe einer IBM-Anlage nach wiederholten Trigrammen an bestimmten Positionen durchgemustert werden. Hierbei wurde diese Suche auf die Positionen 1 ($II.$), 3 ($ww.$), 5 ($DD.$), 7 ($PP.$), 9 ($UC_h.$), 2 ($.C_L$), 4 ($.C_M$), 6 ($.WN$), 8 ($.TT$) und 10 ($.pp$)) in dieser Reihenfolge gelegt. Es war bekannt, welche Klarelemente an welchen Stellen des SY auftreten mussten bzw. könnten.

Beispiele:

> Das Trigramm 00. muss als drittes, fünftes und neuntes Trigramm auftreten, .00 an den Stellen 2 und 6. Wenn also ein WS-Trigramm an den Stellen 3, 5 und 9 mit höchster Frequenz auftritt, dann gehört es zu 00.
> Falls 00. in $.hN_h$ auftritt, dann ist es 009.
> Trigramme, die gleichzeitig sehr häufig in $.C_LC_M$ und in $.WN$ auftreten, sind .00.
> Trigramme, die in $.hN_h$ sehr häufig auftreten, sonst aber selten, sind .90.
> Trigramme, häufig in $ww.$, sind i.a. 03.
> Trigramme, die häufig in $.C_LC_M$ zu finden sind, sind i.a. .04

Es gibt noch mehr detaillierte Regeln[61], die es gestatteten, die Substitutionstafeln mehr oder weniger vollständig zu entwickeln. Das folgende Beispiel stammt aus der ersten Zeitgruppe vom 6. Juni 1943. Dieselbe Tafel wurde übrigens wieder benutzt in

[58] HINSLEY I, S. 339
[59] KAHN a), S. 189
[60] BUDIANSKI, S. 285
[61] NARA Dokument Box ZEMA07, Nr. 3776 «Outline of Procedures for the Solution of Main German Six–figure Meteorological Reports», S. 19 - 21

der 8. Zeitgruppe am 9. Juni und in der ersten Zeitgruppe am 10. Juni desselben Jahres.

WS-Trigr.	$II.$	$ww.$	$DD.$	$PP.$	$UC_H.$	$.C_LC_M$	$.hN_h$	$.WN$	$.TT$	$.pp$	SY-Trigr.
221	1	17	27		8			2		23	001
965	1	8	18		7	2				15	002
953		16	15	1	7			4		6	003
227	2	33	33	4	11	4		1		5	004
467		10	19		7	3		1		11	005
856	1	9	13	1	4					1	007
507	1	19	9		2	1			1	1	008
308		11	28	1	5		2		1	3	009
495						22		33		9	100
877	5		2	9		19		14		10	200
526			3			25		12		5	300
736	1					17		15		3	400
418	1			1		17		18		5	500
230					6	26		32		5	600
166	3				7	16		6		3	700
407	1				17	19		6		4	800
215	1			1	11	17		13		9	900
502				8		1	43				190
388	1						24				090
432		1					36		3		390
766							38				490
030	1		1				21			1	590
511				1			21				790
992					1		29			5	890
654							22		3	1	990
227	2	33	33	4	11	4		1		5	004
390				1		9				1	104
082	2		3	1	1	2			1	6	204
085	2					4				5	304
368	1				6	1			1	5	904
492		10									03.
107	4	4				1					030
960		7									033
469		3									036
595		3							1		038

Da auch verschiedentlich aus manchen Quellen (Spanien, Portugal, Finnland, z.T. auch Frankreich) Wettersynopsen offen ausgegeben wurden, ein Teil davon durch deutsche Sender chiffriert wiedergegeben wurden, war es möglich, durch Klartext-Geheimtext-Vergleich den Schlüssel zu ermitteln.

Französischer Klartext:

SY-Gruppen Zeile	1	2	3	4	5
1	210x-	02864	—	14429	54203
2	20675	02764	26225	15426	60300
3	21620	01852	10202	16128	60805
4	22178	02851	26311	17826	51803
5	2250-	03858	00028	19021	7-602
6	23150	01841	20301	17522	73600
7	23336	01862	16413	14632	33804
8	24020	01761	16201	16624	80803

Dieser Klartext, kombiniert mit dem chiffrierten deutschen Spruch, dabei sind statt der mittleren unbekannten zwei Ziffern Punkte gesetzt.:

SY-Gruppen Zeile	1	2	3	4	5
1 A	21..-	02..64	-..-	14..29	54..03
1 B	069873	152653	303382	005506	691463
2 A	20..75	02..64	26..25	15..26	60..00
2 B	185410	202207	896456	683941	032206
3 A	21..20	01..52	10..02	16..28	60..05
3 B	935296	714428	162188	059478	019660
4 A	22..78	02..51	26..11	17..26	51..03
4 B	640604	864884	744038	514441	741463
5 A	22..0-	03..58	00..28	19..21	7-..02
5 B	296095	993626	432214	075786	248545
6 A	23..50	03..58	20..01	17..22	73..00
6 B	885308	028969	862254	587351	119206
7 A	23..36	01..62	16..13	14..32	33..04
7 B	701739	960288	572657	892666	581183
8 A	24..20	01..61	16..01	16..24	80..03
8 B	519809	038579	005126	572430	504399

Die beiden Trigramme 038 in den Zeilen 4 B und 8 B ergänzten sich zur Aussage

$$(\text{WS})\ 038 = (\text{SY})\ 011.$$

Daraus folgte, dass die volle Gruppe (WS) 263011 lauten musste, also

$$(\text{WS})\ 263 = (\text{SY})\ 744.$$

Mit weiteren Zeilen der beiden Sprüche liessen sich dann neue Entsprechungen

$$(\text{WS}) \mapsto (\text{SY})$$

finden und so die Schlüsseltafel stückweise rekonstruieren.

6.2.2.2.6 Wetterkurzschlüssel. Die erste Ausgabe WKS (Wetterkurzschlüssel) „Weimar“wurde sehr früh im Kriege erobert, die zweite „Eisenach“, die ab 20. Januar 1942 in Kraft war, wurde Ende Oktober von U 559 beschafft. Die dritte „Naumburg“, seit 10. März 1943 in Kraft, wurde im Juni 1944 erobert.[62]
Im Frühjahr 1941 wurden erstmals die SY mit den WKS gemeinsam bearbeitet. Hierbei half, dass die Windrichtung durch vier teilbar sein musste, die geografischen Koordinaten der Position nur ganzzahlig sein durften. Hinzu kamen Vergleiche der Zeitgruppen beider Wettersprüche, der Position mit Peilungserkenntnissen. U.U. half auch der Funkname der U-Boote, die zur Abgabe von Wettermeldungen aufgefordert worden waren. Aus zwei WKS vom 28.2.1942 waren die Funknamen bekannt, aus den SY die übereinstimmende geografische Länge. Diese Angaben reichten aus, um beide Klartexte zu finden, dabei ergab der Vergleich mit den SY, dass die Tafeln für die geografischen Koordinaten linear strukturiert waren.
Auf diesem Wege wurden mit weiteren Dechiffrierungen die Tafeln 1 und 2 des Wetterkurzschlüssels rekonstruiert und bemerkt, dass die Tafeln 4, 5, 7 und 8 identisch waren mit denen der früheren Ausgabe.[63] Ebenso wurde die Tafel 9 stückweise rekonstruiert. Als im Juni 1942 landgebundene Stationen in Norwegen WKS aussendeten, waren natürlich die geografischen Koordinaten fest, die Dechiffrierung damit erheblich erleichtert.

Voraussetzung war das intensive Zusammenwirken von «Hut 8» , «Hut 6» mit der meteorologischen Abteilung, dem U-Boot-Raum, den Peilstationen und der Admiralität.

Das Erobern aller Tafeln in U 559 ermöglichte nun regelmässiges Lesen der WKS.

6.2.3 Kryptanalyse der ENIGMA.

6.2.3.1 Allgemeine Methoden.

6.2.3.1.1 «Cribbing». Wenn zwei Klartexte mit derselben Anfangsstellung chiffriert werden, werden gleiche Buchstaben an gleichen Stellen in gleiche Geheimbuchstaben überführt. Ein Beispiel soll das zeigen[64], dabei ist der Geheimtext, wie üblich in Grossbuchstaben geschrieben, der Klartext in kleinen Buchstaben.

B H N W S M S A W M N T C K N N P Z . .
w e t t e r f u e r d i e n a c h t . .
C N N J T R Q N W S T T C X R C D S L D
m i t m m m d r e i s i e b e n e i n s

Wie man sieht, stimmen auch die Paare r $\mapsto$ M und m $\mapsto$ R bzw. c $\mapsto$ N und n $\mapsto$ C überein.
Wenn man andererseits zwei Sprüche hat, für einen vermutet man den Inhalt, dann hat man verschiedentlich das Glück, dass ein anderer Spruch stellenweise übereinstimmende Geheimbuchstaben aufweist. Im oberen Beispiel sei der erste Spruch mit vermutetem Klartext gegeben, sowie ein weiterer Spruch:

B H N W S M S A W M N T C K N N P Z
w e t t e r f u e r d i e n a c h t
C N N J T *R* Q N W S T T C X R *C* D S
. . t . . *m* . . e . . i e . . *n* . .

[62]ERSKINE h)
[63]Bei ALEXANDER ist ein (fiktives) Beispiel dargestellt
[64]Dieses und die folgenden Beispiele stammen aus MAHON

Die kursiven Buchstaben in den beiden letzten Zeile folgen aus der Tatsache, dass zu einem Klar-Geheimpaar `r M` das entsprechende Paar `R m` gehört, zu `c N` das Paar `n C`.

Wenn man von mehreren Sprüchen die Trigramme für die Textschlüssel aus derselben unbekannten Grundstellung hat, kann man versuchen, diejenigen Sprüche, deren Trigramme sich nur in der 3. Stelle unterscheiden, evtl. mit vermutetem Klartext untereinander zu positonieren, um ggf. Übereinstimmungen zu finden. Im folgenden Beispiel stehen zunächst zwei vermutete Klartexte für den ersten Spruch zur Wahl.

1. Trigramm: `H E X`

```
B H N W S U H D W M T N C N . .
v o r h e r s a g e b e r e . .
w e t t e r b e r e i c h d . .
```

2. Trigramm: `H E N`

```
F D Q R L T U L E W G D Q P B
z u s t a n d o s t w a e r t
```

Der zweite Spruch wird nun verschoben, bis mit dem ersten Übereinstimmungen auftreten. Das ist hier bei vier Schritten der Fall:

```
. . . . B H N W S U H D W M T N C N K H P Z F H Y F R U E K L I G
. . . . v o r h e r s a g e b e r e i c h d r e i t e i l e i n s

F D Q R L T U L E W G D Q P B O X N Z R N C I O Z H X H R R N I N
z u s t a n d o s t w a e r t i g e r k a n a l x x . . . . . n .
```

An den im ersten Spruch unterstrichenen Stellen sieht man die Übereinstimmungen mit dem zweiten Spruch. Aus weiteren passenden Sprüchen lassen sich u.U. die Lücken in den Klartexten Füllen und so weitere Klar-Geheim-Paare finden, wie die Weiterführung des Beispiels mit einem 3. Bigramm `H E K` zeigt:

```
. . . . . . . B H N W S U H D W M T N C N K H P Z F H Y F R U E K L I G
. . . . . . . v o r h e r s a g e b e r e i c h d r e i t e i l e i n s

. . . F D Q R L T U L E W G D Q P B O X N Z R N C I O Z H X H R R N I N
. . . z u s t a n d o s t w a e r t i g e r k a n a l x x . . . . . n .

A V A J V Q S K T W R G P S I Q T R E B H U S E C D L S S J I E Q A I P
. . . . . s . . n . . . . h . e . . n . . . . . n . o . . . u l . . . .
```

Beim dritten Spruch drängt sich das Ergebnis „ohne sinn" auf. Dieses Verfahren wurde in Grossbritannien «Depth Cribbing»[65] genannt. Es erwies sich als besonders nützlich in der Zeit des «Black Out», als wegen der Einführung der ENIGMA M 4 zunächst kein Eingriff in die möglichen Klartexte möglich schien. Die Ähnlichkeit im Vorgehen mit dem beim Banburismus ist deutlich. In der Tat gehörten beide Verfahren eng zusammen. Als der Banburismus Ende 1943 überflüssig wurde, weil genügend Bomben zur Verfügung standen, fand auch die Methode der Suche nach Übereinstimmungen „in der Tiefe" ihr Ende. Zusätzlich wurden über Hollerith-Maschinen alle Sprüche eines Tages miteinander verglichen bzgl. Koinzidenzen von Bigrammen, Trigrammen usw.

Anfang eines jeden Monats wurden die Diskriminanten und die ersten erkannten Tagesschlüssel der verschiedenen Schlüsselbereiche mit den Archiven verglichen, ebenso die Walzenlagen, die Ringstellungen und die Steckerpaarungen. Für manche Schlüsselbereiche gab es teilweise Wiederholungen, einmal sogar beim Afrikakorps eine gesamte

[65] MAHON, S. 32

monatliche Schlüsseltafel. Damit war manchmal am ersten Tag eines Monats zu erkennen, welche Einstellungen, wenngleich möglicherweise verwürfelt, für den Rest des Monats zu erwarten waren.[66]

«Straight Cribbing» wurde die Methode genannt, bei der es sich darum handelte, den Inhalt, und damit den wahrscheinlichen Wortlaut, eines Spruches zu vermuten, ohne Tiefe und ohne Kenntnis des Inhalts aus anderen Schlüsseln. Natürlich half bei der Suche die reziproke Eigenschaft der ENIGMA durch den Ausschluss unmöglicher Positionen.

Man musste sich dabei auf die Analyse des Verkehrs stützen und aus der Menge der Sprüche, auf Grund früherer Erfahrungen, die herausfiltern, die verwertbare Inhalte enthalten könnten. Frequenzen, Rufzeichen, Zeitangaben und Länge waren hier Faktoren, die hilfreich waren. Voraussetzung war hier, alle für die Suche evtl. brauchbaren Sprüche über lange Zeit genau zu registrieren und zu vergleichen. Als die Signaturen in einigen Schlüsselkreisen im Spruch selbst verborgen wurden, war das Verfahren sehr erschwert.

Immer wieder war aber die Funkdisziplin so schwach, dass die Klartextpassagen gewissermassen in den Schoss fielen, z.B. funkte im Sommer 1942 Boulogne etwa 3 Monate lang Wettermeldungen mit dem Beginn ZUSTANDOSTWAERTIGERKANAL ! Allerdings wurden im Laufe der Zeit diese kardinalen Fehler abgestellt, auch die Wettermeldungen aus dem Bereich Norwegen oder Ostsee.

Dafür war die Suche nach Wiederholungen bei anderen Absendern erfolgreich, z.B. wenn Alderney täglich dem Seekommandanten Kanalinseln meldete FEUER BRANNTEN WIE BEFOHLEN. Diese regelmässigen Berichte, sofern sie immer in derselben Form abgegeben wurden, waren ideale Quellen für verwendbare Klartexte.

Eine Zeit lang half die Verwendung der Tasten `Q,W,E,R,T,Z`... als Ersatz für die Ziffern `1,2,3,4,5,6`... für stereotype Wettermeldungen zum Finden von Klartextabschnitten.[67]

Beispiel:

```
P P Q I P P W Y Q U E P T O Y
P T W Q T P R Y Q E Z O T I Y
Q P W P Q P E Y Q E T W T Z Y
```
usw.

Hier waren die Buchstaben in den Spalten 1 und 2 immer konstant, sie gaben die Messstation an. die `Y` in den Spalten 8 und 15 waren Kommata, die 9. Spalte enthielt immer die 1 (`Q`). So entstanden die Klartextteile

```
P P . . . . . Y Q . . . . . Y P T . . . . . Y Q ...
```

Ab 1942 wurden Klartexspuren entdeckt, die periodisch auftraten, z.B. im zweimal täglich für die U-Boote in der Arktis gesendeten Wetternachrichten. Drei Funker (A,B,C) wechselten sich tageweise schichtmässig ab, wie z.B. BAC/ACB/CBA/BAC ..., wobei einer den Monatsnamen ausschrieb, die anderen beiden gaben die Monatszahl an (`VIER` für `APRIL`). Ende 1943 bis Frühjahr 1944 gaben drei Fischdampfer aus dem Nordmeer in einem besonderen Handschlüssel Wettermeldungen ab, meist 35 Zeichen lang, 5 Zeichen Präambel, die letzten Zeichen waren ständig `XX,XXXXX`, die aber als `XANTXANT` usw. abgegeben wurden, was einen sichern Klartext von 29 Buchstaben ergab. Diese Sprüche wurden in Tromsö in einen anderen Handschlüssel umgeschlüsselt, nach Wilhelmshaven übermittelt und von dort in „Heimisch" ausgestrahlt. Dabei blieben der Ursprung, die Zeitgruppe und die Seriennummer ungeändert.Zusammen mit den `XANTXANT` ... ergab das einen so sicheren Klartext, dass in dieser Zeit, unabhängig

[66] HINSLEY II, S. 375; BENNETT a), S. 125
[67] MAHON, S. 42

von anderen mit 21 solchen alle 15 Monatsschlüssel in „Heimisch“ gefunden wurden. Eine weitere Verfahrenskonstanz verhalf zu Klartextabschnitten: Jedes U-Boot hatte eine Meldung abzugeben, wenn es die Biscaya verliess oder den 60. Breitengrad Nord überfuhr. Bei der Rückkehr waren Meldungen gefordert mit Position und voraussichtlichem Einlaufen. Dabei wurden weitere Angaben verlangt, die fast alle Zahlenangeben erforderlich machten, was der Anwendung des EINS–Kataloges (siehe Kap. 6.2.3.1.8) entgegen kam.

6.2.3.1.2 Spruchwiederholung in anderen Schlüsseln, «reencodements». Spruchwiederholungen traten auf zwischen Werftschlüssel bzw. R.H.V. und ENIGMA-Schlüsseln, wobei das R.H.V. ab Ende 1943 kaum noch auftrat. Besonders ertragreich erwiesen sich hier die 2mal täglich abgegebenen Wettermeldungen im Bereich 7 (Trondheim).

Minenmeldungen bildeten ebenfalls eine reiche Quelle von Spruchwiederholungen zwischen Werftschlüssel und dem Schlüsselbereich der U-Boote in der Ostsee. Das wurde verschiedentlich ausgenutzt, Minen wurden dort gelegt, wo man sich möglichst gute Klartexte erwartete, wie z. B. KRIEGSANSTEUERUNGSTONNE SWINEMUENDE, was meist unverändert im ENIGMA-Spruch auftauchte.

Zwischen den Schlüsseln von Heer und Luftwaffe einerseits und Marine andererseits hat es wenig Spruchwiederholungen gegeben.

Sehr gute Klartexte konnten benutzt werden durch die vielen Sprüche, die, ursprünglich im Schlüssel M4, im M3 für die U-Boote in der Arktis, in der Ostsee und im Mittelmeer wiederholt wurden. Weiter waren hilfreich die Wettersprüche vom Hoek van Holland, die in Heimisch und anderen Schlüsseln fast ungeändert wiederholt wurden. Die Wettermeldungen von BEREICHDORA, ein Gebiet im Skagerrak und in der westlichen Ostsee, wurden zwar vor dem Wiederchiffrieren z.B. für Heimisch in der inneren Reihenfolge vermischt und in zwei Sprüchen getrennt verschieden gemischt gesendet. Da aber die ursprünglichen Sprüche immer die gleiche Reihenfolge einhielten, Wind, Bewölkung, Sicht und See, war es möglich, in der Neuchiffrierung die ursprüngliche Ordnung wiederherzustellen.

Zwei weitere typische Fälle waren die BELEHRUNGSFUNKSPRUECHE für U-Boote in der Ostsee auf Übungsfahrt; hier war der Inhalt oft unverändert geblieben.

In Heimisch gab es ein über lange Zeit brauchbares Spruchverhalten: Es waren Feststellungen, in welchen Gebieten vor Nord-Norwegen U-Boot-Bekämpfungsmassnahmen für die nächsten 24 Stunden erlaubt waren. Sie gaben darüber hinaus Hinweise auf Bewegungen der deutschen U-Boote in diesem Bereich.

6.2.3.1.3 «HERIVEL-Tips». In der Zeit, als mit den Lochblättern Schlüssel gefunden werden konnten, wurde von HERIVEL eine Beobachtung gemacht, die sich in der folgenden Zeit als hilfreich herausstellen sollte.[68] Nach dem Einstellen der befohlenen Ringpositionen bei den in der Maschine befindlichen Walzen (oder, was sicher aus Bequemlichkeit auch vorkam, beim Einsetzen der Walzen nach dem Stellen der Ringe) waren die Ringstellungen in den Sichtfenstern sichtbar, bzw. dicht benachbarte Stellungen lagen oben. Diese wurden dann – wiederum aus Bequemlichkeit – manchmal als Grundstellung für die Chiffrierung des Spruchschlüssels benutzt. HERIVEL trug alle Grundstellungen, wie sie zeitlich nacheinander eintrafen, in ein quadratisches Schema ein mit den Positionen A ... Z der langsamen Walze als horizontale Koordinaten, den Positionen A ... Z der mittleren Walze als vertikale Koordinaten. Die so definierten Felder wurden mit den Positionen A ... Z der Eingangswalze belegt. Manchmal schälte

[68] WELCHMAN b), S.100

sich eine Konzentration von Eintragungen in einem engen Bereich heraus. Das führte zu dem Schluss, dass dort in der Nähe die Ringstellung des Tagesschlüssels zu finden sein könnte.
Bei den folgenden Grundstellungen war es wahrscheinlich, dass im Bereich der unterstrichenen acht Stellungen

```
HER, TLZ, JFX, APQ, GRJ, AOF, DLS, UEO, RKI, HSQ
VMF, ACY, HRK, ZSF, JWG, GTK, FTJ, SAH, JQP, FSX
HTI, GLP, YWB, FRI, XEJ, DBV, CTR, SVI, SDM, UZR
```

die Ringstellung liegen könnte.

T	J	K	I
S	X		Q
R	I	J	K
	F	G	H

F, G, H langsame Walze, T, S, R mittlere Walze, I, J, K ··· schnelle Walze. Die Anzahl der Versuche, den Spruchschlüssel zu finden, konnte so manchmal wesentlich verringert werden.

6.2.3.1.4 «Cillies». Die Ringstellung allein war aber noch nicht in der Lage, über den chiffrierten Spruchschlüssel den Zugang zum eigentlichen Spruchschlüssel zu öffnen: Die Steckerlage - es waren seit 1939 7 bis 10 Buchstabenpaare versteckert - war unbekannt. Die sehr genaue Buchführung über alle Präambeln der aufgefangenen Funksprüche und ihre Zuordnung zu den einzelnen Funknetzen mittels Rufzeichenvergleichs, Peilung, „Handschrift" der Funker u.a. sowie der Ergebnisse der Dechiffrierung, soweit sie erfolgreich gewesen war, führte zur Entdeckung eines weiteren Fehlers. (In der angelsächsischen Literatur wurde für diesen Fehler der Begriff «Cillies» geprägt.) Manche Funker machten ihn angeblich immer wieder, vor allem nach dem Beginn des Bewegungskrieges im Mai 1940. Er soll darin bestanden haben, dass die Grundstellung zur Chiffrierung des Spruchschlüssels und der Spruchschlüssel selbst (vielleicht unbewusst) aus Mustern der Tastatur gebildet wurden. (BLOCH bezweifelt die Häufigkeit und damit die Bedeutung dieses Fehlers.[69]) Als Beispiel sei ein dreiteiliger Spruch angenommen, dessen drei Präambeln die Gruppen

```
Q A Y          R H R
E D C          K W G
T G B          M W D
```

enthalten sollen.[70] Im allgemeinen hatten die verschiedenen Teile eines mehrteiligen Spruchs auch verschiedene Kenngruppen aus dem Tagesschlüssel. Diese zur Vergrösserung der Geheimhaltung gedachte Methode[71] führte aber dazu, dass die zusammengehörigen Kenngruppen eines Schlüsselbereichs zu erkennen waren, und somit die Funksprüche leicht nach solchen Bereichen sortiert werden konnten.

Weiter sei angenommen, dass noch weitere zu diesem Bereich gehörenden Sprüche vorlagen, z. B. mit den Präambelteilen

```
Q W E          M F W
Q A P          K L F
```

[69] BLOCH d), F 4
[70] Dieses Beispiel ist in Anlehnung an WELCHMAN b), S. 105 - 110 konstruiert.
[71] In „Schlüsselanleitung zur Chiffriermaschine Enigma, vom 13.1.1940" , H.Dv.g.14, Abschnitt IV, angeordnet.

Das Beispiel wird weitergeführt:

Walzenlage I, II, III; Ringstellung `G S K` (aus HERIVEL - Methode)

Von dem 3-teiligen Spruch und den zwei weiteren Sprüchen sind untereinander die Grundstellungen (bekannt) und die chiffrierten Spruchschlüssel (bekannt) angeordnet:

```
Q A Y    E D C    T G B    Q W E    Q A P
R H R    K W G    M D W    M F W    K L F
```

Dabei ist dieses Beispiel fortgeführt mit der (richtig) angenommenen Ringstellung `G S K`. (Die Walzenlage soll aus anderen Überlegungen heraus mit I, II, III als die wahrscheinlichste - und zufällig richtige - erkannt sein. Falls die Walzenlage nicht erkannt war, mussten alle 60 möglichen Fälle auf der zur Pseudo-ENIGMA umgerüsteten TypeX durchgespielt werden.) Die vermuteten Zusammenhänge lassen auf wahrscheinliche tatsächliche Spruchschlüssel

```
W S X    R F V    Z H N    A S D    O K L
```

schliessen.

Paarbildung (Klar - Geheim):

```
W — R;  S — H;  X — R;  R — K;  F — W;  V — G;  Z — M;  H — D;
N — W;  A — M;  S — F;  D — W;  O — K;  K — L;  L — F
```

Daraus ergibt sich — unter Ausnutzung der Reziprozität — eine Kettenbildung:

```
N — W — R — K — L — F     (Kette 1)
W — F — S — H —D          (Kette 2)
Z — M — A                 (Kette 3)
```

mit den Seitenketten

```
W — D;    R — X;    K — O
```

Schema für Kette 1: Die Zeilen zeigen die Ergebnisse der Chiffrierung ohne Stecker der jeweiligen Ketten - Buchstaben bei Ringstellung `GKS` und der links stehenden Grundstellung. Bei der Betrachtung der Spalten ergeben sich Widersprüche, die gewisse Spalten ausschliessen, z.B.: Der Klarbuchstabe `N` (erste Zeile), gesteckert mit `A` (erste Spalte) wird zu `W`, gesteckert mit `L`. Dieses aber wird zu `R`, gesteckert mit `N`: WIDERSPRUCH ! Ebenso findet man Widersprüche in den anderen Spalten, übrig bleibt nur die Spalte mit den Steckerungen `(N N)`, `(W S)`, `(R D)`, `(K T)`, `(L J)`, `(F A)`, `(X P)` und `(O Y)`. Ein entsprechendes Schema mit der Kette 2 liefert dazu noch das Steckerpaar `(H Z)`. Die versuchsweise Chiffrierung von `RFV` zu `KWG` liefert das Paar `(G U)`. Somit kennt man 9 Steckerpaare.[72]

***	A	B	C	D	E	F	G	H	I	J	K	L	M	*N*	O	P	Q	R	S	T	U	V	W	X	Y	Z	N
TGE	L	H	Z	Y	M	K	O	B	P	U	F	A	E	*S*	G	I	W	V	N	X	J	R	Q	T	D	C	W
QAZ	N	X	M	U	Z	C	R	E	J	Y	Q	G	B	*D*	A	V	T	I	L	H	P	O	F	W	S	K	R
EDD	Z	P	B	G	N	F	J	A	R	H	W	U	M	*T*	E	L	D	K	V	Y	X	S	C	Q	O	I	K
QAR	U	F	O	X	A	P	T	N	E	W	H	Z	Q	*J*	R	S	C	I	Y	V	G	L	D	M	B	K	L
QAS	C	P	G	Q	J	F	H	K	I	Y	T	V	X	*A*	M	B	U	E	W	Z	O	D	L	R	S	N	F
***	N	X	M	U	Z	C	R	E	J	Y	Q	G	B	*D*	A	V	T	I	L	H	P	O	F	W	S	K	R
QAB	Y	H	K	Q	R	L	Z	W	A	N	U	O	I	*P*	J	F	S	B	C	X	D	G	V	E	T	M	X
***	Z	P	B	G	N	F	J	A	R	H	W	U	M	*T*	E	L	D	K	V	Y	X	S	C	Q	O	I	K
QAQ	S	K	Q	C	X	V	O	U	L	W	H	A	E	*Y*	M	R	I	P	F	T	N	Z	G	B	J	D	O

Es soll den weiteren fatalen Fehler gegeben haben, für den Spruchschlüssel dieselbe Buchstabengruppe zu wählen wie für die Grundstellung zur Chiffrierung des Spruchschlüssels. Der Verdacht auf solche Zusammenhänge trat auf, wenn bei mehrteiligen Sprüchen z.B. die genannten Grundstellungen lauteten: (Tastaturmuster !)

[72] DEAVOURS/KRUH a), S. 123 ff.

`Q A Y, W S X, E D C`

Verschiedentlich wurden bei fortgesetzten Sprüchen Fehler gemacht, die auch bei Quittierungen von Sprüchen aufgedeckt werden konnten.[73]

Angenommen, die Präambeln von zwei Sprüchen seien

`1725/157/HQRIPT` und `1810/201/QCANPT`

weiter werde angenommen (diese Annahmen trafen auf das Verhalten mancher Funker zu, das war bekannt), der Funker habe als Anfangsstellung für den zweiten Spruch die Endstellung des ersten genommen, dann wäre diese Endstellung des ersten Spruches (152 Stellen zurückgerechnet) u.U. `Q W E`. Dies wäre aber eine Struktur vom Tastenfeld, also wahrscheinlich. Hieraus folgt, dass `Q W E`, chiffriert mit der Einstellung `H Q R` das Ergebnis `I P T` haben musste. Damit waren wesentliche Daten für die Ermittlung des Tagesschlüssels geliefert. Zudem brachten diese kombinierten groben Fehler für einige Teilsprüche bereits kurze Klarabschnitte (die chiffrierten Textschlüssel).

Dabei konnte wegen der unterschiedlichen Positionen der Nuten in den Sperrscheiben der Walzen I bis V oft die Walzenlage bereits ermittelt werden.[74]

Manchmal wurde auch von der Endstellung des ersten Spruches die rechte Walze um ein oder zwei Positionen verdreht, auch diese Fehler konnten von aufmerksamen Kryptologen aufgedeckt werden.

In vielen Fällen wurden die Rotoren beim Einstellen der Ringe für den ersten Spruch eines Tages nicht aus der Maschine genommen, sondern die Ringe wurden in der Maschine selbst fixiert. Danach wurden die Walzen in ihrer Stellung belassen und die sichtbaren Buchstaben als erster Indikator des Tages genommen. Bei mehreren solchen Fehlern innerhalb eines Funknetzes war es möglich, auf die Ringstellung des Tages zu schliessen.(Ringstellung–«givaway»)

Die Ausnutzung dieser Chiffrierfehler (und anderer) half BP als wichtigste Methode bis Mitte September 1940, als die erste kryptologische «Bombe» zur Verfügung stand. Damit wurden immer wieder die Tagesschlüssel von «Red» gefunden und damit grosse Teile des Funkverkehrs gelesen. Erst ab Mitte 1943 traten Cillies seltener auf.

6.2.3.1.5 «Psillies». Hier handelte es sich um eine Art psyologische Cillies. Wenn z.B. in der Präambel `R O M X L V` zu finden war, dann lag es nahe, dass der Funker als frei gewählte Gruppe `M E L` gewählt hatte, oder bei `T O B K S T` die Gruppe `R U K`. Auch hier wurden mit einem Fehler der Textschlüssel und ein Klartext-Geheimtext-Paar offengelegt[75].

6.2.3.1.6 Banburismus. In den Berichten über BP taucht immer wieder der Begriff Banburismus auf. Geprägt wurde er in Hut 8, weil für ein Verfahren zur näheren Bestimmung der Eingangswalze der ENIGMA M (und der Stecker) ab Mai 1941 Lochblätter verwendet wurden, die in der kleinen Stadt Banbury gefertigt worden waren.

Sie enthielten parallel angeordnete von oben nach unten laufende Alphabete A...Z. Die jeweiligen Bögen besassen horizontal so viele Spalten, wie die zu bearbeitenden Sprüche lang waren (u.U. bis zu 200). In diese Bögen wurden die jeweiligen Sprüche eingelocht, die aufeinander folgenden Buchstaben in aufeinander folgende Spalten. Wenn die Bögen verschiedener Sprüche übereinandergelegt werden, zeigten sich gleiche Buchstaben an gleichen Stellen bei durchscheinendem Licht. Wenn man die Bögen

[73] Das folgende Beispiel ist aus NARA Dokument Box CBTE28, No.3620 «Report on 'E' Operations of the GC&CS at Bletchley Park, 'Cryptanalysis of German Army & German Air Force ENIGMA Traffic'», S. 28

[74] SMITH/ERSKINE, S. 453 - 456. Dort ausführliches Beispiel.

[75] Wie Fussnote 68, S. 32

schrittweise relativ zueinander nach rechts oder nach links verschob, erhielt man Aussagen über mögliche Unterschiede der Anfangspositionen der Sprüche beim Chiffrieren. Nötig war, dass man die Häufigkeit der Koinzidenzen bezüglich der Sprache prüfte. Dabei wurde ein Bewertungssystem benutzt, das unterscheiden liess zwischen z.B. dem Auftreten von vier getrennten gemeinsamen Buchstaben und einem Tetragramm usw. Die zweite Bedeutung des Begriffs bezieht sich auf die Auswertung der mit den «Banburies» erhaltenen Aussagen über vergleichbare Sprüche, um damit die möglichen Abstände der chiffrierten Textschlüssel zu finden und über den Ausschluss von Widersprüchen möglicherweise die benutzten Chiffrierwalzen zu identifizieren.
Dieses Verfahren war eine Weiterführung der polnischen Uhrenmethode[76]. Voraussetzung war allerdings die zumindest teilweise Kenntnis der Tauschtafeln der Marine für Bigramme. Nach GOOD[77] reichten oft 20 Sprüche eines Tages aus, die verwendete Tauschtafel zu bestimmen. Dazu kamen Erfahrungen, dass die bei der Kenngruppen-Chiffrierung gebrauchten Füllbuchstaben nicht immer zufallsgerecht gewählt wurden. Wenn es also möglich war, in die Kenngruppen-Chiffrierung einzubrechen, blieb der eigentliche Spruchschlüssel noch verborgen, weil er aus der Verfahrenkenngruppe durch ENIGMA-Chiffrierung nach einem unbekannten Tagesschlüssel (Walzenlage, Ringstellung, Grundstellung, Steckerlage) entstanden war. Wenn aber bei den Sprüchen eines Tages Verfahrenkenngruppen entdeckt wurden, die sich nur in ihren dritten Buchstaben unterschieden, dann konnten sich die dazugehörigen Spruchschlüssel ebenfalls nur in ihren dritten Buchstaben unterscheiden. D.h. solche Sprüche hatten bei der Chiffrierung dieselben Ausgangsstellungen der linken und der mittleren Walze gehabt. Die Unterschiede lagen allein in den Anfangsstellungen der Eingangswalze.

Die eingegangenen Sprüche wurden sowohl auf Hollerith-Karten als auch auf die genannten Lochblätter aus Banbury ausgestanzt. Die Verschiebung zeigte an, um wieviele Schritte die Anfangsstellungen der Chiffriermaschinen bei beiden Sprüchen auseinander gelegen hatten. Man war also in der Lage, Gleichungen aufzustellen, wie z.B.

$$klar(N) = klar(C) + 4$$

wenn ein Spruch mit chiffrierter Lage der Eingangswalze C bei Verschiebung um $+4$ gegenüber einem Spruch mit entsprechender Lage N ein gültiges Maximum von Koinzidenzen zeigte. Diese Aussage hiess, dass in einer Zuordnungstafel für die Eingangswalze und auch die Stecker der Geheimbuchstaben N und C um 4 Stellen auseinander lagen. Andere Spruchpaare lieferten u.U. weitere solche Gleichungen, sodass sich im günstigen Falle grosse Teile der Zuordungstafel rekonstruieren liessen. Die Reziprozität , die die Tafel zeigen musste, war dabei eine wesentliche Hilfe.[78] Banburismus wurde mit dem Ziel gebraucht, die Alphabete 2 und 3, also die der mittleren und der linken Walze zu finden.
Als erstes mussten die passenden Spruchpaare aus der Menge aller Sprüche heraussortiert werden, die dann mit den Banbury-Blättern auf ihre Phasenverschiebung hin untersucht wurden. Passend waren sie, wenn sie sich nur in einem Buchstaben in der dritten Stelle unterschieden. Voraussetzung für diese Methode war der gravierende Fehler im System, dass alle Spüche zweier Tage mit derselben Grundeinstellung chiffriert waren[79]. Ein Beispiel soll das Vorgehen erläutern:[80]
Es entstanden Listen wie z.B.

A Y R	+	6.5	=	A R X	Octogramm *certain*
I U S	+	3.3	=	I U Y	Hexagramm 20:1
E N F	+	3.7	=	E P Q	Pentagramm 17:1
R W C	+	0.13	=	R W L	Tetragramm 4:1

[76]Vgl. RÓŻYCKI, Ende von Kap. 4.2.1
[77]GOOD, in HINSLEY/STRIPP, S. 157
[78]Ein Beispiel gibt BAUER, Kap. 19.6.4.3
[79]ALEXANDER, S. 9, Abschnitt 33
[80]ALEXANDER, S. 99; MAHON, S. 18

Dabei bedeutete + 6.5, dass der erste Spruch um 6 ganze Alphabete und 5 Buchstaben gegenüber dem zweiten versetzt war. Die Aussagen 20:1 usw. betrafen das Mass der Richtigkeit der Aussage.

6.2.3.1.7 ban. Für die Unterscheidung zwischen zufälligen Koinzidenzen und nicht-zufälligen, generell für die Gewichtung von Aussagen von Experimenten, vermuteten Walzenlagen, vermuteten Ringstellungen usw., hatte TURING ein mathematisches Instrument entwickelt. Offenbar hat er dabei nicht die Methoden der Bestimmung des «weight of evidence» von PIERCE[81] und die Arbeiten von FISHER über Statistik[82] gekannt.[83] Ausgehend von Grundsätzen über bedingte Wahrscheinlichkeiten (Satz von BAYES) schätzte er das statistische Gewicht eines vorliegenden Ergebnisses ab, das er i.a. in Wettquoten bzgl. der gesetzten Hypothese ausdrückte (z.B. 12:5). Er fand, wie PIERCE, dass statt der Wettquoten daraus abgeleitete Logarithmen addiert werden sollten. Weiter entwickelte er ein Masssystem, in dem er die Einheit 1 ban einführte, die Bewertung eines Ereignisses, das die Richtigkeit einer gesetzten Hypothese 10mal wahrscheinlicher werden liess. (Entsprechend wurde der 10. Teil ein deciban - db - genannt. Man beachte die logarithmische Skala wie beim Dezibel.) Auf diese Weise wurden Abschätzungen gewissermassen mechanisch möglich und konnten - in anderen Formularen - durch einfache Addition bzw. Subtraktion ausgewertet werden. Jeder Gleichung aus Koinzidenzen wie der obigen wurde sofort eine Bewertung in db beigegeben. Das ganze Verfahren war also eine Art «sequential analysis», bei der ein Zielverhältnis (Hypothese) vorgegeben war und die Ausgänge von Experimenten so lange addiert bzw. subtrahiert wurden, bis das Zielverhältnis erreicht war oder aber die Hypothese als äusserst unwahrscheinlich verworfen werden musste. Der mathematische (und philosophische) Hintergrund ist bei GOOD dargestellt.[84]

Ein Teil der Paare

```
B B C  +  .2   =  B B E
E N F  +  3.7  =  E P Q
R W C  +  .13  =  R W L
P N X  +  .5   =  P I C
I U S  +  3.3  =  I U Y
Z D R  +  5.5  =  Z I X
```

führte zu einer Darstellung als Kette

```
R....X....C.E..........L
```

Diese Buchstaben mussten mit diesen gegenseitigen Abständen im Alphabet der rechten Walze auftreten. Um die richtige Zuordnung zum Alphabet zu bekommen, wurde die Kette am Alphabet entlanggeführt. Widersprüche führten zum Ausschluss der jeweiligen Stellung. Dabei wurde mit eingerechnet, dass zu r$\mapsto$ A gehört a$\mapsto$ R.
Die erste Position

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
R . K . M X . . . . C X E . . . . A . . . . . L . .
. . . . . . . . . . . . . . . . . . . . . . . F . .
```

führte bereits zum Widerspruch, weil zu x sowohl L als auch F zugeordnet sein müsste. Weiter widersprüchliche Stellungen sind

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
. . S . U L . . R . . F . X . . . I C . E . . N . .
. . D C F E . . . . . Q . . . . L T . . . R . A . .
```

[81] PIERCE, 1878 bzw. 1923
[82] FISHER
[83] HODGES, S. 197
[84] GOOD b), GOOD c)

Eine gute Stellung ergibt sich für

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
. . D C F E . . . . . Q . . . . L . . R . . . Y X .
```

wo die weiteren Paare F + 7 = Q, S + 3 = Y, D + 16 = U gut untergebracht werden können. Weiter passt das Paar D + 16 = U in das Schema.
Das Paar R W C + 13 = R W L zeigt, dass zwischen C und L die mittlere Walze nicht weiterrückte. Da die Schaltpositionen der Walzen II, IV, VI, VII und VIII zwischen d und q liegen, sind diese Walzen als rechte Walzen bereits auszuschliessen. Das Paar P N X + 5 = P I C lässt auf eine Weiterschaltung der mittleren Walze zwischen X und C schliessen. dazwischen liegen die Schaltpositionen der Walzen V, VI, VII und VIII. Daraus folgt: die rechte Walze ist Walze V.

Mit weiteren Paaren lässt sich die gesamte Zusammenhang der Walze V zum Alphabet bestimmen. Bei der Entscheidung, um welche Walze es sich handelt, halfen auch der Walzenlage, dass Steckerpaare nie zueinander benachbarte Buchstaben enthielten u.a.m.

Mit einem ähnlichen Verfahren konnte man die Alphabet-Zuordnung für die mittlere Walze bestimmen.

Das Ziel war, die Anzahl der möglichen Walzenkombinationen so weit zu verringern, dass die weiter Bearbeitung mit der «Bombe» erleichtert wurde (von 336 auf sehr viel weniger, im günstigsten Fall auf 3). Als etwa 1943 genügend Bombenkapazität, auch der schnelleren Typen, zur Verfügung stand, wurde das Banbury-Verfahren eingestellt.

An diesem Beispiel wird sehr deutlich, dass es ein grosser Fehler war, die Walzen I bis V mit verschiedenen Schaltstellen zu versehen.

6.2.3.1.8 EINS-Katalog. Die von TURING schon 1939 festgestellte Tatsache, dass etwa 90% aller Sprüche der Marine wenigstens einmal das Tetragramm /eins/ enthielten, wurde über Vergleichskataloge ausgenutzt. Für die Walzenlage eines Tages und die Stecker des Tages wurden die Ergebnisse des Chiffrierens der Gruppe /eins/ für alle 17576[85] Anfangsstellungen in Kataloge aufgenommen. Jedes Tetragramm des Spruches dann auf Übereinstimmungen mit Eintragungen in dem entsprechenden Katalog geprüft. Mit Hollerith-Maschinen wurde dieser Vergleich recht schnell möglich. Wenn die Bigrammtafeln bekannt waren und genügend viele Sprüche mit dieser Methode bearbeitet waren, liess sich aus der Tafel die offene Verfahrengruppe finden, /eins/ führte zum tatsächlichen Textschlüssel. Mehrere solche Klartext-Geheimtext-Paare führten zu einem Menu für die «Bombe», womit die Grundstellung gefunden werden konnte[86].

Wenn eine übereinstimmende Stelle gefunden war, musste versuchsweise von der gefundenen Walzenposition weitergearbeitet werden. In etwa 25% der Fälle führte dies zur Ermittlung des Spruchschlüssels.

Es war nötig, auf diesem Wege möglichst viele Sprüche zu erkennen, um Aussagen über die Häufigkeit von Klartextstücken und Steckermethoden zu erhalten.

6.2.3.1.9 «Rodding». Die erste Methode, die ENIGMA-Sprüche in BP anzugehen, war die mit den charakteristischen Streifen, daher «Rodding» genannt.[87] Damit sollten die rechte Chiffrierwalze und ihre Anfangsstellung identifiziert werden.

Für einen Spruch ohne Verwendung von Steckern (wie z.B. im spanischen Bürgerkrieg) ist das Verfahren dem Prinzip nach bereits in Kap. 3.2 gezeigt. Es bekam besondere Bedeutung beim Bearbeiten von Sprüchen, die mit der Reichsbahn-Enigma chiffriert

[85] verschiedene Autoren sprechen von 105000
[86] BUDIANSKI, S. 346
[87] TURING's «Treatise on Enigma» und Tony SALE im Internet «Virtual Wartime Bletchley Park»

waren: Diese Maschine hatte ebenfalls keine Stecker. Ein Beispiel in Tabelle 6.1 soll das Verfahren zeigen (Zur Information: Walzenlage I III II, Ringstellung `ZZZ`, Anfangsstellung `AAH`, Verwendung von Tabelle A.4 im Anhang). Man musste mit den verschiedenen Walzen I, II, usw. und dabei für die verschiedenen Anfangsstellungen in den «rod-squares» des Kap. 2.1 die Zeilenpositionen für die Klar-Geheimtext-Paare feststellen und sehen, ob für weitere Anfangsstellungen (Verschiebung nach rechts) weitere Klar-Geheimtextpaare in denselben Zeilen zu finden wären.

```
V A U G S O Q A T G R G E H M E K Y N Q   Geheimtext
F E S T U N G V O N M E L D E K O P F K   Klartext
i j k l m n o p q r s t u v w x y z a b   Walzenstellung

F Y N B W I E L T Y K G C W P I D E K N   l
V B E I M H C R O W P E S N Z V C K P B   c
* . . . . . . . * . . * . . . . . . . .

W E X M A V H D K S X J F B V O H C D J   k
S A F R N J D W P K L R U Y C X S H E M   s
. * . . . . . . . . . . . . . . . . . .

B G S O K E X Q L M S V Z D Y T I F N G   t
I X U C V K Y T F B I Q V H D Z T M F A   i
. . * . . . . . . . . . . * . . . . * .

M H W T B U J X S E A H P U G C Y S L E   h
U Q M G Z S N O U X B F A V K H P I X L   v
. . . * . . . . . . . . . . . . . . . .

L P K F U R Z S H V Q C Y F N S E A W Q   f
Q L G V S A T I W R D Z G O T F B X R K   g
. . . . * . . . . . . . . . . . . . . *

P D Y K G N V A M I E Y R K F G M P T X   n
R N H A T O P V Y C G B W L I Q J Y M H   w
. . . . . * . * . . . . . . . . . * . .

T U A D H L G B Q N V O D R M Y U B J O   b
G K O J E T Q Y R G U P B X E M R D Z V   e
. . . . . . * . . * . . . . * . . . . .

X S T Z C G K F A P M U N C Q L X T A I   a
Y V D W L Z U G C J R W I E A U N G B C   j
. . . . . . . . . . * . . . . . . . . .

E Z L H O W B N J F Z S L G H N Q U Y T   o
H T P L F Y R M N T W A E Z U J G O H W   u
. . . . . . . . . . . . * . . . . . . .

O I B U P Q W Z D H C X M J R K Z N I U   x
Z O C X J F M U Z L H D X Q J E F L O S   m
. . . . . . . . . . . . . . . * . . . .

J C V Q R X A E I D Y N K S L A O J V R   y
D W R S Y B F J E Z O L T M B P K W S Z   z
. . . . . . . . . . . . . . . . * . . .
```

Tabelle 6.1:

Die rechte Spalte zeigt die verwendeten Zeilen, zugleich eine Zugriffsmöglichkeit zur mittleren Chiffrierwalze. Hier greift der Satz bei Tabelle 2.1 in Kap. 2.1. Bei falscher Walze oder falscher Walzenposition ist keine Häufung zu bemerken. Im Beispiel mit der richtigen Walze II und der richtigen Anfangsstellung i sieht man die Häufungen in einzelnen Zeilen. Diese Zeilenpositionen geben Ein- und Ausgang für die mittlere Walze an (die im entsprechenden Walzenquadrat in einer Spalte liegen mussten, solange die mittlere Walze nicht rückte). Die „Koppelung“ von Paaren der Zeilenpositionen half natürlich auch beim EDechiffrieren eines Spruches.

6.2.3.1.10 SKO, «Stecker Knock Out», «DUENNA». In BP wurde eine Technik entwickelt, die erste Walze samt ihrer Anfangsstellung zu identifitzieren und gleichzeitig die Stecker und die Verbindungen der Umkehrwalze zu bestimmen. Dies war mötig, wenn die Umkehrwalze Dora verwendet worden war. In manchen Fällen war allerdings die erste Walze bereits bekannt.

Ausgangspunkt war die Annahme, welche Walze als schnelle Walze verwendet würde. Aus weiteren Annahmen über verwendete Steckerverbindungen liessen sich mit Hilfe von Streifen (Kap. 2.1) die weilige durch die Steckeranlagen begründeten Ausgänge von (Stecker + schnelle Walze) gewinnen. Evtl. auftretende Widersprüche führten dann zum Verwerfen der gemachten Annahmen und begründeten deren Änderung.

Günstig erwiesen sich Stellen im Gefüge Klartext-Geheimtext, wo in geringem Abstand gleiche Klar–Buchstaben aufeinander folgten («Beetle»), was für die Positionierung entsprechender Streifen hilfreich war, oder auch die Nähe gleicher Klartext–Geheimtext–Buchstaben («Starfish») bzw. auch das Auftreten von «females».[88]
Die so gewonnenen widerspruchsfreien Ausgänge waren gleichzeitig die Eingangspaarungen für die aus mittlerer Walze, langsamer Walze und Umkehrwalze gebildeten virtuellen Umkehrwalze, deren weiter Analyse mit weiteren Annahmen begonnen werden konnte.

Wenn die richtigen Positionen der beiden rechten Walzen bereits bekannt waren, konnten die Stecker und die Umkehrwalzen-Verbindungen mittels vorgefertigter Lisen, in denen zu den jeweiligen Stellungen mehrfach aufgetretener Klar-Geheim-Paare die verschiednenen Walzenkombinationen mit ihren Ein- und Ausgängen katalogisiert waren, Stecker und die Komplexe (linke Walze + Umkehrwalze) auf widerspruchsfreie Möglichkeiten durchgetestet werden. Dieses Verfahren wurde DUENNA genannt, auch später automatisiert.

Beispiel: (Erste Spalte: häufige Klar-Geheim-Gruppe, zweite Spalte: (einige) Kombinationen der beiden rechten Walzen, die anderen Spalten zeigen die Ausgänge aus diesen Kombinationen beim darüber bezeichneten Eingang.)

**	**	A	B	C	D	E	F	G	H	I	J	K	L
EN	BS	R	T	Q	U	F	N	A	E	L	V	W	X
EN	FI	S	J	N	U	R	X	D	B	E	A	W	M
EN	NA	N	A	X	R	S	Q	L	V	Y	T	J	Q
EN	MQ	A	V	S	D	E	L	R	J	M	F	Q	C
EU	KJ	R	S	K	A	B	G	E	O	Q	J	Y	V
EU	NY	M	B	E	F	U	C	V	W	A	N	S	L
MR	MR	L	V	K	N	G	H	Z	Y	X	J	T	B

Angenommen, `E` sei mit `a` gesteckert, `N` mit `b`. Dann müssen die Spalten A und B als Ausgänge auf mögliche Widersprüche hin untersucht werden. Hier zeigen die Zeilen 3 und 4 den Widerspruch `N/A` und `A/V`. Die Annahme musste also verworfen werden. Die Annahme `E/a` und `N/g` führte hier zu den Ausgängen `R/A, S/D, N/L, A/R, R/A, M/F` und `L/N`. Hier waren nicht Widersprüche, sondern mehrfache Bestätigungen zu finden, was ein Weiterarbeiten mit diesen Annahmen rechtfertigte und als nächste Kombination `U/d` nahelegte.

[88] MARKS b), Part II, S. 188 ff.

Der Nachteil dieser Methode: Für jede Konfiguration waren 520 Listen zu erstellen, die dann genau abgeglichen werden mussten. «beetle» - und «starfish» - Möglichkeiten konnten hier den Zeitaufwand erheblich herabsetzen. (Mit 500 Mitarbeiterstunden waren die Chancen auf einen Erfolg etwa 30 %.)

Die Entwicklung einer Automatisierung der Methode führte zur DUENNA Mark I, später auch Mark II. [89]

Am Beispiel in Anlehnung an MARKS [90]:
Gegeben die Klar - Geheimpaare

```
lopau lklam
CZJBA WLHGL
```

Nach der Steckerbestimmung zu

```
A/I, C/N, D/L, E/V, F/X, G/X, H/S, J/T, M/Y, O/Z
```

lieferte die Streifenmethode für die Eingänge jeweils als Geheimbuchstaben bzw. Klarbuchstaben nach dem Durchgang durch die drei Chiffrierwalzen die Paarungen

```
P/F, A/X, T/Z, D/R, Y/S, U/L, F/P, N/G, R/D, A/X
```

was in der Tat nach Fussnote 9 in MARKS sieben der zwölf in der Umkehrwalze gesteckerten Paarungen ergab.[91].

Wenn die Stecker (aus «SKO» o. ähnlichen Methoden) bekannt waren, konnte mit Hilfe der Streifen die Lagen und die Stellungen der Walzen bestimmt werden und so über sog. «Halfbombes» die Steckerung der UD gefunden werden. Allerdings war, solange die Maschine DUENNA noch nicht zur Verfügung stand (vor November 1944) das Verfahren ausserordentlich aufwendig. 400 Personen waren in vier Schichten eingesetzt, 32 «Bombes» mussten aus dem Betrieb genommen werden, um genügend Personal an das Problem der UD zu setzen.

Die DUENNA selbst prüfte eine Walzenfolge in etwa 90 Minuten.[92] In BP wurde eine Maschine aus vier «Bombes» zusammengesetzt («Giant»), aber das brachte keinen Erfolg. In den USA wurde im Dezember 1944 der sog. «Autoscritcher», eine langsame elektro–mechanische Maschine, die nur vier von 24 Problemen löste, das erste am 6.3.1945.

6.2.3.1.11 «Bombe» Sobald die Verdrahtungen der Walzen bekannt waren, wurden in BP einige TypeX Maschinen modifiziert, sodass sie als Pseudo-ENIGMAs wirkten und zur Herstellung von Lochblättern benutzt werden konnten.

Es steht ohne Zweifel fest, dass ohne die polnische Vorleistung, u.a. die Lieferung von Walze I bis V an die Briten, die weitere Entwicklung in BP viel länger gedauert hätte. Erst aus U 33 gelangten die Briten im Februar 1940 in den Besitz von Walze VI und VII. HINSLEY behauptet, die Existenz der Walze VIII sei damals noch unbekannt gewesen.[93] Im August 1940 sei sie aber auf See erbeutet worden. Demgegenüber schreibt SKILLEN, die Existenz der Walze VIII sei durch Befragung der Überlebenden von U 33 bekannt geworden. Die Beute aus U 110 am 9.5.1941 hätte auch aus einer ENIGMA mit dem kompletten Satz von acht Walzen bestanden.[94] (Kap. 6.2.3.3.1, S. 168)
Die Verdrahtungen der „Marinewalzen“ sind bereits in Kap. 1.1 dargestellt.

[89] Die erstere ist beschrieben in NARA Dokument «Report Proposed Design for DUENNA MARK ONE, 25 February 1944 - OP-20-GMF»

[90] S. 181 in Part II

[91] Walzenlage: `III, II, I`, Ringstellung: `EVP`, Grundstellung: `INS`

[92] SMITH/ERSKINE

[93] HINSLEY III/2, App. 30, S. 957

[94] SKILLEN a), S. 89

Es hatte nach PYRY weiter Kontakte gegeben zwischen den polnischen Kryptologen REJEWSKI, ZYGALSKI und RÓŻYCKI in BRUNO und KNOX und TURING in England.[95] TURING plante, die polnische BOMBA weiterzuentwickeln: Eine Batterie von Vertauschern («scrambler»), die synchron alle möglichen Stellungen durchlaufen sollten, um den vorliegenden Geheimtext mit dem in der jeweiligen momentanen Stellung chiffrierten Klartextstück zu vergleichen («simultaneous scanning»). Notwendig war auf alle Fälle ein Klartext zum Geheimtext. Ein Durchlaufen aller Vertauscherpositionen mit dem Geheimtext allein war nicht sinnvoll, weil die Anzahl der Buchstaben eines Spruches für eine aussagekräftige Statistik nicht ausreichte.[96] Bei diesem ersten gedanklichen Entwurf handelte es sich um einen direkten Angriff («brute force attack»), dem deutscherseits wegen der Vielzahl von Chiffriermöglichkeiten keine Chance eingeräumt worden war. Überlegungen in dieser Richtung lagen bei BP nahe, weil nicht mit der Fortdauer der doppelten Chiffrierung des Spruchschlüssels und somit mit dem Auftreten von «females» gerechnet werden konnte.

TURING wich von der polnischen Version ab, den Stromweg nach der Umkehrwalze wieder in denselben Walzen zurückzuführen. Er entwickelte einen «double-ended-scrambler», also einen Vertauscher, der – bildlich gesprochen – aus zwei gleichen Sätzen von Chiffrierwalzen und der Umkehrwalze bestand. Der Stromweg lief durch den ersten Satz, die Umkehrwalze, von dort durch den zweiten Satz. Wesentlich dabei war, dass auf diese Weise zwei Eingänge/Ausgänge zum Vertauscher entstanden, anstatt wie bei der ENIGMA und bei der polnischen BOMBA ein Eingang und „am anderen Ende“ ein Registriergerät (Lampe oder Relais).

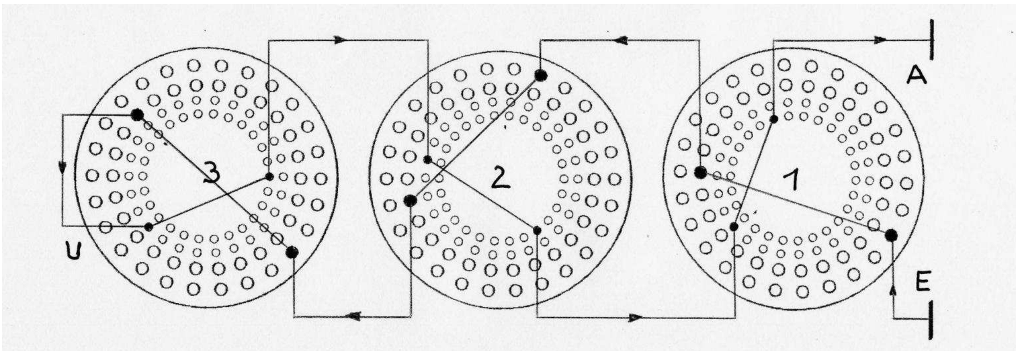


Abbildung 6.1: TURING-Vertauscher

In der konstruktiven Ausformung wurden die Vertauscher in einem Haltegestell auf Treibachsen gesteckt, die die einzelnen den Chiffrierwalzen entsprechenden Trommeln rehten, die oberste am schnellsten (Abbild der langsamen Walze), nach einem Umlauf wurde die darunter angebrachte mittlere Trommel um 1/26 ihres Umfangs weitergedreht, nach einem vollen Umlauf der mittleren Trommel die untere um 1/26 ihres Umfangs[97]. Jede Trommel hatte an der Rückseite vier konzentrische Kreise von je 26 Kontakten, die von entsprechenden Kreisen von Kontaktbürsten am Gestell abgegriffen werden konnten. Innerhalb jeder Trommel waren die zwei äusseren Kontaktsätze wie die Verdrahtung einer ENIGMA-Walze miteinander verbunden, ebenso die zwei inneren Kontaktsätze. Eine Halteplatte stellte schliesslich die Verbindung zwischen den

[95]KAPERA, S. 23
[96]DEAVOURS/KRUH b), S.331
[97]WHITEHEAD schreibt, dass das Weiterschalten der zweiten Trommel nach eineinhalb Umdrehungen der ersten erfolgte.

Trommeln her. Ausserdem war an der Rückseite die Verdrahtung der Umkehrwalze fest geschaltet.

Der Stromweg führte von `E` zu einem Kontakt der obersten Trommel 1 (äusserste Reihe) in dieser innen, entsprechend der Verdrahtung einer Chiffrierwalze, zu einem Kontakt der zweiten Reihe, von dort über die Halteplatte zu einem Kontakt der äussersten Reihe der mittleren Trommel 2, weiter entsprechend zur unteren Trommel 3, von dort zur rückseitigen Umkehrwalzen-Verdrahtung `U`. Diese war dann verbunden mit dem dritten Kontaktsatz der untersten Trommel, in dieser mit dem Kontaktsatz des vierten Kontaktkreises.[98] Über die Halteplatte lief die Verbindung weiter zu den inneren Kontaktsätzen der mittleren Trommel usw., bis schliesslich das Ende des Stromweges `A` bei einem Kontakt des innersten Kreises der obersten Trommel lag.
Der Eingang lief über ein 26-adriges Kabel an den äusseren Kontaktring der obersten Trommel, der Ausgang ebenfalls über ein 26-adriges Kabel vom inneren Kontaktring dieser Trommel. Aus der Reziprozität der ENIGMA folgte, dass Eingang und Ausgang vertauschbar waren.

In einem Gestell waren anfangs 10 solcher Halteplatten nebeneinander montiert, später 12. Bei JOHNSON[99] enthält ein Gestell sogar $2 \cdot 12$ Halteplatten. Man kann davon ausgehen, dass aus Klartext und Geheimtext bis zu 12 Buchstabenpaare verwendet worden sind. Sehr viel längere Klartexte waren nicht praktikabel, weil dann keine Rücksicht auf die durch die Eingangswalze bzw. die mittlere Walze induzierte Weiterschaltung der Nachbarwalze genommen werden konnte.

Das 26-adrige Ausgangskabel konnte mit seinem anderen Ende an den Eingang eines anderen Vertauschers gelegt sein oder an eine Registerschaltung.

Menu Vor der Inbetriebnahme musste das sog. Menu geschaltet werden:
Über einen ausgewählten Knoten als Eingang (möglichst einen, der mehreren Schleifen angehörte) wurde mit einem 26-adrigen Kabel ein Register an die Schleife angekoppelt. Das Register gestattete einmal, Spannung an eine der 26 Leitungen zu legen (entsprechend dem für diesen Knoten gewählten Steckerbuchstaben) und in die Schleife einzuspeisen, zum anderen zeigte diese Einheit an, wenn am Eingangsknoten als Ausgang der Vertauscherkette an der Leitung eines anderen Steckerbuchstabens Spannung anlag, die dann wiederum eingespeist wurde. Die Registrierung erfolgte über Relais. Logische Schaltungen ermöglichten, die beiden Zielzustände

1) Spannung nur am Eingangsknoten;
2) Spannung an allen Leitungen ausser einer einzigen

zu erkennen und die Apparatur zu stoppen. Da die oberste Trommel sehr schnell rotierte, war das Abstoppen ein Problem. Eine Quelle nennt als Umdrehungszahl der obersten Trommel 1800 U/min[100], sodass für das Durchlaufen einer Walzenlage etwa 12 Minuten nötig gewesen wären. Andere Quellen sprechen von 60 U/min, bei späteren wurden bis zu 3000 U/min versucht, wobei Schwierigkeiten mit den Kontakten auftraten[101]. Für das Schalten eines Menus mussten 35 bis 50 Minuten gerechenet werden, für die Änderung der Walzenlagen etwa 10 Minuten. Wenn das Menu nicht mehr als 12 Elemente enthielt, konnten drei Walzenlagen gleichzeitig getestet werden.

Da die manuelle Änderung des Menus bei geänderter Walzenlage auch einige Minuten in Anspruch genommen hat, wären diese Zeitangaben kompatibel mit der Aussage, dass für ein vollständiges Austesten aller 60 Walzenlagen etwas mehr als 12 bis 15 Stunden

[98] Es kann auch sein, dass die Reihenfolge dritter/vierter Kontaktkreis vertauscht war. Die Quellen sind hier nicht genau. Vgl. WELCHMAN b), Appendix, S. 307

[99] JOHNSON, S. 347

[100] DEAVOURS/KRUH a), S. 123

[101] NARA Dokument Box CBTE28, Nr. 3620 «Cryptanalysis of German Army & German Air Force ENIGMA Traffic», S. 59

gebraucht worden wären.[102] Auch die Aussage bei HODGES[103], dass im Register pro Sekunde mindestens 20 logische Entscheidungen gefällt worden wären, steht im Einklang zu diesen Zahlen. Die hohe Drehzahl war möglich, weil zum Registrieren sehr schnelle Relais mit einer Ansprechzeit von etwa 0,001 s verwendet worden waren.[104] Wenn die Registerlogik einen Zielzustand erkannt hatte, wurden nur die mittlere und die untere Trommel zum Ablesen ihrer Positionen gestoppt. Diese Stellungen und der Status des Registers wurden abgelesen und zur weiteren Prüfung verwendet. Man muss bedenken, dass es durchaus auch zufallsbedingte falsche Stops gab. Je grösser die Anzahl der Schleifen war, umso mehr Kontrollmöglichkeiten und umso weniger falsche Stops ergaben sich.

Schleifen TURINGs ursprüngliche Idee war, eine Gruppe von Vertauschern, deren Anfangsstellungen den relativen Positionen der Buchstaben aus dem Spruch entsprachen, synchron laufen zu lassen und in jeder Position die Übereinstimmung mit dem Klartext zu prüfen. Wegen der unbekannten Steckerstellungen war dies jedoch unmöglich. Die Lösung sah TURING in Schleifen in Paaren von Klarelementen und Geheimelementen. Am Beispiel des Spruches

`U M K H O P Z B I T I A J U X V B Z A I`

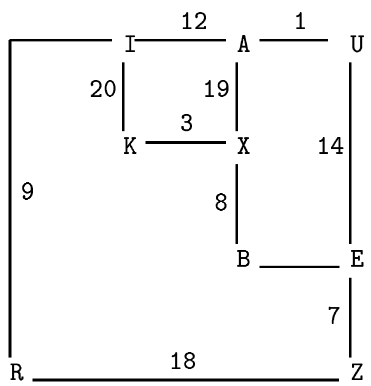
mit dem Klartext

`a n x a l l e x r e g i m e n t e r x k`

liessen sich aus den Paaren aus zusammengehörenden Klar- und Geheimelementen die Schleifen

1) XAUEB
2) EZRIAU
3) XAIK
4) XBEZRIK
5) XBEUAIK
6) XAUEZRIK
7) XAIRZEB

bilden, für die letzten drei grafisch:



An den Knoten des Graphen stehen die Schleifenbuchstaben, an den Kanten zwischen ihnen die relativen Stellungen der Vertauscher, die einen Knoten in den anderen überführen.

[102]WELCHMAN b), S. 144
[103]HODGES, S. 184
[104]WELCHMAN b), S. 144

Das Problem der unbekannten Stecker verlor durch diese Schleifenbildung einen Teil seiner Vielfältigkeit. Angenommen, bei Schleife Nr. 3 sei der Buchstabe X gesteckert mit $St(X)$, A mit $St(A)$, I mit $St(I)$ und K mit $St(K)$. Dann erhielt man, wenn man die Buchstaben der Schleife nacheinander mit entsprechenden Walzenpositionen bearbeitete

$$\begin{aligned} St(X) &= St(A) \cdot Vert(19) \\ St(A) &= St(I) \cdot Vert(12) \\ St(I) &= St(K) \cdot Vert(20) \\ St(K) &= St(X) \cdot Vert(3) \end{aligned}$$

$Vert(\ldots)$ ist die Wirkung des Vertauschers, der in der angegebenen Position den rechten Buchstaben in den linken überführt.

Das liess sich zusammenfassen zu

$$St(X) = St(X) \cdot Vert(19) \cdot Vert(12) \cdot Vert(20) \cdot Vert(3)$$

M.a.W.: Beim Durchlaufen einer Schleife traten die Stecker der „inneren“ Glieder nicht mehr auf. Daraus erwuchs eine Möglichkeit zur Prüfung von Walzenlage, Walzenstellung und auch Steckerlage. Angenommen, es wäre der richtige Stecker für X gewählt und am Knoten X eingespeist, ebenso seien Walzenlage und Walzenpositionen richtig, dann musste am Ende des Schleifendurchlaufs am Knoten X wieder der Steckerbuchstabe erscheinen. Wenn der falsche Stecker bei sonst gleichen Voraussetzungen am Knoten X eingegeben wäre, dann würden an diesem Knoten alle Buchstaben ausser dem richtigen erscheinen, der so zu erkennen wäre. Gleichzeitig wäre jeder dieser beiden Versuchsausgänge ein Indiz für richtig gewählte Walzenlage und Walzenpositionen.

Wenn keiner der beiden Fälle eintrat, d.h. am Eingangsknoten alle Buchstaben vertreten wären, dann waren Walzenlage bzw. Walzenpositionen falsch gewählt. Nicht immer traten am Eingangsknoten alle Buchstaben auf. Dann war es nötig, einen der noch fehlenden erneut einzuspeisen. Damit war TURINGs Grundgedanke bei diesem System erfüllt, Hypothesen bzgl. Walzenlage und Walzenstellungen dadurch zu falsifizieren, dass keine Steckerlage die vorgegebenen Korrespondenzen von Klartext und Geheimtext zu realisieren gestattete.

Mit der angenommenen Walzenlage III, II, I und der Anfangsposition der Walzen `A, A, A` sei in der Schleife

`X B E U A I K`

für `X` der angenommene Steckerbuchstabe `A` eingegeben. Das Zeichen $\mapsto$ symbolisiert die Wirkung der Vertauscher der Schleife:

$$\begin{gathered} \mathtt{A} \mapsto \mathtt{J},\ \mathtt{J} \mapsto \mathtt{V},\ \mathtt{V} \mapsto \mathtt{B},\ \mathtt{B} \mapsto \mathtt{C},\ \mathtt{C} \mapsto \mathtt{N},\ \mathtt{N} \mapsto \mathtt{M} \\ \mathtt{M} \mapsto \mathtt{O},\ \mathtt{O} \mapsto \mathtt{Y},\ \mathtt{Y} \mapsto \mathtt{L},\ \mathtt{L} \mapsto \mathtt{G},\ \mathtt{G} \mapsto \mathtt{Q},\ \mathtt{Q} \mapsto \mathtt{X} \\ \mathtt{X} \mapsto \mathtt{F},\ \mathtt{F} \mapsto \mathtt{Z},\ \mathtt{Z} \mapsto \mathtt{K},\ \mathtt{K} \mapsto \mathtt{R},\ \mathtt{R} \mapsto \mathtt{H},\ \mathtt{H} \mapsto \mathtt{W} \\ \mathtt{W} \mapsto \mathtt{D},\ \mathtt{D} \mapsto \mathtt{U},\ \mathtt{U} \mapsto \mathtt{T},\ \mathtt{T} \mapsto \mathtt{I},\ \mathtt{I} \mapsto \mathtt{P},\ \mathtt{P} \mapsto \mathtt{E} \\ \mathtt{E} \mapsto \mathtt{S},\ \mathtt{S} \mapsto \mathtt{A} \end{gathered}$$

Alle 26 Buchstaben tauchen auf, also ist Walzenlage oder Walzenposition falsch.

Mit dem durch einen Stop erkannten ersten Steckerpaar (u.U. Selbststeckerung) konnte man durch Nachvollzug der in den Schleifen vorhandenen Gleichungsketten weitere Steckerpaare gewinnen. Im Beispiel ergab ein Einspeisen am Knoten `X` als zugehörigen Stecker den Buchstaben `J`. Über das Paar `JM` (13. Stelle des Klartextes) war Zugang zum Steckerpaar `MA`, von da zu weiteren Steckerpaaren, sodass am Ende hier 18 Buchstaben erfasst waren. Mit diesen Kenntnissen war eine Dechiffrierung des Spruches schon erfolgreich und lieferte i.a. die restlichen Stecker. Ausserdem - bisher war die Ringstellung `A A A` vorausgesetzt gewesen, die Stopstelle lag im Beispiel bei `A X P` (Walzenlage III, II, I) - lieferte der Dechiffrierversuch die Schaltstelle (`Q`$\mapsto$`R`) in Position 8$\mapsto$9, also mussten Ringstellung und Grundstellung modifiziert werden zu `A A U` bzw. `A X I`.

Im nächsten Schritt, der bis Mai 1940 anwendbar war, konnte der Spruchschlüssel selbst samt der Ringstellung des Tagesschlüssels ermittelt werden. Im Spruchkopf war die Grundstellung für die Chiffrierung des (unbekannten) Spruchschlüssels offen angegeben. Es musste nun durch Probieren diejenige Ringstellung mit der dritten Stelle `U` gesucht werden (maximal noch 676 Möglichkeiten), die bei zweimaligem Tasten der offenen Grundstellung eine wiederholte Dreiergruppe ergab, die mit `I` endete.
Diese Suche ergab hier den Spruchschlüssel `G N I` und die Ringstellung des Tagesschlüssels `G Q U`. Damit waren alle Sprüche des Tages in diesem Schlüsselkreis lesbar.
Das bisherige Verfahren nahm keine Rücksicht auf die Reziprozität der Stecker, wenn man sich, ausgehend vom ersten Steckerpaar, bei der Suche nach weiteren auf die Schleifen selbst beschränkte.

6.2.3.1.12 «diagonal board». WELCHMAN erkannte, dass hier eine markante Eigenschaft des Chiffriersystems ungenutzt geblieben war. Es kam darauf an, eine an einem Knoten entstehende Zuordnung (z.B. `XE`) umgekehrt (d.h. als `EX`) wieder in die Zusammenschaltung einzuspeisen. Dazu ersann er eine einfache Zusatzvorrichtung zur TURINGschen «Bombe» : Das Diagonalfeld («diagonal board»).

Es bestand aus einer Matrix von 26 · 26 Kontaktbuchsen, die diagonal miteinander verbunden werden konnten, z.B. Buchse `DL` mit der Buchse `LD`. Die Kontakte jeder Zeile waren einem Buchstaben (des Menus) zugeordnet, die Kontakte jeder Spalte repräsentierten den jeweiligen Steckerbuchstaben.

Alle Kontakte einer Zeile - also alle möglichen Steckerbuchstaben des zugeordneten Menubuchstabens - wurden in einem 26-adrigen Kabel gebündelt, das mit einem zu diesem Menubuchstaben gehörigen Knoten verbunden war. Wenn z.B. an einem Knoten `R` am Ausgang des Vertauschers der Steckerbuchstabe `F` erschien, wurde `F` nicht nur in den evtl. auch am Knoten `R` liegenden weiteren Vertauscher eingespeist, sondern über das Diagonalfeld wurde in den Knoten `F` (so er vorhanden war) der Steckerbuchstabe `R` eingegeben. Auf diese Weise erfolgten wesentlich mehr Durchgänge durch die Vertauscher; man kam mit kürzeren Klartextstücken aus. Dies wiederum verminderte die Gefahr, dass innerhalb des Textes ein Weiterrücken der mittleren Walze erfolgte.

Es ist wahrscheinlich, dass auch an den Ausgangspunkten der aktiven Zeilen des Diagonalfeldes Anzeigen für den Status im Falle eines Stops vorhanden waren. Man hätte sonst nur eine Aussage zur Lage der mittleren und der langsamen Walze erhalten mit der Angabe eines einzigen Steckerpaares. Das hätte neue, allerdings kürzere und langsamere «Bombe» -Läufe oder mühsames Probieren mit der TypeX nötig gemacht. Solche zusätzlichen Statusregister liessen Aussagen über mehrere Stecker gewinnen, gewissermassen zusätzlich zu der Aussage, dass die Hypothese bzgl. Walzenlage und Walzenlage nicht zu verwerfen war. Es ist unwahrscheinlich, dass WELCHMAN und TURING diese Chance nicht genutzt hätten.

Am Beispiel eines Spruches

`I M L H X G S D E B P M Q S G U`

mit dem Klartext

`a n x k o m m a n d e u r x i n`

(Walzenlage: `3 1 2` , Kern: `R G A` , Rel.Pos: `17` Ring: `P` , Grund: `O`) soll die Aussagekraft der «Bombe» mit Diagonalfeld gezeigt werden. Die zusammengehörigen Paare von Klarbuchstaben und Geheimbuchstaben des Beispiels und ihre Umkehrungen sind aufgelistet mit der Nummer der Stelle ihres Auftretens im Text:

2	AD	8	AI	1				
1	BD	10						
2	DA	8	DB	10				
2	EN	9	EP	11				
2	GI	15	GM	6				
2	IA	1	IG	15				
1	LX	3						
4	MG	6	MN	2	MS	7	MU	12
3	NE	9	NM	2	NU	16		
1	OX	5						
1	PE	11						
2	SM	7	SX	14				
2	UM	12	UN	16				
3	XL	3	XO	5	XS	14		

Im angegebenen Beispiel liefert die «Bombe» mit Diagonalfeld bei der Walzenlage III, I, II insgesamt 5 Stops, wovon die Nrn. 1 bis 4 nur mehrdeutige „Lösungen" anbieten. Der Stop Nr. 5 liefert die Zuordnungen

A↦M	B↦B	D↦F	E↦Y
G↦G	I↦I	L↦H	M↦A
N↦N	O↦Z	P↦P	S↦S
U↦U	X↦J		

und damit die Steckerpaare

(AM)(DF)(EY)(LH)(OZ)(XJ)

Die Kernstellung der Walze II liegt bei R G A, die relative Position bei 17, die Ringstellung bei P und die Grundstellung bei O. Daraus folgt als Ergebnis, dass die tatsächliche Ringstellung der Walze II (Eingangswalze) 17 Stellen vor A liegt, also bei J, die Grundstellung wegen des Abstandes P - O bei I. Mit der Grundstellung RGI, der Ringstellung AAJ und den eben ermittelten Steckerpaaren erhält man als Dechiffrierergebnis das von Tabelle 4.24 unten.
Es ist offenbar, dass bei den Geheimbuchstaben C und Q falsche Klarbuchstaben entstehen, also ist das nächste (und letzte) Steckerpaar (CQ), womit der Klartext vollständig erscheint. Neben den Aussagen über die Eingangswalze und die Stecker ist aber eine weitere Erkenntnis entstanden: Die Abstände zwischen Ringstellung und Grundstellung betragen für die mittlere Walze 6 und für die dritte Walze 17. Jede Kombination von Ringstellung und Grundstellung, die diesen Vorgaben entspricht (z.B. Ringstellung ABJ, Grundstellung RHI oder Ringstellung BCJ, Grundstellung SII usw.) liefert die gleichen Ergebnisse, vorausgesetzt, dass die mittlere Walze nicht selbst weiterrückt. Das würde aber die genaue Lage der zweiten Stelle von Ringstellung und Grundstellung definieren.

Es gab zwei verschiedene Typen von «Bombes»: «Standard», dabei wurde jeder Stop abgelesen und aufgeschrieben, und «Jumbo», bei dem die Liste der Steckerpaare automatisch in einer Liste ausgegeben wurden. Etwa drei Viertel der Maschinen waren vom Standardtyp, der Rest Jumbo. Bei beiden Typen war als Zusatz die Berücksichtigung des Verbotes, benachbarte Buchstaben in Steckerpaaren zu verwenden «CSKO (Consecutive Stecker Knock Out)», möglich. Als bei der Marine die Griechenwalzen eingeführt wurden, war ein normales Angehen der Sprüche mit der für drei Walzen ausgelegten «Bombe» nicht mehr ohne weiters möglich. Zumindest erforderte es wegen der 26 möglichen Konfigurationen der Umkehrwalze die 26-fache Zeit.

Als Lösung wurde eine vierte Trommel unter den bisherigen angebracht, dazu erhöhte Umdrehungsgeschwindigkeit der Trommeln und Elektronenröhren statt Relais im logischen Entscheidungssystem der «Bombe». Bei WELCHMAN erscheint dieser Versuch als erfolgreich[105] mit mehr als zehnfachem Gewinn an Geschwindigkeit. Nach ERSKINE waren diese erweiterten «Bombes» aber nicht besonders günstig im Betrieb.[106] HODGES spricht sogar von enttäuschendem Ergebnis bei dem Versuch mit extrem schnellen Trommeln. Dadurch blieb die Arbeit an der elektronischen Logikschaltung ohne Wert. Auch eine Vorrichtung, die das Austesten der bei den Stops der «Bombe» registrierten Lagen vereinfachen und beschleunigen und zur Vermeidung des mühsamen Probierens von Hand führen sollte, wurde zwar entwickelt, zeigte aber im praktische Betrieb kaum einen Wert.[107] Die Hilfe kam von den Vereinigten Staaten (siehe Kap. 6.2.1). 1941 versuchten die Briten zunächst, ihr Wissen vor den Amerikanern zu verschleiern, weil sie die amerikanischen Sicherheitsstandards für nicht gut genug hielten. Die USA sollten nur solche Informationen erhalten, die für sie selbst wichtig erschienen, und um die sie ausdrücklich gebeten hätten. Im Juli 1942 wurden amerikanische Offiziere nach Bletchley Park geschickt, um die britischen kryptanalytischen Methoden zu studieren. Im Zusammenhang damit bekamen die Amerikaner auch die Baupläne der britischen «Bombe» . Es wurde dabei auch erkannt, dass in Grossbritannien das Problem einer extrem schnellen Maschine schwer zu lösen wäre. Ebenso war klar, dass Grossbritannien keine ihrer «Bombes» in die USA verschiffen konnte, noch dazu wäre es sicher nicht die neueste. Daher wurde im November 1942 in den USA die Entwicklung initiiert. Ab Mai 1943 standen die ersten Exemplare bereit. Sie hatten keine Ähnlichkeit mit den britischen Geräten. Ende 1943 standen in den USA 96 solcher Geräte zur Verfügung, die die wesentliche Last der Bearbeitung der deutschen Marine-Sprüche zu tragen hatten.[108] Die Entwicklung ging zu einer Maschine, die ohne rotierende Trommeln arbeitete. Sie simulierte die Verdrahtung der Trommeln mit Schrittschaltern und die Rotation (also die Potenzen P^x von Kap. 2.1) mit Relais, später mit Elektronenröhren. Dies ergab schnellere Durchläufe der «Bombe» und vor allem einen Zeitgewinn bei der Menueinstellung.[109] Ein Charakteristikum der amerikanischen Geräte war, dass im Betrieb die Walze, die am weitesten von der Umkehrwalze entfernt war, am langsamsten rotierte, was natürlich Auswirkungen auf die einzustellenden Menus hatte. Angepeilt wurde eine Geschwindigkeit von etwa 1750 Umdrehungen/Minute, was bedeutete, dass ein Durchlauf für eine 4-Walzen-Konfiguration nur etwa 22 Minuten dauerte.[110] Das U.S. Navy Department versprach im September 1942, bis Jahresende 360 Exemplare dieser schnellen «Bombe» zu bauen und die Arbeit an den U-Bootschlüsseln in die eigene Hände zu nehmen.[111] ERSKINE schreibt demgegenüber, dass die Vier-Walzen-«Bombe» der US Navy erst im August 1943 in Gebrauch genommen wurde.[112] Immerhin belief sich die Produktion auf 12 3-Walzen-Maschinen im Monat. Im Januar 1944 wurde die Herstellung der 3-Walzen-Maschine gestoppt, es wurden nur noch 4-Walzen-Maschinen hergestellt.

Die Arbeit an den U-Bootschlüsseln wurde nun ab Herbst 1943 zunehmend in den USA mit den dort vorhandenen 100 4–Walzen–Maschinen vollzogen, wozu die aufgefangenen Sprüche von Bletchley Park geliefert wurden[113]. Ab Mitte 1944 übernahm OP–20–G die gesamte Dechiffrierarbeit für den Schlüssel «Shark»mit den aufgefangenen Sprüchen, die von BP geliefert wurden[114].

[105]WELCHMAN b), S. 148
[106]ERSKINE/WEIERUD, S. 241
[107]HODGES, S. 227
[108]NARA Dokument Box ZEMA34, Nr.4584«History of the Bombe Project»
[109]DEAVOURS/KRUH a), S. 140
[110]NARA- Dokument Box ZEMA10, Nr. 3815«Project 68003 - Cryptanalysis of the German (ENIGMA) Cipher»
[111]HODGES, S. 235
[112]ERSKINE/WEIERUD, S. 241
[113]HODGES, S. 235
[114]BUDIANSKI, S. 295

Eine Maschine in BP wurde für «ISK»genutzt, um die Weiterschaltung der Umkehrwalze, wie bei der Reichsbahn-ENIGMA, mit verändertem «Diagonal Board»zu bearbeiten.

Im Internet sind einige gute Simulationsprogramme zur «Bombe» zu finden, mit denen die obigen Beispiele nachvollzogen werden können.

6.2.3.2 ENIGMA bei Heer und Luftwaffe.

6.2.3.2.1 Notschlüssel. Mitte August 1944 erbeuteten die Briten die Vorschrift zur Bildung der Notschlüssel der Luftwaffe, das Verfahren war also bekannt[115]. Als Anfang September die Schlüssel «Jaguar» (Luftwaffenkdo. West) und «Snowdrop» (Luftgau westl. Frankreich) kompromittiert waren, blieb der Gen.d.Lw.Kanalinseln ohne gültige Schlüssel (der Transport von Schlüsseln mit Flugzeugen war verboten) und war weitgehend auf Notschlüssel angewiesen. Zu allem Überfluss machte der Jafü Süd im Schlüssel des Jagdkorps II die Schlüssel für 8.9. bis 10. 9. bekannt:

	Schlüsselwort	Kenngruppenwort
8.	OSTSEEFISCH	TRENNSCHNITT
9.	NIMROD	HARFE
10.	RANDGEBIET	DUENENLANSCHAFT

Daraus folgten die Kenngruppen TEN, HRE und DNN (UE als ein Buchstabe gezählt!). Über einen weiteren Spruch erfuhren die Briten die vorgesehene Reihenfolge von zehn Kenngruppen. In einem weiteren dechiffrierten Spruch wurde angeordnet, dass ab 1.10. die Kenngruppenwörter als Schlüsselwörter zu benutzen wären, in umgekhrter Reihenfolge und in umgekehrter Lesart, die Schlüsselwörter als Kenngruppenwörter. Da nunmehr die Wörter „von beiden Seiten“ vorlagen, war die Rekonstruktion erleichtert, sodass selbst Wörter wie TRANSPORTNACHSCHUB und ANSCHAUUNGSUNTERRICHT ermittelt wurden.

Für die Zeit vom 11. bis 20.10. mussten alle Wörter von hinten gelesen werden, die Kenngruppenwörter in der Folge 1 . . . 10, die Schlüsselwörter von 10 . . . 1.
Ein Beispiel soll die Findung der Wörter zeigen:

Indikator: ASH; Walzenfolge: 451

B/H , E/I , F/Q , J/U , K/W , L/P , M/S , O/V , R/Z , T/X

Nicht gesteckert sind: ACDGNY
Ringstellung: CYD, daher die Positionen

```
C Y D
G N A
4 5 1
```

Zur Konstruktion des 13 · 2 Tableaus:

Wegen der Folge 4 - 5 kann zwischen G und N keiner der im Alphabet dazwischen liegenden Buchstaben auftreten. Das hat zur Folge, dass die Stecker heissen müssen: H/B, I/E, J/U, K/W, L/P und M/S. H/B und I/E müssen rechts von D/A stehen. A, B, E können nicht im Schlüsselwort sein, weil sie sonst an der ersten Stelle im Stecker stehen müssten, wohl aber könnte N im Schlüsselwort auftreten. Wenn C darin wäre, dann auch D, auch H liegt nahe. Nach D dürfte liegen F. Soweit ergibt es das Bild (unterstrichene Buchstaben im Schlüsselwort):

$\underline{C}$? Y $\underline{D}$ F ? $\underline{H}$? ? ? ? ? ?
G ? $\underline{N}$ A Q ? B ? ? ? ? ? ?

[115]NARA Dokument Box CBMH15, Nr. 1238A, «Capt. W. FRIED Reports», F-103

Nach `Q` müsste liegen `O`, weil es ein Buchstabe vor `Q` sein muss. Wegen der Abstände bei der Bildung des Tableaus liegt nahe, dass auf `H` folgt `M` und darauf `Z`. Somit ergibt sich:

$$\begin{array}{ccccccccccccc} \underline{\texttt{C}} & ? & \texttt{Y} & \underline{\texttt{D}} & \texttt{F} & \texttt{V} & \underline{\texttt{H}} & \texttt{M} & \texttt{Z} & ? & ? & ? & ? \\ \texttt{G} & ? & \underline{\texttt{N}} & \texttt{A} & \texttt{Q} & \underline{\texttt{O}} & \texttt{B} & \texttt{S} & \texttt{R} & ? & ? & ? & ? \end{array}$$

Versuche mit den restlichen Steckern ergibt schliesslich

$$\begin{array}{ccccccccccccc} \underline{\texttt{C}} & \texttt{K} & \texttt{Y} & \underline{\texttt{D}} & \texttt{F} & \texttt{V} & \underline{\texttt{H}} & \texttt{M} & \texttt{Z} & \underline{\texttt{I}} & \texttt{J} & \texttt{X} & \underline{\texttt{L}} \\ \texttt{G} & \texttt{W} & \underline{\texttt{N}} & \texttt{A} & \texttt{Q} & \underline{\texttt{O}} & \texttt{B} & \texttt{S} & \underline{\texttt{R}} & \texttt{E} & \texttt{U} & \underline{\texttt{T}} & \texttt{P} \\ 4 & & 5 & 1 & & & 2 & & & 3 & & & \end{array}$$

Das führt zur Lösung

```
N O R D L I C H T
A B E F G J K M P
Q S U V W X Y Z
```

6.2.3.2.2 «Autoscritcher». Nach der Einführung der steckerbaren UD bei deutschen Streitkräften wurde zunächst gerätselt, wie diese Vorrichtung beschaffen sein könnte. Zunächst wurde davon ausgegangen, dass es sich um eine Konstruktion ähnlich den Griechenwalzen bei der Marine handelte. Erst, als ein Schlüsselblatt mit den Angaben der vorgeschriebenen Steckerung der Umkehrwalze in alliierte Hände gefallen war, wurde die wahre Konstruktion erkannt.

Sowohl in BP als auch in Arlington Hall (USA) wurden in Einzelfällen die tatsächlichen Verbindungen von jeweils aktuellen Umkehrwalzen ermittelt.
Schliesslich wurde in Arlington Hall ein Gerät entwickelt, das die Verbindungen der Umkehrwalze und auch die Lage der Stecker bestimmen konnte: «Autoscritcher»[116] Der Autoscritchers setzte voraus, dass über eine Länge von 150 bis 200 Buchstaben ein Geheimtext mit zugehörigem Klartext bekannt war. Da in vielen Funkkreisen die UD nicht eingesetzt war, gab es viele Spruchwiederholungen in anderen Schlüsseln, sodass diese Bedingung oft erfüllt war.

Zunächst wurden im gesamten Text übereinstimmende Klar-Geheimpaare für alle Stellungen der langsamen und mittleren Chiffrierwalze aufgespürt und zu für diese an den Stellen des Spruches, an denen sie gefunden wurden, durch vollständiger Suche mit $26 \cdot 26$ Möglichkeiten versucht, mögliche Stecker festzulegen. Mit diesen Daten war es dann möglich, die langsame Walze und ihre Stellung sowie die Verbindungen der UD zu erkennen.

Der «Autoscritcher» arbeitet mit Relais und kam 1944 zum Einsatz. Eine voll elektronische Version «Superscritcher»[117] stand erst 1946 zur Verfügung, zu spät für den Einsatz gegen die deutsche Wehrmacht.

6.2.3.3 Marine-ENIGMA.

6.2.3.3.1 M 3. Beim Funkschlüssel M galt seit spätestens 1. 5. 1937 ein Spruchschlüssel-Protokoll, nach dem die Grundstellung jeweils für zwei Tage gültig war (siehe Kap. 1.3.2.2). Wenn es also gelungen war, die Textschlüssel des ersten Tages zu ermitteln, dann erhielt man ein Schema wie

```
.. A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
1. T V X M U I W N F L P J D H Y K Z S R A E B G C O Q
2. E Y K W A Q X R T U C N S L V Z F H M I J O D G B P
3. J G D C F E B P Z A V Q W O N H L T U R S K M Y X I
```

[116] DEAVOURS c), CRAWFORD/FOX
[117] NARA Dokument BOX ZEMA188, Nr. 4334 «Superscritcher I u. II»

Es zeigte, wie der Geheimbuchstabe zu jedem Buchstaben des Alphabets an den Positionen 1, 2 oder 3 des jeweiligen Trigramms lautet.

Im Gegensatz zu den Funksprüchen der Luftwaffe «Red» war es den Briten nach Kriegsbeginn zunächst nicht gelungen, die ENIGMA-Sprüche der Kriegsmarine zu lesen. Einmal lag es am komplizierten Chiffrierprotokoll, das durch Vorgabe von Walzenstellungen individuelle Fehler weitgehend ausschloss, zum anderen daran, dass zusätzlich Walze VI bis VIII verwendet wurden, deren Verdrahtungen (und bei Walze VIII deren Existenz) in BP zunächst nicht bekannt waren.

Als TURING 1939 in die Organisation eintrat, interessierte er sich für das Chiffriersystem der Marine und setzte dort ein, wo die Polen 1937 resigniert hatten.[118]

Bei den Sprüchen vom 5.Mai 1937 gab es

Indikator	Anf.-Stellg.
`KFJX EWTW`	`PCV`
`SYLG EWUF`	`BZV`
`JMHO UVQG`	`MEM`
`JMFE FEVC`	`MYK`

Hier konnte man annehmen, dass die fünften und sechsten Buchstaben des Indikators die dritte Stelle des Spruchschlüssels bestimmten, die ersten beiden die erste Stelle des Schlüssels. Eine einfache Ersetzung der Buchstaben des Textschlüssels durch Bigramme war nicht anzunehmen, sonst hätte der letzte Textschlüssel lauten müssen `MYY`

Beispiele vom 2. Mai

`EXDP IVJO`	`VCP`
`XXEX JXJY`	`VUE`
`RXXX JLWA`	`NUM`

zeigen, dass offenbar die Bigramme `EX` und `XX` sowohl den Buchstaben `V` als auch `U` zugeordnet sein mussten, abhängig von der Position. Der Schluss wurde gezogen, dass eine Chiffreirung der Grundstellung und eine darauf folgende Substitution durch Bigramme eine Rolle spielen mussten.

Weil Sprüche inzwischen mit dem Verfahren FORTYWEEPY nicht mehr lesbar waren und diese Entwicklung ihren Grund darin hatte, dass inzwischen Ziffern in Worten ausgedrückt wurden[119], konzentrierte sich TURING auf Sprüche zunächst aus 1938. Als erster Tag wurde Anfang 1940 der 28. November 1938 gebrochen, danach noch weitere 4 Tage. Allerdings bedeutete das noch nicht, dass man den gesamten Verkehr nun lesen konnte. Die Polen bedankten sich in einem Brief an TURING für den Erfolg beim 28.11.1938.[120] Hier wurde das Problem deutlich, die Tatsache der Entzifferung von ENIGMA-Sprüchen absolut geheim zu halten, damit nicht die deutschen Chiffrierverfahren etwa geändert würden. Die Geheimhaltung ging so weit, dass selbst Empfänger der Informationen, die aus ENIGMA-Sprüchen stammten, diese Tatsache nicht erfahren durften.

Zu der Zeit waren nur 6 Buchstaben gesteckert, der Angriff war leichter. Dabei wurde auch entdeckt, dass ein Buchstabe niemals zwei Tage nacheinander gesteckert war. Wenn also die Stecker eines Tages bekannt waren, kannte man von vornherein 12 ungesteckerte Buchstaben des folgenden Tages.[121] Die Nutzung der Fortsetzungen endete allerdings im September 1939, weil die Rufzeichen der Empfänger wegfielen und somit

[118] Seine Motivation: 'It would be so interesting to break it.'

[119] Ein Kriegsgefangener hatte diese Tatsache im November 1939 ausgeplaudert

[120] P.R.O. HW 24/12, Nr. 83440: „Wir danken Y vielmals für die Mitteilung der eleganten Methode Kx, die wir mit Erfolg beim 29.2.40 angewandt haben. Wir sind Ihnen sehr verpflichtet für die Übersendung der vielen gelösten Tage, wir können natürlich in dieser Beziehung mit Y nicht wetteifern. Herrn T. senden wir herzliche Glückwünsche und vielen Dank für den gelösten 28.11.38.“

[121] ALEXANDER, Chapter II, par. 20.

nicht mehr ausgemacht werden konnte, welche Sprüche Fortsetzungen waren. Zu dieser Zeit begann der EINS - Katalog eine zunehmende Rolle zu spielen. Durch das Aufbringen von Schiff 26 im April 1940 fanden die Briten reichlich zueinander gehörende Klar- und Geheimtexte mit Schlüsseln für zwei Tage (23. und 24. April).[122] An derselben Stelle schreibt HINSLEY, dass im August 1940 die Walze VIII als Beute in britische Hände gelangt war. Aus den veröffentlichten Quellen ist nicht klar zu erkennen, ob BP schon vor dieser Beute von der Existenz der Walze VIII Kenntnis hatte.

Die Walzen VI und VII waren bereits Anfang 1940 erbeutet worden.

In der Beute von Schiff 26 befanden sich auch die Einzelheiten des Indikatorsystems, und das Signalbuch für Kurzsignale.

Mit den nun bekannten Schlüsseln wurden alle Sprüche mit Hilfe des EINS - Kataloges ausgewertet und die Bigrammtafeln rekonstruiert. Trotzdem verhalfen diese Kenntnisse ausserhalb der Tage, für die nun Chiffrierunterlagen vorlagen, nur zu wenigen weiteren Erfolgen beim Lesen von ENIGMA- Sprüchen. Zudem waren im Schlüsselbereich „Heimisch“ ENIGMA-Sprüche und Sprüche im Reservehandverfahren auf den ersten Blick nicht auseinanderzuhalten, weil in beiden Verfahren die Kenngruppen am Anfang des Spruches am Ende wiederholt wurden. Allenfalls erlaubten die von der jeweiligen Kommandostelle hinzugefügten Leitnummern die Identifizierung als ENIGMA-Sprüche.

Hervorzuheben ist hier, dass im Februar 1941 der 28. April 1940 gebrochen werden konnte, der erste Erfolg mit Hilfe der «Bombe» auf Grund eines angenommenen Klartextes und durch alle 336 Möglichkeiten der Walzenpositionen.

Da die Erfolge nicht im gewünschten Umfange eintraten, plante die Navy Angriffe, um an Schlüsselmaterial zu kommen. Bei dem Unternehmen der britischen Marine gegen die Lofoten wurden vom Vorpostenboot „Krebs“ am 4.3.1941 die Schlüssellisten für Februar erbeutet, die nun rückwirkendes Lesen vieler Sprüche ermöglichten. Der volle Erfolg blieb jedoch noch aus, da die für die Dechiffrierung notwendigen Doppelbuchstaben- Tauschtafeln nicht bekannt waren. Ende März waren sie jedoch fast vollständig rekonstruiert. Im Mai 1941 wurden diese Tafeln (Ausgabe „Bach“) von Bord des erbeuteten U 110 geholt. ERSKINE bezeichnet diese Tafeln als eins der wichtigsten Dokumente für BP.[123] Damit war der Weg frei für viele Erfolge, allein am 14.5. wurden 90 Sprüche gelesen. Aus U 110 wurden auch das U-Boots-Kurzsignalheft, das Signalbuch der Kriegsmarine und die Unterlagen für das Chiffrierverfahren „Offizier“ für April 1941 gesichert. Letzteres war aber offenbar keine grosse Hilfe. Die ebenfalls gewonnene Chiffriermaschine selbst war insofern keine Sensation, als in BP schon einige vorhanden waren (z.B. solche, die im Norwegen-Feldzug in britische Hände gefallen waren). Erst nachdem Schlüsseltafeln für Juni und Juli von den durch geplante Aktionen aufgebrachten Wetterschiffen „München“ und„Lauenburg“ im Mai bzw. Juni 1941 in britische Hände gelangt waren, begann der laufende Erfolg beim Lesen von Sprüchen im Bereich „Heimisch“ ab August 1941. Auch die Rekonstruktion der ab 15. Juni gültigen neuen Bigramm-Tauschtafeln gelang wegen der Fülle der lesbaren Sprüche ohne allzu grosse Mühe[124]. Anfang Dezember 1941 wurden bei Angriffen auf drei Vorpostenboote vor der norwegischen Küste die neuen Bigrammtafeln erbeutet, eine grosse Hilfe für die Fortführung des Banburismus[125]. Eine wesentliche Hilfe war dabei, dass die innere Einstellung der Maschine noch im Gegensatz zur täglichen Änderung für die äussere Einstellung bei „Heimisch“ nur alle zwei Tage geändert wurde. So benötigte Hut 8 im August 1941 für den Schlüssel des ersten Tages etwa drei Tage, für den des zweiten Tages dagegen nur etwa 24 Stunden.

[122] HINSLEY II/2, App. 30, S. 957
[123] ERSKINE b), S. 497
[124] ERSKINE b)
[125] SEBAG-MONTEFIORE, S. 300

Zum kontinuierlichen Brechen des Schlüssels „Heimisch“ trug die Beschränkumg der Walzenlagen bei den zusammengehörigen Tagen bei: Wenn z.B. am 1. und 2. des Monats die Lage der Walzen I, VI, II war und am 5. und 6. Tag VIII, III, IV, dann kamen für den 3. und 4. Tag in der ersten Position weder I noch VIII, in der zweiten Position weder VI noch III und in der dritten weder II noch IV in Frage. Eine weitere Bedingung besagte, dass immer wenigstens eine der Walzen VI, VII und VIII benutzt werden musste. Diese Beschränkungen, die ein Abgehen von zufälligen Walzenlagen darstellte, verminderte (im angegebenen Beispiel) die für den 3. und 4. Tag möglichen Walzenlagen von 336 auf 133, was den Kryptologen von BP die Arbeit erleichterte.

1944 wurden Strukturen für die Wahl der linken Walze an aufeinander folgenden Zwei-Tages-Perioden festgestellt (1. Spalte aktuelle linke Walze, Zeilen gaben die Anzahl der Fälle an, in denen die Walze der ersten Zeile auftrat):[126]

	1	2	3	4	5	6	7	8
1	.	.	1	10	19	42	53	44
2	1	.	4	13	16	42	41	58
3	4	2	.	10	23	35	25	38
4	30	35	12	.	13	20	24	15
5	45	48	28	19	.	4	8	5
6	35	29	39	37	20	.	8	4
7	29	32	29	42	30	9	.	.
8	34	28	22	23	29	16	7	.

Das hiess, dass nach einer Periode mit linker Walze I mit hoher Wahrscheinlichkeit eine der Walzen VI, VII oder VIII benutzt wurde. Eine weitere Beobachtung half, die Anzahl der durchzuprobierenden Walzenlagen noch mehr zu verringern : Es gab 15 Walzenlagen im Monat, dabei war es extrem selten, dass eine Lage dreimal auftrat. Alle Lagen, die im Laufe eines Monats bereits zweimal vorgekommen waren, konnten für den Rest des Monats ausgeschlossen werden. Eine enorme Ersparnis an „Arbeitszeit“ für die «Bombes».

Eine weitere Hilfe waren die Wettermeldungen, die von der Marine-Funkstelle Norddeich regelmässig chiffriert gesendet wurden. In Hut 10 war dieser Schlüssel im Februar 1941 gebrochen worden. (Vgl. Kap. 6.2.2.2.5) Nachdem vom Wetterschiff „München“ (wie von U 110) der Wetterkurzschlüssel sichergestellt werden konnte, erkannte man, dass die Wettermeldungen von Norddeich oft vorangegangene Wettermeldungen der U-Boote enthielten. Somit lieferten die Sprüche von Norddeich brauchbare Klartextannahmen von i.a. sieben Buchstaben Länge für die Menus der «Bombe» bzgl. U-Boot-Sprüchen im Bereich „Heimisch“. Diese Wetterkurzmeldungen dauerten nur etwa 10 Sekunden und waren wegen der Gefahr der Peilung bei längeren Sprüchen eingeführt worden. (Gepeilt wurde trotz der Kürze, wenngleich anfangs recht ungenau.)

Solange die U-Boot-Funksprüche im Bereich „Heimisch“ angesiedelt waren, konnten auch viele Sprüche im „Werftschlüssel“ als wahrscheinlichen Klartext verwendet werden, weil sie manchmal wortgetreu in beiden Verfahren gesendet wurden. Widersprüchlichkeit herrscht bezüglich der Einbeziehung der Atlantik- U-Boote in „Heimisch“ nach April 1941. Es soll bis Oktober eine veränderte Version benutzt worden sein.[127] Möglicherweise handelt es sich dabei um die Folge eines Stichwortbefehls (Vgl. Kap. 1.3.2.5.1). Ein solcher („Prokyon“) war vorher schon einmal (am 23.5.1940) erlassen worden.[128]

Der Inhalt des ab Spätsommer 1941 neu eingeführen Kurzsignalheftes[129] wurde bis zum Frühjahr 1942 nur bruchstückweise erkannt.[130]

[126] MAHON, Kap. XI, S. 6
[127] ERSKINE a), S. 180
[128] Beitrag zum Kriegstagebuch SkL vom 21.5.1940, S. 30: „Schiff 26 und Schlüsselsicherheit“ , BA/MA RM7/193
[129] M.Dv.Nr. 96 anstelle des U-Boots- Kurzsignalheftes M.Dv.Nr. 299
[130] ERSKINE b), S. 502

Der in „Hydra“ umbenannte Schüssel „Heimisch“ blieb übrigens für die U-Boote im Nordmeer bis Juni 1944 gültig.[131]

Seitens der U-Boot-Führung wurden laufend weitere Erschwerungen für die unbefugte Dechiffrierung eingeführt, manche, um angesichts der alliierten Erfolge bei der Vermeidung von Convoy-Kontakten mit U-Booten als möglich erachteter Spionage entgegenzuwirken. Ab August wurde als Bootsadresse der Name des Kommandanten genannt.

Wesentlich war auch die Verschleierung von Positionen. Die deutsche Marine benutzte ein Quadratnetz, das die Erdoberfläche in Grossquadrate einteilte. (Kap. 1.3.2.10) Aus der Beute vom Vorpostenboot „Krebs“ erhielten die Alliierten auch einige Karten mit solchen Marinequadraten. Weitere solche für den Atlantik bekamen sie aus dem Wetterschiff „München“ und von „U 110“ in die Hand. Durch Vergleiche von Vorkommnissen (Sichtungen, Angriffen, Versenkungen, Peilungen usw.) war es möglich, Klartextannahmen für deutsche Funksprüche zu gewinnen.

Im Juni 1941 wurden die Positionen nicht mehr nach Marinequadraten angegeben, sondern (Kap. 1.3.2.10) relativ nach Kompassrichtung und Entfernung zu Festpunkten mit Codenamen (z.B. Hammer, Hecht, usw.). Mit den Festpunkten war BP im Juli 1941 einigermassen vertraut. Man darf nicht vergessen, dass in BP alle Informationen an einer Stelle zusammenliefen. So waren die Auslaufsmeldungen im „Werftschlüssel“ bekannt, charakteristische Kurzmeldungen, die von gepeilten Positionen aus abgegeben waren, Fühlungshalter-Signale (gepeilt), all das zusammen mit evtl. Gefangenenaussagen usw. engte die Möglichkeiten für die Bedeutungen der Festpunkte ein, sodass das Bild immer klarer wurde.

In einem Spruch von 504 Gruppen, der nie gebrochen worden ist, hat DÖNITZ befohlen, dass ab 10.9.1941 die Positionsangabe durch Festpunkte fallen gelassen werden sollte, weil sie sich offenbar nicht bewährt hatte. Im September 1943 wurde erneut Festpunkte benutzt, aber nach kurzer Zeit wieder fallengelassen. Dafür wurden nun die beiden Buchstaben in der Angabe von Positionen im Marinequadratnetz besonders chiffriert. Zunächst wurde zur Chiffrierung über jede der 26 Spalten der benutzten Kenngruppen-Tauschtafel eins der häufigsten Bigramme des Quadratnetzes geschrieben. Aus den 26 darunterstehenden wurde als Geheimgruppe jeweils eine willkürlich ausgewählt. [132] Dies hat in BP immer wieder zu Schwierigkeiten bei der Deutung der im evtl. dechiffrierten Spruchtext angegebenen Positionen geführt.[133] Verschiedentlich war es allerdings möglich, durch aufeinander folgende Sprüche mit alter bzw. neuer Chiffrierung Einblick in die Tauschtafeln bekommen, auch manchmal durch Befehle des Befehlshabers der U-Boote. Es muss hier beachtet werden, dass diese Chiffrierung der Bigramme die Verwendung bei Kurzsignalen nach der Vorschrift M. Dv. Nr. 96 (Kurzsignalheft 1941) ausschloss, da dort für die Quadratangaben besondere Geheimgruppen definiert wurden. Ab 24.11.1941 wurden für die Chiffrierung der Grossquadrate besondere Tauschtafeln eingeführt. Die dazu jeweils zu benutzenden Tauschtafeln wurden durch fiktive Anschriften festgelegt. Die Schwierigkeiten bei der Deutung der die Grossquadrate darstellenden Bigramme nach der im April 1943 eingeführten Erschwerung der unbefugten Dechiffrierung durch Definition der Tauschtafeln mit weiblichen Vornamen [134] konnten erst als überwunden angesehen werden, als im Juni 1944 aus U 505 u.a. ein „Adressbuch“ geborgen werden konnte. Die Beute aus U 505 war reichlich und brachte den alliierten Diensten grosse Hilfen:[135]

[131] Y'BLOOD, S. 30
[132] KAHN a), S. 204
[133] HINSLEY II, App. 9, S. 682
[134] U-Boot Kartenschlüssel, Stichwort . Adressbuch, vom 5.4.1943, NARA Dokument (engl.), Box CBKJ21, Nr. 1673«U-Boat Chart Cipher, Catchword Address Book»
[135] NARA Dokument Box ZEMA20, Nr.35285N,«The German Naval Ciphers», S.87

Zwei Chiffriermaschinen ENIGMA Nr. 3467 und 4473
Einen Drucker für ENIGMA
Dienstvorschriften:
Schlüssel M - Allgemeine Bestimmungen 1941
Schlüssel M Verfahren M-Allgemein M.Dv.Nr. 32/1
Schlüssel M-Verfahren M Offizier und M Stab M.Dv.Nr. 32/2
Bestimmungen zur Wahrung der Schlüsselsicherheit bei Verlusten von Schlüsselmitteln M.Dv.Nr. 949
Reservehandverfahren 49, M.Dv. Nr. 929/1
Signalschlüssel für den Funksignaldienst M.Dv.Nr. 114
Ständige Kriegsbefehle des BdU zu M.Dv. Nr. 97
Wetterkurzschlüssel M.Dv.Nr. 443
Kenngruppenbuch - K-Buch M.Dv.Nr. 98, Ausgabe 1941
Doppelbuchstabentauschtafel für Kenngruppen, Kennwort „Mündung“ zu M.Dv.Nr. 98, ebenso für Kennwort „Quelle“
Kurzsignalheft 1941
Kenngruppenheft Nr. 5 zum Kurzsignalheft 1941, M.Dv.Nr. 86
Geheime Marinefunknamenliste M.Dv.Nr. 82, Ausgabe 1942
Spruchschlüsseltafel für den Wetterkurzschlüssel, 3. Ausgabe
Adressbuch Ausgabe April 1943
Schlüsselheft F,49
Schlüssel Triton Juni 1944
Schlüsseltafeln M-Offizier
Drei geheime Briefbücher U 505

Eine ausführliche Darstellung der Chiffrierungen des Gitternetzes hat ERSKINE veröffentlicht.[136] In einem handschriftlichen Bericht wird dargestellt, wie z.B. die 1941 und 1943 benutzten Tafeln „Becker“ und „Krause“ in BP bzw. in den USA rekonstruiert worden sind.[137]

6.2.3.3.2 Offizier. Bei dem Problem der Offizier-Sprüche war zu unterscheiden zwischen den Schlüsselbereichen, bei denen nur die Walzenanordnung spezifisch war,die innere Einstellung einschliesslich der Steckerlage aber dem Schlüssel Allgemein entsprach und der normalen Offiziers-Chiffrierung, bei der auch die Stecker aus der Schlüsseltafel für die Offizierssprüche genommen werden mussten.

Im ersten Fall half seit Novemver 1943 eine schnelle amerikanische Maschine („Hypo“), die den Spruch bei allen möglichen Walzenstellungen dechiffrierte und über die entstehenden Buchstaben Statistiken führte, also in etwa so etwas wie Spracherkennung betrieb. Es wurden auch der einer oder mehrere hochfrequente Buchstaben mit jeder Startposition chiffriert, und durch Filmvergleich wurde festgestellt, welche Startposition die höchste Trefferquote, gemessen am vorliegenden Geheimtext aufwies[138]). Im Laufe eines Monats wurden dann mehr und mehr Tageseinstellungen erkannt, was auch durch die unsinnige Regel erleichtert wurde, dass jeder Buchstabe in der Walzenstellung des Monats in jeder der Positionen nur einmal auftreten durfte.

Im zweiten Fall mit den Offizier-eigenen Steckern war das Problem etwas schwieriger. Beim ersten Spruch des Monats musste mit versuchten Klartext unter der Verwendung der Bomben gearbeitet werden, was u.U. bis zu 100 verschiedene Versuche nötig machte. Hier halfen auch Fortsetzungen von Sprüchen, wo das `/fort/` den Einstieg erleichterte.

[136] ERSKINE a)
[137] NARA Dokument Box CBKJ21, Nr. 1675«General Nature of Address Book»
[138] BUDIANSKI, S. 288

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	
A	.	.	1	1	.	.	.	1	1	.	.	.	1	.	1	.	.	.	.	.	.	.	.	.	.	.	
B	.	.	.	.	.	1	2	1	2	1	2	.	2	.	.	.	.	.	1	.	2	.	.	.	.	1	←
C	.	1	.	.	.	.	.	.	1	.	.	1	.	.	.	.	.	.	.	1	.	.	.	.	.	.	
D	1	.	.	1	.	.	1	.	1	.	1	.	.	.	1	.	.	.	.	1	1	.	.	.	.	.	
E	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	
F	2	1	.	3	.	.	2	1	3	1	.	.	5	.	.	.	.	1	.	.	4	.	.	.	1	.	←
G	.	1	.	.	.	1	.	.	.	.	.	.	1	1	.	.	1	.	.	.	.	.	.	1	.	.	
H	3	.	.	2	1	.	2	.	3	1	1	.	6	.	.	.	.	1	.	1	3	.	.	.	1	.	←
I	.	.	1	.	1	.	.	1	.	1	.	.	1	.	.	1	.	1	.	.	.	.	1	.	.	.	
J	1	.	.	1	.	.	1	.	1	.	.	.	.	1	.	.	.	.	.	.	1	.	.	.	.	.	
K	.	1	.	.	.	.	.	.	.	.	.	1	.	.	.	.	1	1	.	.	.	.	.	.	.	.	
L	.	.	.	.	.	.	.	.	.	.	.	.	.	.	1	.	.	.	.	.	.	.	.	.	.	.	
M	1	.	.	.	1	.	1	.	1	.	1	.	.	.	.	.	.	1	.	.	.	.	.	.	.	.	
N	.	.	1	.	.	1	.	.	.	.	.	.	1	.	.	.	1	1	.	.	.	.	.	.	.	.	
O	1	1	.	1	.	.	.	1	.	1	.	.	1	1	.	1	.	.	.	.	.	.	.	.	.	.	
P	4	.	1	3	.	.	2	.	2	.	.	1	6	.	.	1	1	.	.	.	3	.	.	.	1	.	←
Q	.	.	.	.	.	.	.	.	.	.	1	1	.	.	.	.	.	.	.	.	1	.	.	1	.	.	
R	1	.	.	.	.	1	1	.	.	.	1	.	2	1	.	.	.	.	1	.	1	.	.	1	.	.	
S	3	.	.	2	.	1	3	1	4	1	1	.	6	.	.	.	.	.	1	.	3	.	.	.	1	.	←
T	.	.	.	1	1	.	1	.	1	.	.	1	1	.	.	.	.	.	.	.	.	.	.	1	.	.	
U	1	.	.	1	.	.	.	.	.	.	1	.	.	.	.	.	1	.	1	.	1	.	.	.	.	.	
V	.	1	.	.	.	.	1	1	1	1	.	.	.	.	1	.	.	1	1	.	.	.	.	.	.	.	
W	2	.	.	2	.	1	2	.	2	.	.	.	3	.	.	.	.	.	1	.	3	.	.	.	.	.	←
X	.	.	1	.	1	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	1	.	.	.	.	.	
Y	.	.	.	.	.	.	.	.	1	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	
Z	1	.	.	1	.	.	.	.	.	.	1	.	1	.	.	.	.	.	.	1	.	.	.	.	.	.	

Tabelle 6.2:

Die Stecker wurden mit einer Methode ermittelt, die «Dottery» genannt wurde. Dabei wurde der Spruch – die Walzenanordnung war mit anderen Methoden bekannt – ohne gesetzte Stecker getastet und die entstehenden Buchstaben in einem 26 · 26-Raster wie im Beispiel registriert. (Tabelle 6.2)
Von links wurden die Spruchbuchstaben eingegeben, das Ergebnis wurde in den Spalten eingetragen. Zur Auswertung war zu beachten, dass sechs Buchstaben nicht versteckert waren. Diese mussten im Ergebnis entsprechend der Sprachstatistik verteilt sein. Wenn in einer Spalte mehr Ereignisse auf eine geringe Zahl von Zellen zu finden waren (hier die Spalte `M`), dann konnte man davon ausgehen, dass es sich um die Spalte mit dem Stecker für `E` handelte.

Die Zeilen mit gehäuftem Auftreten von Ereignissen und in der Sprachstatistik weisen auf ungesteckerte Buchstaben hin. (In der Tabelle mit Pfeilen gekennzeichnet.)

Nachdem der Stecker für `E` gewonnen war, konnten weitere gefunden werden, indem, ausgehend von der Anfangslage der Walzen, für die gesamte Spruchlänge nur der Buchstabe getippt wurde, der der Stecker von `E` war. Dann mussten beim Vergleich des Geheimtextes mit dem Ergebnis dieser Eingabe die Paare hervortreten, die gegenseitige Steckerbuchstaben waren, u.U. auch Bestätigungen für Steckerlosigkeit.

Aus den Spalten im obigen Beispiel liessen sich auch Vermutungen bzgl. der Stecker für weitere, im Deutschen häufige Buchstaben (`T, O, N, I, A`) entnehmen, hier bezogen auf die Spalten `A, D, G, I` und `U`[139].

Wenn für einen Tag im Monat die Steckerlage und die Walzeneinstellung für einen Offiziers-Schlüssel gefunden waren, konnten alle Offizier-Sprüche des Monats gelesen

[139]SEBAG-MONTEFIORE, S. 350ff

werden. Mit bekannten Steckern fand man andere Offizier-Schlüssel des Tages, mit diesen dann andere Stecker-Kombinationen usw[140].

6.2.3.3.3 M 4. Am 5.10.1941 wurde für die Atlantik-U-Boote ein eigener Schlüsselkreis eingeführt („Triton") mit dem Schlüssel M Form M 4, allerdings noch mit der Griechenwalze Beta in neutraler Position, als 3-Walzen-Maschine. Angeblich soll - nach KAHN - in U 570 im August 1941 bereits ein Schlüssel M Form M 4 gefunden worden sein, aber wohl ohne Griechenwalze. Das ist eher unwahrscheinlich.[141] ALLASON spricht davon, die Einführung der Form M 4 sei durch einen Kurzspruch ($\beta\beta$) angekündigt worden. [142] Weil nunmehr kaum noch inhaltliche Gemeinsamkeiten mit dem Schlüsselkreis „Werftschlüssel" bestand, mussten im wesentlichen die Wetterkurzmeldungen für das Gewinnen von für die «Bombe» brauchbaren Klartexten herhalten.[143] Erleichterung brachten aber auch weitere Doppelbuchstaben-Tauschtafeln, die in britischen Besitz gelangt waren:

11.6.41 „Teich" aus Schiff Gedania
Jan. 42 „Ufer", „Strom" aus Schiff Geier

Die Tatsache, dass „Strom" auch in U 505 im Februar 1943 gefunden wurde, weist auf die lange Geltungsdauer der Tafel hin.

Im Dezember 1941 ist versehentlich eine normalerweise noch mit der Griechenwalze Beta in der neutralen Position A (Siehe Kap. 1.1) als M 3 zu betreibende Form M 4 mit falscher Stellung der Walze Beta benutzt worden. Der falsch abgesetzte Spruch wurde mit der richtigen Stellung anschliessend wiederholt.[144] Dadurch soll es BP möglich gewesen sein, die inneren Verdrahtungen der Griechenwalze Beta und der Umkehrwalze B dünn zu bestimmen. ERSKINE bezweifelt, dass dies mit diesem einen Spruch möglich gewesen sein soll.[145]

Mit dem 1.2.1942 wurde der Schlüssel M Form M 4 als 4-Walzen-Maschine benutzt, von diesem Tage an war BP, was den Schlüsselbereich Triton angeht, praktisch für 10 Monate blind. Das traf die britische Führung besonders hart, weil gerade die U-Boote die grösste Gefahr für die Versorgung der Britischen Inseln und somit für die Fortführung des Krieges bildeten.

Allerdings blieben aus anderen Schlüsselbereichen Kenntnisse erhalten. Der Schlüsselbereich „Heimisch" war in „Hydra" umbenannt worden, z.B. Aussagen über Ausfahrten und Rückkehr von U-Booten, Geleite usw.[146], aus dem Werftschlüssel über Küstenschiffahrt[147], sowie aus einem Teilschlüssel von „Hydra" ein fast vollkommenes Bild von der Indienststellung bis zur ersten Kriegsfahrt neuer U-Boote. (BEESLY nennt diesen Schlüssel «Thetis»[148], aber HINSLEY[149] und ERSKINE[150] schreiben übereinstimmend, dass «Thetis» nie gebrochen worden wäre.) In diesen Schlüsseln wurden von den rund 1200 täglichen Sprüchen im Monat über 10000 Sprüche gelesen.[151] Ausserdem war noch eine gewisse Hilfe für das Raten über Orte und Absichten der U-Boote gegeben durch die bisherigen Erfahrungen über Taktik und Perönlichkeiten der Kommandanten, Marschgeschwindigkeiten, Reichweiten der einzelnen Typen usw.[152]

[140] ALEXANDER, S. 15, Abschnitt 55
[141] KAHN a), S. 214
[142] ALLASON, S. 223
[143] Ab Frühjahr 1941 nach dem Wetterkurzschlüssel, M.Dv. Nr. 443 von 1940
[144] HINSLEY II, App. 19, S. 747
[145] ERSKINE a), Fussnote 73, S. 181
[146] DEUTSCH, S.22; ROHWER b), S. 642
[147] GOULTER, S. 93
[148] BEESLY a) Teil II, S.374; b), S. 146
[149] HINSLEY II, App. 4, S. 664
[150] ERSKINE a), S. 176
[151] KAHN a), S. 215
[152] BEESLY b), S. 145

Aus dem Werftschlüssel folgte auch die Kenntnis, dass von April bis Oktober 1942 die Grundstellungen von „Heimisch" und „Triton" einfach gespiegelt waren: z.B. `ABC` und `CBA`.[153]

Im Frühjahr 1942 wurde der Wetterkurzschlüssel geändert. Ein solcher Spruch bestand nun aus 11 Buchstaben und benutzte einen Spruchschlüssel von vier Buchstaben.[154] Damit war eine wesentliche Quelle für brauchbare Klartexte verstopft. Es gelang BP nur, Sprüche von zwei Tagen im Februar und einen vom 14.3.1942 zu dechiffrieren. Im letzteren Falle soll es sich um die Mitteilung von DÖNITZ auf vielen Schlüsseln gehan4delt haben, dass er zum Admiral befördert worden war. (Siehe Kap. 1.4.2.2 (Werftschlüssel)) Sechs «Bombes» mussten dazu 17 Tage rund um die Uhr laufen. (Vermutlich - Aussagen liegen nicht vor - wurden die verschiedenen Walzenlagen der drei rechten Walzen mit jeweils einer veränderten Umkehrwalze, entsprechend einer Stellung der Griechenwalze Beta, durchgefahren.)

Die Erlösung für BP kam erst, als U 559 am 30.10.1942 vor Port Said zum Auftauchen gezwungen und aus ihm neben dem 1942 geänderten Wetterkurzschlüssel auch das Kurzsignalheft und diverse weitere Chiffriermaterialien geborgen worden waren.

Nun standen wieder Klartexte zur Verfügung aus Wetter- und anderen Kurzsignalen. Am 24.11. kam das Material aus U 559 in BP an. Es wurde sofort angewandt, bis dann am 13.12. insgesamt 12 U-Bootspositionen aus 15 Wetterkurzmeldungen der Tage 5. bis 7.12 erkannt wurden.[155] Dabei sahen die Mitarbeiter in BP zu ihrem Erstaunen, dass bei diesen Schlüsseln die 4-Walzen-ENIGMA mit neutralisierter Griechenwalze als M 3 benutzt wurde, also mit Spruchschlüsseln aus nur drei Buchstaben.[156] Wenn ein Tageschlüssel aus einer Kurzmeldung dreistellig gefunden war, waren nur noch 26 Versuche nötig, um die restliche, vierte Stelle zu bestimmen und andere U-Bootsprüche zu lesen.

Im allgemeinen lief es so ab, dass der Befehlshaber der U-Boote von einem U-Boot eine Wettermeldung anforderte, diese dann geliefert und vom BdU quittiert wurde. Anschliessend wurde sie allgemeien ausgestrahlt, aber alles mit der 4 - Walzen ENIGMA M 4 als 3 - Walzen Enigma !

Ende 1942 standen BP insgesamt 49 «Bombes» zur Verfügung, also schon eine höhere Kapazität.

Eine gewisse Schwierigkeit entstand für BP, als die Griechenwalzen Beta und Gamma nicht nur mit den zugehörigen dünnen Walzen `B` bzw. `C` verwendet wurden, sondern auch „über Kreuz". So waren die Kombinationen im Schlüssel „Triton" [157]

1943:

Juni: `B B`; Juli: `C C`; Aug.: `B C`; Sept.: `C B`; Okt.: `B B`; Nov.: `B C`; Dez.: `C C`

1944:

Jan.: `C B`; Feb.: `B B`; März `C C`; Apr.: `B C`; Mai: `C B`; Juni `C C`; Juli: `B B` Aug.: `B C`; Sept.: `C C`; Okt.: `B B`

Ab September 1943 war kein Banburismus mehr nötig, da inzwischen sowohl «bombes» als auch Klartexte in genügender Anzahl verfügbar waren. Wenn zum Finden

[153] ALEXANDER, Abschn.34
[154] HINSLEY II, App. 19, S. 749
[155] ERSKINE a), S. 170
[156] ERSKINE/WEIERUD, S. 241
[157] MAHON , Kap. XI, S.10

der Bigramme ausser der Grundstellung alle Daten bekannt waren, halfen halfen der EINS–Katalog, die «rodding» Methode, speziell auf EINS bzw KRKR eingestellte «Bombes»oder ein Durchlauf durch alle möglichen Stellungen mit der Annahme, der Klarspruch bestehe nur aus den Buchstaben E oder N.

Im März 1943 trat ein neuer Wetterkurzschlüssel in Kraft, in dem der Hinweis auf die Grundstellung nur noch durch einen einzigen Buchstaben gegeben wurde. Da dies den vollen Durchlauf durch alle möglichen Walzenstellungen und -Positionen bedeutet hätte, fielen damit die Wetterkurzmeldungen erneut als Quellen für Klartext-Annahmen aus. Aber das Kurzsignalheft war weiterhin in Kraft geblieben. Damit gelang es zwischen dem 19. März und Ende Juni 1943 an 90 von 112 Tagen mit Hilfe von Sichtmeldungen und anderen Kurzmeldungen, die im M 3-Modus abgesetzt wurden (i. Zshg. mit Peilungen), in den Schlüssel „Triton“ einzubrechen.[158]

Dies gelang im Zusammenspiel der Methoden: Aus eingepeilten Wetterkurzmeldungen wurde durch Vergleich mit den dechiffrierten DAN–Meldungen, auch über die Zeitgruppe, der Zusammenhang zwischen den Wettersprüchen der U-Boote und von DAN hergestellt. Dies führte mit Hilfe des Kurzsignalheftes zunehmend zum Gewinn von Klartextstücken zu den U-Boot–Sprüchen und mit den «Bombes» zu den Schlüsseln selbst.[159] Die Verdrahtung der am 1. Juli 1943 eingeführten Zusatzwalze Gamma zur dünnen Umkehrwalze C soll bereits nach 10 Tagen bekannt gewesen sein. [160] [161].

In BP wurde auch versucht, durch grafische Aufnahme der Morsezeichen die individuellen „Handschriften“ der Funker zu dokumentieren und zu vergleichen. (Verfahren «Tina») Dieses Projekt erwies sich als nicht sehr erfolgreich.

Ab Juni 1943 kam die erste britische Hochgeschwindigkeits–«Bombe» für vier Walzen zum Einsatz, ab August 1943 die schnelleren amerikanischen «Bombes», von denen in kurzer Zeit eine immer grösser Anzahl zur Verfügung stand. Nun war auch ein volles Durchlaufen aller mögliche Stellungen in den Bereich der realen Möglichkeiten gelangt.

Nachdem im Juni 1944 in U 505 ein Adressbuch zur Chiffrierung der Positionsangaben gefunden worden war, war damit ein weiterer Schritt zur weniger problematischen Lösung der Funksprüche der deutschen U-Boote getan.

6.2.3.3.4 Funkschlüsselgespräch. Zusätzlich wurde im April 1943 das sog. Funkschlüsselgespräch eingeführt. Dies gestattete unmittelbaren Dialog über Funk, setzte aber besonders geschulte Funker voraus. Es war bereits im Herbst 1941 zur möglichen Einführung erprobt worden.[162] Als Spruchschlüssel wurde dabei der Drei-Buchstaben-Schlüssel verwendet, der um den verdoppelten letzten Buchstaben zum Vier-Buchstaben-Schlüssel verlängert worden war.[163]

6.2.3.3.5 Kurier. Im August 1944 wurden Versuche mit einem Schnellsendeverfahren begonnen, das das Mithören von Sprüchen und ihre Peilung unmöglich machen sollte. (Verfahren „Kurier“) (BP hatte bereits Kenntnis davon durch einen gelesenen Spruch vom 22.6.) Dabei wurden Frequenzen abweichend von den U-Boot-Frequenzen wechselnd benutzt, bis 9.12. täglich eine Frequenz, die in „Triton“ festgelegt wurde. Ab 9.12. wurde die jeweilige Frequenz in einem Bigramm ausgedrückt, das zweimal mit 4 Blendern chiffriert wurde. Jede Stunde änderten sich diese zwei 4er–Gruppen.

[158] ERSKINE a), Fussnoten 96, 103, 105, S. 182
[159] Ein ausführliches Beispiel bei ALEXANDER und in MAHON
[160] ERSKINE a), Fussnote 110, S. 183
[161] ALEXANDER, S. 61, Abschnitt 6
[162] HIRSCHFELD, S. 141 - 144
[163] ERSKINE a), S. 174

Die Nutzung von „Kurier“ endete am 2.2.1945.[164] Die Alliierten hatten im April 1945 Geräte zur Frequenzfindung und Aufnahme solcher Sprüche fertig, die Versuche mit „Kurier“ waren aber inzwischen abgebrochen.[165]

In der zweiten Hälfte 1944 änderte sich das gesamte Schlüsselbild der U-Boote: Es wurden individuelle Schlüssel für jedes Boot eingeführt. Zusammen mit wesentlich weniger Gebrauch von Funksprüchen und der Benutzung der Schnorchel, was die Radarfindung erschwerte, war den Booten schlechter beizukommen. Trotzdem war zu diesem Zeitpunkt der U-Bootkrieg gewonnen; die Bedrohung war von Grossbritannien und seinen Verbündeten abgewehrt worden.[166]

Ein Beispiel für eine erfolgreiche Ermittlung des Klartextes ist in Anlage B gegeben.

Eine weitere Erschwerung kündigte sich im Schlüssel „Potsdam“ im April 1945 ohne Vorankündigung an: Eine Grundstellungstafel mit 288 Grundstellungen, die mindestens einen Monat gültig war. Auch der Schlüssel „Hydra“ erhielt eine Grundstellungstafel. Da aber viele Sprüche mit den Dringlichleitsvermerken `BINE, MUKE, WESP` oder `KRKR` versehen waren, konnten manche Sprüche mit einer „Mehrfachbombe“, genannt «Fillibuster», die gleichzeitig alle vier berücksichtigte,[167] doch gelesen werden und ein Muster der Grundstellungsliste erkannt werden.

Am 5.5.1945 wurden neue Bigrammtafeln eingeführt, ihre Zahl wurde von 9 auf 15 erhöht.

6.2.3.4 Abwehr-ENIGMA.

Als 1941 mehr und mehr Sprüche in diesem System auftauchten, begann KNOX mit der Analyse. Er ging dabei den Weg, den auch REJEWSKI beschritten hatte (Kap. 3.1.2.1), indem er die Charakteristiken entwickelte. Durch geniale Intuition hatte er Erfolg bei der Bestimmung einiger reziproker Paare in den acht Positionen, was dann zu weiteren Schlüssen führte. Schliesslich fiel ihm auf, dass häufig für einige Spruchschlüssel die Zyklen der Charakteristik einer Stufe aus denen der folgenden Stufe durch Verschieben um eine Stelle in der Folge `QWERTZU`... entstanden.

6.2.3.4.1 «crab». Dies war nur möglich, wenn zwischen der Chiffrierung des ersten und des zweiten Buchstabens des (vierstelligen) Spruchschlüssels und ebenso zwischen der Chiffrierung des 5. und des 6. Buchstabens des (verdoppelten) Spruchschlüssels alle Walzen – einschliesslichder Umehrwalze – weiterrückten. KNOX nannte dieses Vorkommnis «crab».
Knox schloss daraus:

1) Die Maschine besass eine Umkehrwalze, die vor Beginn der Chiffrierung eingestellt werden konnte und während der Chiffriervorgänge auch – wie die anderen Walzen – weiterrückte.

2) Die Eingangswalze der verwendeten ENIGMA war `QWERTZ` ....

3) Die Chiffrierwalzen hatten eine Vielzahl von Positionen zum Weiterschalten der Nachbarwalze, sonst wäre das Autreten von «crabs» sehr selten.

4) Es gab andere Positionen, bei denen alle vier Walzen gleichzeitig weiterrückten, nicht aber vier Positionen weiter (wie bei den «crabs»). KNOX nannte diese Eigenschaft «lobster».

[164] Nara Dokument Box ZEMA44, Nr. 4685«The History of Hut Eight 1939 - 1945»
[165] HINSLEY II, App.5, S. 852
[166] BENNETT b)
[167] MAHON, S. 110

6.2.3.4.2 «lobster». Diese «lobster» vor allem halfen bei der bekannten Neigung der deutschen Funker, statt vier Zufallsbuchstaben vierstelligen Namen o.ä. als Textschlüssel zu verwenden, die Textschlüssel zu finden. Allerdings erforderte das sehr viel Probieren.

Mit den gefundene Textschlüsseln und ihrer Chiffrierung gelang es, die Verdrahtung der jeweilig rechten Walze zu ermitteln.[168].

Es muss aber gesagt werden, dass lange vermutete Klartextsequenzen wegen der sehr häufigen Weiterschaltung der Walzen – im Gegensatz zur Wehrmacht-ENIGMA – nicht hilfreich waren.

Die Theorie entspricht der bei REJEWSKI.[169]

Als im März 1945 dazu übergegangen wurde, den Ring der 4. Walze nicht nur bei `Z` zu lassen, war es zu spät.

[168] Ein Beispiel ist von CARTER unter www.bletchleypark.org.uk/abwehr.pdf zu finden
[169] DEAVOURS b), S. 194 - 196

Kapitel 7

Sowjetische Erfolge ?

Über sowjetische Erfolge bei der Dechiffrierung von ENIGMA-Sprüchen gibt es nur sehr wenige Quellen. Es steht wohl fest, dass die Rote Armee spätestens bei ihrem Sieg in Stalingrad Chiffriermaschinen in die Hand bekommen hat. Wie weit dann laufende Dechiffriererfolge, unabhängig von eroberten Chiffrierunterlagen, zu verzeichenen waren, ist nicht bekannt. Alle Versuche, hier Einblick in russische Archive zu erhalten, sind vergeblich gewesen.
Ab 1943 hat die Sowjetunion allerdings auf britische Informationen über deutsche Truppen in der Sowjetunion verzichtet, was auf eigene Dechiffriererfolge hinweisen könnte.

Am 18.9.1842 warnte der Nachrichtenoffizier des deutschen XXX. Korps, dass die gut organisierte russische Funkaufklärung die Fähigkeit hätte, jede unserer Sprüche zu lesen. Im Januar 1943 stellte die Nachrichten-Abteilung des OKH fest, dass die Russen sicher Enigma-Sprüche entziffert hätten.[1]

In einem Gespräch mit dem Autor sagte der ehem. KGB - General Prof. Dr. S. KONDRASCHOW, in Russland gebe es auch kluge Leute, nur habe er leider ihre Namen alle vergessen.

GOLOVKO behauptet[2], die sowjetischen Dienste hätten den Spruch von Admiral DÖNITZ an die „Scharnhorst“ zeitgleich mit den Briten dechiffriert. In einer ausgedehnten Diskussion zwischen JUKES, MILNER-BARRY und ERSKINE , auch über die Frage, wie weit die Rote Armee Sprüche des Heeres gelesen haben könnte, wird die GOLOVKO'sche Behauptung als unwahrscheinlich angesehen.[3] Möglicherweise bezog sich GOLOVKO auf einen anderen Spruch DÖNITZ' in einem Marine-Handschlüssel einige Tage nach dem Spruch an die „Scharnhorst“. BEESLY vermutet, dass die sowjetische Marine am 30.7.1944 aus dem versenkten U 250 eine ENIGMA geborgen haben könnten.[4] Möglicherweise sind die Sprüche der Reichsbahn (steckerlose ENIGMA) gelesen worden, möglicherweise auch Sprüche des Marine–Kommandos Süd (Mittelmeer, Balkan und Schwarzes Meer). Letzterer Schlüsselbereich soll nach HINSLEY ein relativ unkompliziertes Vorkriegsmodell der Chiffriermaschine verwendet haben, dessen Sprüche ohne besondere Schwierigkeiten zu lesen gewesen wären[5], dazu ein sehr einfaches Chiffrierverfahren (Siehe Kap. 1.1). In diesem Zusammenhang muss auf die sowjetischen Agenten CAIRNCROSS, BARON (Deckname) hingewiesen werden, die in BP gearbeitet haben. In Arlington Hall war WEISBAND als sowjetischer Agent tätig gewesen. Es könnte durchaus sein, dass sie neben anderen Erkenntnissen von BP den Sowjets auch über Dechiffrierungsmethoden berichtet haben.[6]

[1] GLANTZ, b), S. 230
[2] GOLOVKO, S. 189
[3] JUKES a); JUKES b); MILNER-BARRY; ERSKINE e); ERSKINE f)
[4] BEESLY b), S. 94
[5] HINSLEY II, S. 28
[6] ERSKINE c), S. 185

Kapitel 8

Schluss

Aus den vorangegangenen Fakten geht hervor, wie die geschickte, alle Quellen der Information zusammenfassende Organisation der Alliierten tiefen Einblick in die Struktur und Absichten ihres Gegners gewinnen half, allerdings unterstützt durch z.T. (im Nachhinein unverständliche) Fehler beim Entwurf bzw. bei Änderungen der deutschen Chiffriersysteme, verbunden mit dem unverbrüchlichen Glauben an die unantastbare Sicherheit der deutschen Schlüssel trotz immer wieder aufgetretener Zweifelsanlässe. Dies ist ein Beispiel, wie geheime Systeme nicht gehandhabt werden sollten. Es wird auch deutlich, wie scheinbare Verbesserungen der Sicherheit eines Systems tatsächlich den Einbruch in das System begünstigen können. Für 30 Jahre unterlag alles mit Bletchley Park Zusammenhängende einer strengen Geheimhaltung, einige Akten dürfen sogar erst etwa 2015 der Öffentlichkeit zugänglich gemacht werden. Es ist daher verständlich, dass die inzwischen angewachsene Menge der Veröffentlichungen zu diesem Thema nur jeweils Erinnerungsbruchstücke mit begrenzten Erfahrungen der Zusammenhänge darstellen kann (wobei natürlich die noch geheimen Inhalte ausgespart bleiben). Da inzwischen auch ein Teil der Akteure gestorben ist, ist das heutige Bild notwendig an einigen Stellen kursorisch oder lückenhaft geblieben. Eine ausführliche, aus den Akten kompilierte Darstellung der gesamten britischen nachrichtendienstlichen Szene, in der auch die Bedeutung des Lesens der ENIGMA - Sprüche deutlich wird, hat HINSLEY geliefert. Den ersten und entscheidenden Schritt zur Dechiffrierung der ENIGMA hat der polnische militärische Nachrichtendienst bereits 1932 getan: Die Rekonstruktion der Chiffriermaschine. Diese Leistung geht allein auf einen Mann zurück: Marian REJEWSKI. Dieser Mathematiker, er war seinerzeit 27 Jahre alt, hat später seine mathematischen Überlegungen in verschiedenen Veröffentlichungen bekanntgemacht, wobei allerdings beim Vergleich der einzelnen Quellen Unstimmigkeiten zu beobachten sind. Dies dürfte darauf zurückzuführen sein, dass REJEWSKI nur auf sein Gedächtnis nach über 40 Jahren zurückgreifen konnte. Trotzdem kann gesagt werden, dass ohne die polnischen Erfolge vor 1939 für die Briten der „fliegende Start“ bei Kriegsbeginn und die weiteren grossen Erfolge nicht möglich gewesen wären. Gelang es doch in der Zeit von Mitte 1941 bis Januar 1945, allein von der Marine 324000 Sprüche zu entziffern, so viele sind jedenfalls im Public Record Office registriert.[1] Das Gewicht der gewonnenen Erkenntnis ergab sich natürlich erst nach dem Lesen. Zwei Beispiele mögen das am Ende illustrieren:

1) 21. Januar 1942, Reichsmarschallbefehl: Der Reichsmarschall befiehlt, dass alle Offiziere, Unteroffiziere und Mannschaften der Luftwaffe, die zum Führer oder zum Reichsmarschall befohlen werden, ..., auf alle Fälle frei von Läusen sein müssen.[2]

2) Der Befehl an die VII. Armee und den General der Panzertruppen Eberbach vom

[1] CALVOCORESSI, S. 96
[2] KESARIS, S. 3

9.8.1944, 18.00 Uhr, den Angriff auf Mortain wieder aufzunehmen. Die Kenntnis dieses Befehls stammt vom 10.8., 3.49 Uhr, der Angriff wurde für den 11.8. vermutet. Das Dokument trägt die Nummer XL 5461 im Public Record Office.[3]

Die Chiffriermaschine wäre einem unberechtigten Dechiffrierungsversuch gegenüber wesentlich widerstandsfähiger gewesen, wenn nicht viele Fehler ihre Wirksamkeit und Sicherheit vermindert hätten. WELCHMAN schrieb 1982:

> *...the [Enigma] machine as it was would have been impregnable if it had been used properly.*[4]

Dieses Urteil wiegt besonders schwer, als es sich bei WELCHMAN um einen der kompetentesten Kryptologen in BP handelte.

Ein Fehler war z.B., dass nicht alle Walzen mehr Kerben zum Weiterschalten und bei allen Walzen in gleicher Anzahl unf Lage gehabt hätten. Auch, dass die steckerbare Umkehrwalze in der Marine M 4 nicht zum Einsatz kam, muss als Fehler gerechnet werden.
Beim Gebrauch war es den alliierten Diensten anfangs eine Hilfe, dass niemals ein Buchstabe an zwei aufeinander folgenden Tagen gesteckert war. Waren die Buchstaben eines Tages bekannt, war die Auswahl für den nächsten Tag eingeschränkt. Als später die Anzahl der Stecker mit 10 Paaren festgehalten wurde, führte das immer zu 6 ungesteckerten Buchstaben. Da i.a. nicht zwei benachbarte Buchstaben in einem Steckerpaar auftreten durften, war die Anzahl der Möglichkeiten weiter eingeschränkt. Eine Variation der Anzahl der gesteckerten Buchstaben, wie sie beim Heer vorübergehend in Gebrauch war, hätte die jeweils gegebene Anzahl der Möglichkeiten der Steckerung vermindert. Weiter führte die Beschränkung der Auswahl der Walzen bei den zwei Tage gültigen Chiffrierprotokollen der Marine dazu bei, dass statt 336 Walzenlagen nur wesentlich weniger zu überprüfen waren.

Leider ist die Stereotypie, die Todsünde der Kryptographie, viel zu häufig aufgetreten (Beispiele in Kap.6.2.3.1.1). Durch die Gleichheit von Formulierungen einerseits und ihrer Stellung in den Sprüchen andererseits ist dem Einbruch in die Sprüche Vorschub geleistet worden. Dazu gehört auch die Masse der Spruchwiederholungen in verschiedenen Schlüsseln, ohne Paraphrasierungen, die notwendig gewesen wäre. Ein einfaches Mittel wäre z.B. gewesen, die Spruchanfänge jeweils an verschiedene Stellen des Spruches selbst zu legen. Weiter haben Vorlieben des Funkpersonals für gewisse Schlüsselbuchstabenfolgen, wenn sie durch genaue Statistik der Dechiffrierer aufgedeckt werden konnten, die Sicherheit ders Systems geschwächt.
Alle starren Regeln, z.B. dass ein Schlüssel nie zwei gleiche Buchstaben enthalten dürfte,haben gerade durch diese Beschränkung den Einbruch in den Schlüssel erleichtert.

Schliesslich muss noch der Vorwurf erhoben werden, dass fast alle Veränderungen des Chiffriersystems nur häppchenweise erfolgten und nicht mehrere Änderungen zum gleichen Zeitpunkt. So, wie es geschehen ist, konnte jeweils auf genügend viel alte Struktur zurückgegriffen werden, um die Veränderung zu identifizieren und unwirksam werden zu lassen.

In diesen Zusammenhang gehört auch, dass zeitweise Schlüssel eines Schlüsselkreises später in einem anderen ungeändert wiederholt wurden. So war z.B. in einem Monat (1942 ?) der Schlüssel «Scorpion II» die Wiederholung des Schlüssels «Primrose» vom Vormonat[5]. Wenn also der erste Tag des Monats in «Scorpion»gebrochen war, waren die Tagesschlüssel für den Rest des Monats bekannt. Zumindest fahrlässig war es,

[3] BENNETT b)
[4] nach BAUER, pers. Mitteilung
[5] Mndl. Mitteilung von R. ERSKINE

im Dezember 1944 den Kanalfestungen im Schlüssel „Hydra I“ in einem Spruch zu übermitteln, wie aus dem Schlüssel für November die für die nächsten drei Monate zu konstruieren wären.

Weiter ist es unverständlich, dass nach mehreren Verdachtsfällen und der folgenden Meldung aus der Schweiz[6] keine Reaktion erfolgte zur vollständigen Verbesserung des Chiffriersystems:

> *Am 10.8 ging folgende Meldung über KO[7] Schweiz ein:*
> *Seit einigen Monaten Entzifferung deutschen Marinecodes hinsichtlich Befehlen an operierende U-Boote geglückt. Alle Befehle werden mitgelesen.*
> *Zusatz: Quelle Amerika–Schweizer in hoher Sekretärstellung in USA–Marine–Ministerium.*

In mehreren Konferenzen zur Überprüfung von beunruhigenden Übereinstimmungen entzifferter englischer Lagemeldungen über deutsche U-Boote und der tatsächlichen Lage wurde jedoch immer wieder „bewiesen“, dass die Alliierten keinesfalls in der Lage sein könnten, das Chiffriersystem der U-Boote zu brechen[8]. Dabei war die deutsche Seite durchaus im Bilde über z.B. anzuwendende IBM-Methoden. Schon 1943 wurde festgestellt, dass mit einem passenden Klartext die Einstellung einer ENIGMA mit Steckern gefunden werden könnte. 1944 hat ein Lt. FROWEIN von der Abteilung Schlüsselsicherheit des Oberbefehlshabers der Marine eine Methode entwickelt, mit etwa 70000 IBM-Karten einen Katalog von Rotor-Transformationen zu erstellen, mit dem es möglich war, Klartext zu chiffrieren, ihn mit Geheimtext abzugleichen und auf logische Widersprüche zu untersuchen. Das war schon eine Art «Scritching», wie es Arlington Hall in den U.S.A. für die Sprüche des Heeres entwickelte[9].

---

[6] KTB des BdU vom 13.8.1943; SMITH/ERSKINE, S.375

[7] KO: „Kriegsorganisation“, d.h. Abwehr.

[8] Operative Geheimhaltung im U-Bootskrieg Jan. 1943, BA/MA RM7/107 und NARA Dokument Box CBCB43, Nr. 908«German Naval Enigma Machine»

[9] BUDIANSKI, S. 335

Anhang A

Matrizen

Anwendung der Matrizen der Tabellen A.1 bis A.6:

Version A:

Unter der Walzenstellung (Kopfleiste) vom Buchstaben der rechten Eingangsseite der Walze im Matrixfeld nach links gibt der Zeilenbuchstabe den linken Ausgang aus der Walze. Umgekehrt: Den linken Eingangsbuchstaben als Zeilenbuchstaben gewählt liefert unter der Walzenstellung (Kopfleiste) im Matrixfeld den rechten Ausgangsbuchstaben der Walze.

Bei Version B ist das Zuordnungsverfahren umgekehrt.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	U	V	W	D	W	Y	Z	I	N	Q	R	T	Q	X	Y	E	R	G	A	S	X	N	R	T	Q	K
B	W	X	E	X	Z	A	J	O	R	S	U	R	Y	Z	F	S	H	B	T	Y	O	S	U	R	L	V
C	Y	F	Y	A	B	K	P	S	T	V	S	Z	A	G	T	I	C	U	Z	P	T	V	S	M	W	X
D	G	Z	B	C	L	Q	T	U	W	T	A	B	H	U	J	D	V	A	Q	U	W	T	N	X	Y	Z
E	A	C	D	M	R	U	V	X	U	B	C	I	V	K	E	W	B	R	V	X	U	O	Y	Z	A	H
F	D	E	N	S	V	W	Y	V	C	D	J	W	L	F	X	C	S	W	Y	V	P	Z	A	B	I	B
G	F	O	T	W	X	Z	W	D	E	K	X	M	G	Y	D	T	X	Z	W	Q	A	B	C	J	C	E
H	P	U	X	Y	A	X	E	F	L	Y	N	H	Z	E	U	Y	A	X	R	B	C	D	K	D	F	G
I	V	Y	Z	B	Y	F	G	M	Z	O	I	A	F	V	Z	B	Y	S	C	D	E	L	E	G	H	Q
J	Z	A	C	Z	G	H	N	A	P	J	B	G	W	A	C	Z	T	D	E	F	M	F	H	I	R	W
K	B	D	A	H	I	O	B	Q	K	C	H	X	B	D	A	U	E	F	G	N	G	I	J	S	X	A
L	E	B	I	J	P	C	R	L	D	I	Y	C	E	B	V	F	G	H	O	H	J	K	T	Y	B	C
M	C	J	K	Q	D	S	M	E	J	Z	D	F	C	W	G	H	I	P	I	K	L	U	Z	C	D	F
N	K	L	R	E	T	N	F	K	A	E	G	D	X	H	I	J	Q	J	L	M	V	A	D	E	G	D
O	M	S	F	U	O	G	L	B	F	H	E	Y	I	J	K	R	K	M	N	W	B	E	F	H	E	L
P	T	G	V	P	H	M	C	G	I	F	Z	J	K	L	S	L	N	O	X	C	F	G	I	F	M	N
Q	H	W	Q	I	N	D	H	J	G	A	K	L	M	T	M	O	P	Y	D	G	H	J	G	N	O	U
R	X	R	J	O	E	I	K	H	B	L	M	N	U	N	P	Q	Z	E	H	I	K	H	O	P	V	I
S	S	K	P	F	J	L	I	C	M	N	O	V	O	Q	R	A	F	I	J	L	I	P	Q	W	J	Y
T	L	Q	G	K	M	J	D	N	O	P	W	P	R	S	B	G	J	K	M	J	Q	R	X	K	Z	T
U	R	H	L	N	K	E	O	P	Q	X	Q	S	T	C	H	K	L	N	K	R	S	Y	L	A	U	M
V	I	M	O	L	F	P	Q	R	Y	R	T	U	D	I	L	M	O	L	S	T	Z	M	B	V	N	S
W	N	P	M	G	Q	R	S	Z	S	U	V	E	J	M	N	P	M	T	U	A	N	C	W	O	T	J
X	Q	N	H	R	S	T	A	T	V	W	F	K	N	O	Q	N	U	V	B	O	D	X	P	U	K	O
Y	O	I	S	T	U	B	U	W	X	G	L	O	P	R	O	V	W	C	P	E	Y	Q	V	L	P	R
Z	J	T	U	V	C	V	X	Y	H	M	P	Q	S	P	W	X	D	Q	F	Z	R	W	M	Q	S	P

Tabelle A.1: Walze I, A

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	E	J	K	C	H	B	X	J	N	Q	D	I	C	J	K	S	H	D	A	W	G	N	F	U	E	K
B	K	L	D	I	C	Y	K	O	R	E	J	D	K	L	T	I	E	B	X	H	O	G	V	F	L	F
C	M	E	J	D	Z	L	P	S	F	K	E	L	M	U	J	F	C	Y	I	P	H	W	G	M	G	L
D	F	K	E	A	M	Q	T	G	L	F	M	N	V	K	G	D	Z	J	Q	I	X	H	N	H	M	N
E	L	F	B	N	R	U	H	M	G	N	O	W	L	H	E	A	K	R	J	Y	I	O	I	N	O	G
F	G	C	O	S	V	I	N	H	O	P	X	M	I	F	B	L	S	K	Z	J	P	J	O	P	H	M
G	D	P	T	W	J	O	I	P	Q	Y	N	J	G	C	M	T	L	A	K	Q	K	P	Q	I	N	H
H	Q	U	X	K	P	J	Q	R	Z	O	K	H	D	N	U	M	B	L	R	L	Q	R	J	O	I	E
I	V	Y	L	Q	K	R	S	A	P	L	I	E	O	V	N	C	M	S	M	R	S	K	P	J	F	R
J	Z	M	R	L	S	T	B	Q	M	J	F	P	W	O	D	N	T	N	S	T	L	Q	K	G	S	W
K	N	S	M	T	U	C	R	N	K	G	Q	X	P	E	O	U	O	T	U	M	R	L	H	T	X	A
L	T	N	U	V	D	S	O	L	H	R	Y	Q	F	P	V	P	U	V	N	S	M	I	U	Y	B	O
M	O	V	W	E	T	P	M	I	S	Z	R	G	Q	W	Q	V	W	O	T	N	J	V	Z	C	P	U
N	W	X	F	U	Q	N	J	T	A	S	H	R	X	R	W	X	P	U	O	K	W	A	D	Q	V	P
O	Y	G	V	R	O	K	U	B	T	I	S	Y	S	X	Y	Q	V	P	L	X	B	E	R	W	Q	X
P	H	W	S	P	L	V	C	U	J	T	Z	T	Y	Z	R	W	Q	M	Y	C	F	S	X	R	Y	Z
Q	X	T	Q	M	W	D	V	K	U	A	U	Z	A	S	X	R	N	Z	D	G	T	Y	S	Z	A	I
R	U	R	N	X	E	W	L	V	B	V	A	B	T	Y	S	O	A	E	H	U	Z	T	A	B	J	Y
S	S	O	Y	F	X	M	W	C	W	B	C	U	Z	T	P	B	F	I	V	A	U	B	C	K	Z	V
T	P	Z	G	Y	N	X	D	X	C	D	V	A	U	Q	C	G	J	W	B	V	C	D	L	A	W	T
U	A	H	Z	O	Y	E	Y	D	E	W	B	V	R	D	H	K	X	C	W	D	E	M	B	X	U	Q
V	I	A	P	Z	F	Z	E	F	X	C	W	S	E	I	L	Y	D	X	E	F	N	C	Y	V	R	B
W	B	Q	A	G	A	F	G	Y	D	X	T	F	J	M	Z	E	Y	F	G	O	D	Z	W	S	C	J
X	R	B	H	B	G	H	Z	E	Y	U	G	K	N	A	F	Z	G	H	P	E	A	X	T	D	K	C
Y	C	I	C	H	I	A	F	Z	V	H	L	O	B	G	A	H	I	Q	F	B	Y	U	E	L	D	S
Z	J	D	I	J	B	G	A	W	I	M	P	C	H	B	I	J	R	G	C	Z	V	F	M	E	T	D

Tabelle A.2: Walze I, B

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	I	N	Z	V	R	L	E	X	S	T	Z	C	G	K	F	A	P	M	U	N	C	Q	L	X	T
B	J	O	A	W	S	M	F	Y	T	U	A	D	H	L	G	B	Q	N	V	O	D	R	M	Y	U	B
C	P	B	X	T	N	G	Z	U	V	B	E	I	M	H	C	R	O	W	P	E	S	N	Z	V	C	K
D	C	Y	U	O	H	A	V	W	C	F	J	N	I	D	S	P	X	Q	F	T	O	A	W	D	L	Q
E	Z	V	P	I	B	W	X	D	G	K	O	J	E	T	Q	Y	R	G	U	P	B	X	E	M	R	D
F	W	Q	J	C	X	Y	E	H	L	P	K	F	U	R	Z	S	H	V	Q	C	Y	F	N	S	E	A
G	R	K	D	Y	Z	F	I	M	Q	L	G	V	S	A	T	I	W	R	D	Z	G	O	T	F	B	X
H	L	E	Z	A	G	J	N	R	M	H	W	T	B	U	J	X	S	E	A	H	P	U	G	C	Y	S
I	F	A	B	H	K	O	S	N	I	X	U	C	V	K	Y	T	F	B	I	Q	V	H	D	Z	T	M
J	B	C	I	L	P	T	O	J	Y	V	D	W	L	Z	U	G	C	J	R	W	I	E	A	U	N	G
K	D	J	M	Q	U	P	K	Z	W	E	X	M	A	V	H	D	K	S	X	J	F	B	V	O	H	C
L	K	N	R	V	Q	L	A	X	F	Y	N	B	W	I	E	L	T	Y	K	G	C	W	P	I	D	E
M	O	S	W	R	M	B	Y	G	Z	O	C	X	J	F	M	U	Z	L	H	D	X	Q	J	E	F	L
N	T	X	S	N	C	Z	H	A	P	D	Y	K	G	N	V	A	M	I	E	Y	R	K	F	G	M	P
O	Y	T	O	D	A	I	B	Q	E	Z	L	H	O	W	B	N	J	F	Z	S	L	G	H	N	Q	U
P	U	P	E	B	J	C	R	F	A	M	I	P	X	C	O	K	G	A	T	M	H	I	O	R	V	Z
Q	Q	F	C	K	D	S	G	B	N	J	Q	Y	D	P	L	H	B	U	N	I	J	P	S	W	A	V
R	G	D	L	E	T	H	C	O	K	R	Z	E	Q	M	I	C	V	O	J	K	Q	T	X	B	W	R
S	E	M	F	U	I	D	P	L	S	A	F	R	N	J	D	W	P	K	L	R	U	Y	C	X	S	H
T	N	G	V	J	E	Q	M	T	B	G	S	O	K	E	X	Q	L	M	S	V	Z	D	Y	T	I	F
U	H	W	K	F	R	N	U	C	H	T	P	L	F	Y	R	M	N	T	W	A	E	Z	U	J	G	O
V	X	L	G	S	O	V	D	I	U	Q	M	G	Z	S	N	O	U	X	B	F	A	V	K	H	P	I
W	M	H	T	P	W	E	J	V	R	N	H	A	T	O	P	V	Y	C	G	B	W	L	I	Q	J	Y
X	I	U	Q	X	F	K	W	S	O	I	B	U	P	Q	W	Z	D	H	C	X	M	J	R	K	Z	N
Y	V	R	Y	G	L	X	T	P	J	C	V	Q	R	X	A	E	I	D	Y	N	K	S	L	A	O	J
Z	S	Z	H	M	Y	U	Q	K	D	W	R	S	Y	B	F	J	E	Z	O	L	T	M	B	P	K	W

Tabelle A.3: Walze II, A

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	I	B	H	O	D	L	N	P	S	B	W	K	G	Y	N	A	P	H	U	V	D	J	Y	Q	F
B	J	C	I	P	E	M	O	Q	T	C	X	L	H	Z	O	B	Q	I	V	W	E	K	Z	R	G	B
C	D	J	Q	F	N	P	R	U	D	Y	M	I	A	P	R	C	J	W	X	F	L	A	S	H	C	K
D	K	R	G	O	Q	S	V	E	Z	N	J	B	Q	D	S	K	X	Y	G	M	B	T	I	D	L	E
E	S	H	P	R	T	W	F	A	O	K	C	R	E	T	L	Y	Z	H	N	C	U	J	E	M	F	L
F	I	Q	S	U	X	G	B	P	L	D	S	F	U	M	Z	A	I	O	D	V	K	F	N	G	M	T
G	R	T	V	Y	H	C	Q	M	E	T	G	V	N	A	B	J	P	E	W	L	G	O	H	N	U	J
H	U	W	Z	I	D	R	N	F	U	H	W	O	B	C	K	Q	F	X	M	H	P	I	O	V	K	S
I	X	A	J	E	S	O	G	V	I	X	P	C	D	L	R	G	Y	N	I	Q	J	P	W	L	T	V
J	B	K	F	T	P	H	W	J	Y	Q	D	E	M	S	H	Z	O	J	R	K	Q	X	M	U	W	Y
K	L	G	U	Q	I	X	K	Z	R	E	F	N	T	I	A	P	K	S	L	R	Y	N	V	X	Z	C
L	H	V	R	J	Y	L	A	S	F	G	O	U	J	B	Q	L	T	M	S	Z	O	W	Y	A	D	M
M	W	S	K	Z	M	B	T	G	H	P	V	K	C	R	M	U	N	T	A	P	X	Z	B	E	N	I
N	T	L	A	N	C	U	H	I	Q	W	L	D	S	N	V	O	U	B	Q	Y	A	C	F	O	J	X
O	M	B	O	D	V	I	J	R	X	M	E	T	O	W	P	V	C	R	Z	B	D	G	P	K	Y	U
P	C	P	E	W	J	K	S	Y	N	F	U	P	X	Q	W	D	S	A	C	E	H	Q	L	Z	V	N
Q	Q	F	X	K	L	T	Z	O	G	V	Q	Y	R	X	E	T	B	D	F	I	R	M	A	W	O	D
R	G	Y	L	M	U	A	P	H	W	R	Z	S	Y	F	U	C	E	G	J	S	N	B	X	P	E	R
S	Z	M	N	V	B	Q	I	X	S	A	T	Z	G	V	D	F	H	K	T	O	C	Y	Q	F	S	H
T	N	O	W	C	R	J	Y	T	B	U	A	H	W	E	G	I	L	U	P	D	Z	R	G	T	I	A
U	P	X	D	S	K	Z	U	C	V	B	I	X	F	H	J	M	V	Q	E	A	S	H	U	J	B	O
V	Y	E	T	L	A	V	D	W	C	J	Y	G	I	K	N	W	R	F	B	T	I	V	K	C	P	Q
W	F	U	M	B	W	E	X	D	K	Z	H	J	L	O	X	S	G	C	U	J	W	L	D	Q	R	Z
X	V	N	C	X	F	Y	E	L	A	I	K	M	P	Y	T	H	D	V	K	X	M	E	R	S	A	G
Y	O	D	Y	G	Z	F	M	B	J	L	N	Q	Z	U	I	E	W	L	Y	N	F	S	T	B	H	W
Z	E	Z	H	A	G	N	C	K	M	O	R	A	V	J	F	X	M	Z	O	G	T	U	C	I	X	P

Tabelle A.4: Walze II, B

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	T	Z	E	Y	L	X	M	W	I	V	K	U	J	A	L	S	I	R	F	Q	C	Q	V	N	Q	N
B	A	F	Z	M	Y	N	X	J	W	L	V	K	B	M	T	J	S	G	R	D	R	W	O	R	O	U
C	G	A	N	Z	O	Y	K	X	M	W	L	C	N	U	K	T	H	S	E	S	X	P	S	P	V	B
D	B	O	A	P	Z	L	Y	N	X	M	D	O	V	L	U	I	T	F	T	Y	Q	T	Q	W	C	H
E	P	B	Q	A	M	Z	O	Y	N	E	P	W	M	V	J	U	G	U	Z	R	U	R	X	D	I	C
F	C	R	B	N	A	P	Z	O	F	Q	X	N	W	K	V	H	V	A	S	V	S	Y	E	J	D	Q
G	S	C	O	B	Q	A	P	G	R	Y	O	X	L	W	I	W	B	T	W	T	Z	F	K	E	R	D
H	D	P	C	R	B	Q	H	S	Z	P	Y	M	X	J	X	C	U	X	U	A	G	L	F	S	E	T
I	Q	D	S	C	R	I	T	A	Q	Z	N	Y	K	Y	D	V	Y	V	B	H	M	G	T	F	U	E
J	E	T	D	S	J	U	B	R	A	O	Z	L	Z	E	W	Z	W	C	I	N	H	U	G	V	F	R
K	U	E	T	K	V	C	S	B	P	A	M	A	F	X	A	X	D	J	O	I	V	H	W	G	S	F
L	F	U	L	W	D	T	C	Q	B	N	B	G	Y	B	Y	E	K	P	J	W	I	X	H	T	G	V
M	V	M	X	E	U	D	R	C	O	C	H	Z	C	Z	F	L	Q	K	X	J	Y	I	U	H	W	G
N	N	Y	V	F	E	S	D	P	D	I	A	D	A	G	M	R	L	Y	K	Z	J	V	I	X	H	W
O	Z	G	W	F	T	E	Q	E	J	B	E	B	H	N	S	M	Z	L	A	K	W	J	Y	I	X	O
P	H	X	G	U	F	R	F	K	C	F	C	I	O	T	N	A	M	B	L	X	K	Z	J	Y	P	A
Q	Y	H	V	G	S	G	L	D	G	D	J	P	U	O	B	N	C	M	Y	L	A	K	Z	Q	B	I
R	I	W	H	T	H	M	E	H	E	K	Q	V	P	C	O	D	N	Z	M	B	L	A	R	C	J	Z
S	X	I	U	I	N	F	I	F	L	R	W	Q	D	P	E	O	A	N	C	M	B	S	D	K	A	J
T	J	V	J	O	G	J	G	M	S	X	R	E	Q	F	P	B	O	D	N	C	T	E	L	B	K	Y
U	W	K	P	H	K	H	N	T	Y	S	F	R	G	Q	C	P	E	O	D	U	F	M	C	L	Z	K
V	L	Q	I	L	I	O	U	Z	T	G	S	H	R	D	Q	F	P	E	V	G	N	D	M	A	L	X
W	R	J	M	J	P	V	A	U	H	T	I	S	E	R	G	Q	F	W	H	O	E	N	B	M	Y	M
X	K	N	K	Q	W	B	V	I	U	J	T	F	S	H	R	G	X	I	P	F	O	C	N	Z	N	S
Y	O	L	R	X	C	W	J	V	K	U	G	T	I	S	H	Y	J	Q	G	P	D	O	A	O	T	L
Z	M	S	Y	D	X	K	W	L	V	H	U	J	T	I	Z	K	R	H	Q	E	P	B	P	U	M	P

Tabelle A.5: Walze III, A

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	W	I	J	K	N	K	N	A	K	P	S	F	O	H	Q	R	Y	V	S	P
B	D	E	F	G	H	X	J	K	L	O	L	O	B	L	Q	T	G	P	I	R	S	Z	W	T	Q	C
C	F	G	H	I	Y	K	L	M	P	M	P	C	M	R	U	H	Q	J	S	T	A	X	U	R	D	E
D	H	I	J	Z	L	M	N	Q	N	Q	D	N	S	V	I	R	K	T	U	B	Y	V	S	E	F	G
E	J	K	A	M	N	O	R	O	R	E	O	T	W	J	S	L	U	V	C	Z	W	T	F	G	H	I
F	L	B	N	O	P	S	P	S	F	P	U	X	K	T	M	V	W	D	A	X	U	G	H	I	J	K
G	C	O	P	Q	T	Q	T	G	Q	V	Y	L	U	N	W	X	E	B	Y	V	H	I	J	K	L	M
H	P	Q	R	U	R	U	H	R	W	Z	M	V	O	X	Y	F	C	Z	W	I	J	K	L	M	N	D
I	R	S	V	S	V	I	S	X	A	N	W	P	Y	Z	G	D	A	X	J	K	L	M	N	O	E	Q
J	T	W	T	W	J	T	Y	B	O	X	Q	Z	A	H	E	B	Y	K	L	M	N	O	P	F	R	S
K	X	U	X	K	U	Z	C	P	Y	R	A	B	I	F	C	Z	L	M	N	O	P	Q	G	S	T	U
L	V	Y	L	V	A	D	Q	Z	S	B	C	J	G	D	A	M	N	O	P	Q	R	H	T	U	V	Y
M	Z	M	W	B	E	R	A	T	C	D	K	H	E	B	N	O	P	Q	R	S	I	U	V	W	Z	W
N	N	X	C	F	S	B	U	D	E	L	I	F	C	O	P	Q	R	S	T	J	V	W	X	A	X	A
O	Y	D	G	T	C	V	E	F	M	J	G	D	P	Q	R	S	T	U	K	W	X	Y	B	Y	B	O
P	E	H	U	D	W	F	G	N	K	H	E	Q	R	S	T	U	V	L	X	Y	Z	C	Z	C	P	Z
Q	I	V	E	X	G	H	O	L	I	F	R	S	T	U	V	W	M	Y	Z	A	D	A	D	Q	A	F
R	W	F	Y	H	I	P	M	J	G	S	T	U	V	W	X	N	Z	A	B	E	B	E	R	B	G	J
S	G	Z	I	J	Q	N	K	H	T	U	V	W	X	Y	O	A	B	C	F	C	F	S	C	H	K	X
T	A	J	K	R	O	L	I	U	V	W	X	Y	Z	P	B	C	D	G	D	G	T	D	I	L	Y	H
U	K	L	S	P	M	J	V	W	X	Y	Z	A	Q	C	D	E	H	E	H	U	E	J	M	Z	I	B
V	M	T	Q	N	K	W	X	Y	Z	A	B	R	D	E	F	I	F	I	V	F	K	N	A	J	C	L
W	U	R	O	L	X	Y	Z	A	B	C	S	E	F	G	J	G	J	W	G	L	O	B	K	D	M	N
X	S	P	M	Y	Z	A	B	C	D	T	F	G	H	K	H	K	X	H	M	P	C	L	E	N	O	V
Y	Q	N	Z	A	B	C	D	E	U	G	H	I	L	I	L	Y	I	N	Q	D	M	F	O	P	W	T
Z	O	A	B	C	D	E	F	V	H	I	J	M	J	M	Z	J	O	R	E	N	G	P	Q	X	U	R

Tabelle A.6: Walze III, B

Verdrahtung der schnellen Walze auf Grund der Untersuchung der Indikatoren.
Walzenanordnung: 321; Ringstellung: AAA; Grundstellung AAA.

Basis		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	:	A	G	I	B	H	C	Z	M	R	V	J	P	K	S	U	D	T	Q	O	L	W	E	X	N	Y	F
2	:	B	H	J	C	I	D	A	N	S	W	K	Q	L	T	V	E	U	R	P	M	X	F	Y	O	Z	G
3	:	C	I	K	D	J	E	B	O	T	X	L	R	M	U	W	F	V	S	Q	N	Y	G	Z	P	A	H
4	:	D	J	L	E	K	F	C	P	U	Y	M	S	N	V	X	G	W	T	R	O	Z	H	A	Q	B	I
5	:	E	K	M	F	L	G	D	Q	V	Z	N	T	O	W	Y	H	X	U	S	P	A	I	B	R	C	J
6	:	F	L	N	G	M	H	E	R	W	A	O	U	P	X	Z	I	Y	V	T	Q	B	J	C	S	D	K
7	:	G	M	O	H	N	I	F	S	X	B	P	V	Q	Y	A	J	Z	W	U	R	C	K	D	T	E	L
8	:	H	N	P	I	O	J	G	T	Y	C	Q	W	R	Z	B	K	A	X	V	S	D	L	E	U	F	M
9	:	I	O	Q	J	P	K	H	U	Z	D	R	X	S	A	C	L	B	Y	W	T	E	M	F	V	G	N
10	:	J	P	R	K	Q	L	I	V	A	E	S	Y	T	B	D	M	C	Z	X	U	F	N	G	W	H	O
11	:	K	Q	S	L	R	M	J	W	B	F	T	Z	U	C	E	N	D	A	Y	V	G	O	H	X	I	P
12	:	L	R	T	M	S	N	K	X	C	G	U	A	V	D	F	O	E	B	Z	W	H	P	I	Y	J	Q
13	:	M	S	U	N	T	O	L	Y	D	H	V	B	W	E	G	P	F	C	A	X	I	Q	J	Z	K	R
14	:	N	T	V	O	U	P	M	Z	E	I	W	C	X	F	H	Q	G	D	B	Y	J	R	K	A	L	S
15	:	O	U	W	P	V	Q	N	A	F	J	X	D	Y	G	I	R	H	E	C	Z	K	S	L	B	M	T
16	:	P	V	X	Q	W	R	O	B	G	K	Y	E	Z	H	J	S	I	F	D	A	L	T	M	C	N	U
17	:	Q	W	Y	R	X	S	P	C	H	L	Z	F	A	I	K	T	J	G	E	B	M	U	N	D	O	V
18	:	R	X	Z	S	Y	T	Q	D	I	M	A	G	B	J	L	U	K	H	F	C	N	V	O	E	P	W
19	:	S	Y	A	T	Z	U	R	E	J	N	B	H	C	K	M	V	L	I	G	D	O	W	P	F	Q	X
20	:	T	Z	B	U	A	V	S	F	K	O	C	I	D	L	N	W	M	J	H	E	P	X	Q	G	R	Y
21	:	U	A	C	V	B	W	T	G	L	P	D	J	E	M	O	X	N	K	I	F	Q	Y	R	H	S	Z
22	:	V	B	D	W	C	X	U	H	M	Q	E	K	F	N	P	Y	O	L	J	G	R	Z	S	I	T	A
23	:	W	C	E	X	D	Y	V	I	N	R	F	L	G	O	Q	Z	P	M	K	H	S	A	T	J	U	B
24	:	X	D	F	Y	E	Z	W	J	O	S	G	M	H	P	R	A	Q	N	L	I	T	B	U	K	V	C
25	:	Y	E	G	Z	F	A	X	K	P	T	H	N	I	Q	S	B	R	O	M	J	U	C	V	L	W	D
26	:	Z	F	H	A	G	B	Y	L	Q	U	I	O	J	R	T	C	S	P	N	K	V	D	W	M	X	E

Quelle: $H =$ (A D F P V Z B E C K M T H X S L R I N Q O J U W Y G)

Tabelle A.7:

Verdrahtung der schnellen Walze auf Grund der Untersuchung der Indikatoren.
Walzenanordnung: 321; Ringstellung: AAA; Grundstellung AAC.

Basis		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	:	A	T	Z	U	R	E	J	N	B	H	C	K	M	V	L	I	G	D	O	W	P	F	Q	X	S	Y
2	:	B	U	A	V	S	F	K	O	C	I	D	L	N	W	M	J	H	E	P	X	Q	G	R	Y	T	Z
3	:	C	V	B	W	T	G	L	P	D	J	E	M	O	X	N	K	I	F	Q	Y	R	H	S	Z	U	A
4	:	D	W	C	X	U	H	M	Q	E	K	F	N	P	Y	O	L	J	G	R	Z	S	I	T	A	V	B
5	:	E	X	D	Y	V	I	N	R	F	L	G	O	Q	Z	P	M	K	H	S	A	T	J	U	B	W	C
6	:	F	Y	E	Z	W	J	O	S	G	M	H	P	R	A	Q	N	L	I	T	B	U	K	V	C	X	D
7	:	G	Z	F	A	X	K	P	T	H	N	I	Q	S	B	R	O	M	J	U	C	V	L	W	D	Y	E
8	:	H	A	G	B	Y	L	Q	U	I	O	J	R	T	C	S	P	N	K	V	D	W	M	X	E	Z	F
9	:	I	B	H	C	Z	M	R	V	J	P	K	S	U	D	T	Q	O	L	W	E	X	N	Y	F	A	G
10	:	J	C	I	D	A	N	S	W	K	Q	L	T	V	E	U	R	P	M	X	F	Y	O	Z	G	B	H
11	:	K	D	J	E	B	O	T	X	L	R	M	U	W	F	V	S	Q	N	Y	G	Z	P	A	H	C	I
12	:	L	E	K	F	C	P	U	Y	M	S	N	V	X	G	W	T	R	O	Z	H	A	Q	B	I	D	J
13	:	M	F	L	G	D	Q	V	Z	N	T	O	W	Y	H	X	U	S	P	A	I	B	R	C	J	E	K
14	:	N	G	M	H	E	R	W	A	O	U	P	X	Z	I	Y	V	T	Q	B	J	C	S	D	K	F	L
15	:	O	H	N	I	F	S	X	B	P	V	Q	Y	A	J	Z	W	U	R	C	K	D	T	E	L	G	M
16	:	P	I	O	J	G	T	Y	C	Q	W	R	Z	B	K	A	X	V	S	D	L	E	U	F	M	H	N
17	:	Q	J	P	K	H	U	Z	D	R	X	S	A	C	L	B	Y	W	T	E	M	F	V	G	N	I	O
18	:	R	K	Q	L	I	V	A	E	S	Y	T	B	D	M	C	Z	X	U	F	N	G	W	H	O	J	P
19	:	S	L	R	M	J	W	B	F	T	Z	U	C	E	N	D	A	Y	V	G	O	H	X	I	P	K	Q
20	:	T	M	S	N	K	X	C	G	U	A	V	D	F	O	E	B	Z	W	H	P	I	Y	J	Q	L	R
21	:	U	N	T	O	L	Y	D	H	V	B	W	E	G	P	F	C	A	X	I	Q	J	Z	K	R	M	S
22	:	V	O	U	P	M	Z	E	I	W	C	X	F	H	Q	G	D	B	Y	J	R	K	A	L	S	N	T
23	:	W	P	V	Q	N	A	F	J	X	D	Y	G	I	R	H	E	C	Z	K	S	L	B	M	T	O	U
24	:	X	Q	W	R	O	B	G	K	Y	E	Z	H	J	S	I	F	D	A	L	T	M	C	N	U	P	V
25	:	Y	R	X	S	P	C	H	L	Z	F	A	I	K	T	J	G	E	B	M	U	N	D	O	V	Q	W
26	:	Z	S	Y	T	Q	D	I	M	A	G	B	J	L	U	K	H	F	C	N	V	O	E	P	W	R	X

Quelle: $H =$ (A I K R F V Q J P G L O M H S U W E Y B D N T X Z C)

Tabelle A.8:

Verdrahtung der schnellen Walze auf Grund der Untersuchung der Indikatoren.
Walzenanordnung: 321; Ringstellung: AAA; Grundstellung AAE.

Basis		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	:	A	V	S	F	K	O	C	I	D	L	N	W	M	J	H	E	P	X	Q	G	R	Y	T	Z	B	U
2	:	B	W	T	G	L	P	D	J	E	M	O	X	N	K	I	F	Q	Y	R	H	S	Z	U	A	C	V
3	:	C	X	U	H	M	Q	E	K	F	N	P	Y	O	L	J	G	R	Z	S	I	T	A	V	B	D	W
4	:	D	Y	V	I	N	R	F	L	G	O	Q	Z	P	M	K	H	S	A	T	J	U	B	W	C	E	X
5	:	E	Z	W	J	O	S	G	M	H	P	R	A	Q	N	L	I	T	B	U	K	V	C	X	D	F	Y
6	:	F	A	X	K	P	T	H	N	I	Q	S	B	R	O	M	J	U	C	V	L	W	D	Y	E	G	Z
7	:	G	B	Y	L	Q	U	I	O	J	R	T	C	S	P	N	K	V	D	W	M	X	E	Z	F	H	A
8	:	H	C	Z	M	R	V	J	P	K	S	U	D	T	Q	O	L	W	E	X	N	Y	F	A	G	I	B
9	:	I	D	A	N	S	W	K	Q	L	T	V	E	U	R	P	M	X	F	Y	O	Z	G	B	H	J	C
10	:	J	E	B	O	T	X	L	R	M	U	W	F	V	S	Q	N	Y	G	Z	P	A	H	C	I	K	D
11	:	K	F	C	P	U	Y	M	S	N	V	X	G	W	T	R	O	Z	H	A	Q	B	I	D	J	L	E
12	:	L	G	D	Q	V	Z	N	T	O	W	Y	H	X	U	S	P	A	I	B	R	C	J	E	K	M	F
13	:	M	H	E	R	W	A	O	U	P	X	Z	I	Y	V	T	Q	B	J	C	S	D	K	F	L	N	G
14	:	N	I	F	S	X	B	P	V	Q	Y	A	J	Z	W	U	R	C	K	D	T	E	L	G	M	O	H
15	:	O	J	G	T	Y	C	Q	W	R	Z	B	K	A	X	V	S	D	L	E	U	F	M	H	N	P	I
16	:	P	K	H	U	Z	D	R	X	S	A	C	L	B	Y	W	T	E	M	F	V	G	N	I	O	Q	J
17	:	Q	L	I	V	A	E	S	Y	T	B	D	M	C	Z	X	U	F	N	G	W	H	O	J	P	R	K
18	:	R	M	J	W	B	F	T	Z	U	C	E	N	D	A	Y	V	G	O	H	X	I	P	K	Q	S	L
19	:	S	N	K	X	C	G	U	A	V	D	F	O	E	B	Z	W	H	P	I	Y	J	Q	L	R	T	M
20	:	T	O	L	Y	D	H	V	B	W	E	G	P	F	C	A	X	I	Q	J	Z	K	R	M	S	U	N
21	:	U	P	M	Z	E	I	W	C	X	F	H	Q	G	D	B	Y	J	R	K	A	L	S	N	T	V	O
22	:	V	Q	N	A	F	J	X	D	Y	G	I	R	H	E	C	Z	K	S	L	B	M	T	O	U	W	P
23	:	W	R	O	B	G	K	Y	E	Z	H	J	S	I	F	D	A	L	T	M	C	N	U	P	V	X	Q
24	:	X	S	P	C	H	L	Z	F	A	I	K	T	J	G	E	B	M	U	N	D	O	V	Q	W	Y	R
25	:	Y	T	Q	D	I	M	A	G	B	J	L	U	K	H	F	C	N	V	O	E	P	W	R	X	Z	S
26	:	Z	U	R	E	J	N	B	H	C	K	M	V	L	I	G	D	O	W	P	F	Q	X	S	Y	A	T

Quelle: $H =$ (A Y G I P D T O H N E J M K F Q S U C W Z B L R V X)

Tabelle A.9:

Verdrahtung der schnellen Walze auf Grund der Untersuchung der Indikatoren.
Walzenanordnung: 321; Ringstellung: AAA; Grundstellung AAS.

Basis		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	:	A	X	I	Q	J	Z	K	R	M	S	U	N	T	O	L	Y	D	H	V	B	W	E	G	P	F	C
2	:	B	Y	J	R	K	A	L	S	N	T	V	O	U	P	M	Z	E	I	W	C	X	F	H	Q	G	D
3	:	C	Z	K	S	L	B	M	T	O	U	W	P	V	Q	N	A	F	J	X	D	Y	G	I	R	H	E
4	:	D	A	L	T	M	C	N	U	P	V	X	Q	W	R	O	B	G	K	Y	E	Z	H	J	S	I	F
5	:	E	B	M	U	N	D	O	V	Q	W	Y	R	X	S	P	C	H	L	Z	F	A	I	K	T	J	G
6	:	F	C	N	V	O	E	P	W	R	X	Z	S	Y	T	Q	D	I	M	A	G	B	J	L	U	K	H
7	:	G	D	O	W	P	F	Q	X	S	Y	A	T	Z	U	R	E	J	N	B	H	C	K	M	V	L	I
8	:	H	E	P	X	Q	G	R	Y	T	Z	B	U	A	V	S	F	K	O	C	I	D	L	N	W	M	J
9	:	I	F	Q	Y	R	H	S	Z	U	A	C	V	B	W	T	G	L	P	D	J	E	M	O	X	N	K
10	:	J	G	R	Z	S	I	T	A	V	B	D	W	C	X	U	H	M	Q	E	K	F	N	P	Y	O	L
11	:	K	H	S	A	T	J	U	B	W	C	E	X	D	Y	V	I	N	R	F	L	G	O	Q	Z	P	M
12	:	L	I	T	B	U	K	V	C	X	D	F	Y	E	Z	W	J	O	S	G	M	H	P	R	A	Q	N
13	:	M	J	U	C	V	L	W	D	Y	E	G	Z	F	A	X	K	P	T	H	N	I	Q	S	B	R	O
14	:	N	K	V	D	W	M	X	E	Z	F	H	A	G	B	Y	L	Q	U	I	O	J	R	T	C	S	P
15	:	O	L	W	E	X	N	Y	F	A	G	I	B	H	C	Z	M	R	V	J	P	K	S	U	D	T	Q
16	:	P	M	X	F	Y	O	Z	G	B	H	J	C	I	D	A	N	S	W	K	Q	L	T	V	E	U	R
17	:	Q	N	Y	G	Z	P	A	H	C	I	K	D	J	E	B	O	T	X	L	R	M	U	W	F	V	S
18	:	R	O	Z	H	A	Q	B	I	D	J	L	E	K	F	C	P	U	Y	M	S	N	V	X	G	W	T
19	:	S	P	A	I	B	R	C	J	E	K	M	F	L	G	D	Q	V	Z	N	T	O	W	Y	H	X	U
20	:	T	Q	B	J	C	S	D	K	F	L	N	G	M	H	E	R	W	A	O	U	P	X	Z	I	Y	V
21	:	U	R	C	K	D	T	E	L	G	M	O	H	N	I	F	S	X	B	P	V	Q	Y	A	J	Z	W
22	:	V	S	D	L	E	U	F	M	H	N	P	I	O	J	G	T	Y	C	Q	W	R	Z	B	K	A	X
23	:	W	T	E	M	F	V	G	N	I	O	Q	J	P	K	H	U	Z	D	R	X	S	A	C	L	B	Y
24	:	X	U	F	N	G	W	H	O	J	P	R	K	Q	L	I	V	A	E	S	Y	T	B	D	M	C	Z
25	:	Y	V	G	O	H	X	I	P	K	Q	S	L	R	M	J	W	B	F	T	Z	U	C	E	N	D	A
26	:	Z	W	H	P	I	Y	J	Q	L	R	T	M	S	N	K	X	C	G	U	A	V	D	F	O	E	B

Quelle: $H =$ (A T Z Q V Y W R C E G O I L N X D H J M K S U B P F)

Tabelle A.10:

Verdrahtung der schnellen Walze auf Grund der Untersuchung der Indikatoren.
Walzenanordnung: 321; Ringstellung: AAA; Grundstellung LGS .

Basis		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	:	A	X	I	Q	J	Z	K	R	M	S	U	N	T	O	L	Y	D	H	V	B	W	E	G	P	F	C
2	:	B	Y	J	R	K	A	L	S	N	T	V	O	U	P	M	Z	E	I	W	C	X	F	H	Q	G	D
3	:	C	Z	K	S	L	B	M	T	O	U	W	P	V	Q	N	A	F	J	X	D	Y	G	I	R	H	E
4	:	D	A	L	T	M	C	N	U	P	V	X	Q	W	R	O	B	G	K	Y	E	Z	H	J	S	I	F
5	:	E	B	M	U	N	D	O	V	Q	W	Y	R	X	S	P	C	H	L	Z	F	A	I	K	T	J	G
6	:	F	C	N	V	O	E	P	W	R	X	Z	S	Y	T	Q	D	I	M	A	G	B	J	L	U	K	H
7	:	G	D	O	W	P	F	Q	X	S	Y	A	T	Z	U	R	E	J	N	B	H	C	K	M	V	L	I
8	:	H	E	P	X	Q	G	R	Y	T	Z	B	U	A	V	S	F	K	O	C	I	D	L	N	W	M	J
9	:	I	F	Q	Y	R	H	S	Z	U	A	C	V	B	W	T	G	L	P	D	J	E	M	O	X	N	K
10	:	J	G	R	Z	S	I	T	A	V	B	D	W	C	X	U	H	M	Q	E	K	F	N	P	Y	O	L
11	:	K	H	S	A	T	J	U	B	W	C	E	X	D	Y	V	I	N	R	F	L	G	O	Q	Z	P	M
12	:	L	I	T	B	U	K	V	C	X	D	F	Y	E	Z	W	J	O	S	G	M	H	P	R	A	Q	N
13	:	M	J	U	C	V	L	W	D	Y	E	G	Z	F	A	X	K	P	T	H	N	I	Q	S	B	R	O
14	:	N	K	V	D	W	M	X	E	Z	F	H	A	G	B	Y	L	Q	U	I	O	J	R	T	C	S	P
15	:	O	L	W	E	X	N	Y	F	A	G	I	B	H	C	Z	M	R	V	J	P	K	S	U	D	T	Q
16	:	P	M	X	F	Y	O	Z	G	B	H	J	C	I	D	A	N	S	W	K	Q	L	T	V	E	U	R
17	:	Q	N	Y	G	Z	P	A	H	C	I	K	D	J	E	B	O	T	X	L	R	M	U	W	F	V	S
18	:	R	O	Z	H	A	Q	B	I	D	J	L	E	K	F	C	P	U	Y	M	S	N	V	X	G	W	T
19	:	S	P	A	I	B	R	C	J	E	K	M	F	L	G	D	Q	V	Z	N	T	O	W	Y	H	X	U
20	:	T	Q	B	J	C	S	D	K	F	L	N	G	M	H	E	R	W	A	O	U	P	X	Z	I	Y	V
21	:	U	R	C	K	D	T	E	L	G	M	O	H	N	I	F	S	X	B	P	V	Q	Y	A	J	Z	W
22	:	V	S	D	L	E	U	F	M	H	N	P	I	O	J	G	T	Y	C	Q	W	R	Z	B	K	A	X
23	:	W	T	E	M	F	V	G	N	I	O	Q	J	P	K	H	U	Z	D	R	X	S	A	C	L	B	Y
24	:	X	U	F	N	G	W	H	O	J	P	R	K	Q	L	I	V	A	E	S	Y	T	B	D	M	C	Z
25	:	Y	V	G	O	H	X	I	P	K	Q	S	L	R	M	J	W	B	F	T	Z	U	C	E	N	D	A
26	:	Z	W	H	P	I	Y	J	Q	L	R	T	M	S	N	K	X	C	G	U	A	V	D	F	O	E	B

Quelle: $H =$ (A T Z Q V Y W R C E G O I L N X D H J M K S U B P F)

Tabelle A.11:

Verdrahtung der schnellen Walze auf Grund der Untersuchung der Indikatoren.
Walzenanordnung: 321; Ringstellung: `AAA` ; Grundstellung: `AAA`.

Basis		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	:	A	G	I	B	H	C	Z	M	R	V	J	P	K	S	U	D	T	Q	O	L	W	E	X	N	Y	F
2	:	B	H	J	C	I	D	A	N	S	W	K	Q	L	T	V	E	U	R	P	M	X	F	Y	O	Z	G
3	:	C	I	K	D	J	E	B	O	T	X	L	R	M	U	W	F	V	S	Q	N	Y	G	Z	P	A	H
4	:	D	J	L	E	K	F	C	P	U	Y	M	S	N	V	X	G	W	T	R	O	Z	H	A	Q	B	I
5	:	E	K	M	F	L	G	D	Q	V	Z	N	T	O	W	Y	H	X	U	S	P	A	I	B	R	C	J
6	:	F	L	N	G	M	H	E	R	W	A	O	U	P	X	Z	I	Y	V	T	Q	B	J	C	S	D	K
7	:	G	M	O	H	N	I	F	S	X	B	P	V	Q	Y	A	J	Z	W	U	R	C	K	D	T	E	L
8	:	H	N	P	I	O	J	G	T	Y	C	Q	W	R	Z	B	K	A	X	V	S	D	L	E	U	F	M
9	:	I	O	Q	J	P	K	H	U	Z	D	R	X	S	A	C	L	B	Y	W	T	E	M	F	V	G	N
10	:	J	P	R	K	Q	L	I	V	A	E	S	Y	T	B	D	M	C	Z	X	U	F	N	G	W	H	O
11	:	K	Q	S	L	R	M	J	W	B	F	T	Z	U	C	E	N	D	A	Y	V	G	O	H	X	I	P
12	:	L	R	T	M	S	N	K	X	C	G	U	A	V	D	F	O	E	B	Z	W	H	P	I	Y	J	Q
13	:	M	S	U	N	T	O	L	Y	D	H	V	B	W	E	G	P	F	C	A	X	I	Q	J	Z	K	R
14	:	N	T	V	O	U	P	M	Z	E	I	W	C	X	F	H	Q	G	D	B	Y	J	R	K	A	L	S
15	:	O	U	W	P	V	Q	N	A	F	J	X	D	Y	G	I	R	H	E	C	Z	K	S	L	B	M	T
16	:	P	V	X	Q	W	R	O	B	G	K	Y	E	Z	H	J	S	I	F	D	A	L	T	M	C	N	U
17	:	Q	W	Y	R	X	S	P	C	H	L	Z	F	A	I	K	T	J	G	E	B	M	U	N	D	O	V
18	:	R	X	Z	S	Y	T	Q	D	I	M	A	G	B	J	L	U	K	H	F	C	N	V	O	E	P	W
19	:	S	Y	A	T	Z	U	R	E	J	N	B	H	C	K	M	V	L	I	G	D	O	W	P	F	Q	X
20	:	T	Z	B	U	A	V	S	F	K	O	C	I	D	L	N	W	M	J	H	E	P	X	Q	G	R	Y
21	:	U	A	C	V	B	W	T	G	L	P	D	J	E	M	O	X	N	K	I	F	Q	Y	R	H	S	Z
22	:	V	B	D	W	C	X	U	H	M	Q	E	K	F	N	P	Y	O	L	J	G	R	Z	S	I	T	A
23	:	W	C	E	X	D	Y	V	I	N	R	F	L	G	O	Q	Z	P	M	K	H	S	A	T	J	U	B
24	:	X	D	F	Y	E	Z	W	J	O	S	G	M	H	P	R	A	Q	N	L	I	T	B	U	K	V	C
25	:	Y	E	G	Z	F	A	X	K	P	T	H	N	I	Q	S	B	R	O	M	J	U	C	V	L	W	D
26	:	Z	F	H	A	G	B	Y	L	Q	U	I	O	J	R	T	C	S	P	N	K	V	D	W	M	X	E

Quelle: $W =$ `(A D F P V Z B E C K M T H X S L R I N Q O J U W Y G)`

Tabelle A.12:

Verdrahtung der schnellen Walze auf Grund der Untersuchung der Indikatoren.
Walzenanordnung: 321; Ringstellung: `AAA` ; Grundstellung: `AAC`.

Basis		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	:	I	B	H	C	Z	M	R	V	J	P	K	S	U	D	T	Q	O	L	W	E	X	N	Y	F	A	G
2	:	J	C	I	D	A	N	S	W	K	Q	L	T	V	E	U	R	P	M	X	F	Y	O	Z	G	B	H
3	:	K	D	J	E	B	O	T	X	L	R	M	U	W	F	V	S	Q	N	Y	G	Z	P	A	H	C	I
4	:	L	E	K	F	C	P	U	Y	M	S	N	V	X	G	W	T	R	O	Z	H	A	Q	B	I	D	J
5	:	M	F	L	G	D	Q	V	Z	N	T	O	W	Y	H	X	U	S	P	A	I	B	R	C	J	E	K
6	:	N	G	M	H	E	R	W	A	O	U	P	X	Z	I	Y	V	T	Q	B	J	C	S	D	K	F	L
7	:	O	H	N	I	F	S	X	B	P	V	Q	Y	A	J	Z	W	U	R	C	K	D	T	E	L	G	M
8	:	P	I	O	J	G	T	Y	C	Q	W	R	Z	B	K	A	X	V	S	D	L	E	U	F	M	H	N
9	:	Q	J	P	K	H	U	Z	D	R	X	S	A	C	L	B	Y	W	T	E	M	F	V	G	N	I	O
10	:	R	K	Q	L	I	V	A	E	S	Y	T	B	D	M	C	Z	X	U	F	N	G	W	H	O	J	P
11	:	S	L	R	M	J	W	B	F	T	Z	U	C	E	N	D	A	Y	V	G	O	H	X	I	P	K	Q
12	:	T	M	S	N	K	X	C	G	U	A	V	D	F	O	E	B	Z	W	H	P	I	Y	J	Q	L	R
13	:	U	N	T	O	L	Y	D	H	V	B	W	E	G	P	F	C	A	X	I	Q	J	Z	K	R	M	S
14	:	V	O	U	P	M	Z	E	I	W	C	X	F	H	Q	G	D	B	Y	J	R	K	A	L	S	N	T
15	:	W	P	V	Q	N	A	F	J	X	D	Y	G	I	R	H	E	C	Z	K	S	L	B	M	T	O	U
16	:	X	Q	W	R	O	B	G	K	Y	E	Z	H	J	S	I	F	D	A	L	T	M	C	N	U	P	V
17	:	Y	R	X	S	P	C	H	L	Z	F	A	I	K	T	J	G	E	B	M	U	N	D	O	V	Q	W
18	:	Z	S	Y	T	Q	D	I	M	A	G	B	J	L	U	K	H	F	C	N	V	O	E	P	W	R	X
19	:	A	T	Z	U	R	E	J	N	B	H	C	K	M	V	L	I	G	D	O	W	P	F	Q	X	S	Y
20	:	B	U	A	V	S	F	K	O	C	I	D	L	N	W	M	J	H	E	P	X	Q	G	R	Y	T	Z
21	:	C	V	B	W	T	G	L	P	D	J	E	M	O	X	N	K	I	F	Q	Y	R	H	S	Z	U	A
22	:	D	W	C	X	U	H	M	Q	E	K	F	N	P	Y	O	L	J	G	R	Z	S	I	T	A	V	B
23	:	E	X	D	Y	V	I	N	R	F	L	G	O	Q	Z	P	M	K	H	S	A	T	J	U	B	W	C
24	:	F	Y	E	Z	W	J	O	S	G	M	H	P	R	A	Q	N	L	I	T	B	U	K	V	C	X	D
25	:	G	Z	F	A	X	K	P	T	H	N	I	Q	S	B	R	O	M	J	U	C	V	L	W	D	Y	E
26	:	H	A	G	B	Y	L	Q	U	I	O	J	R	T	C	S	P	N	K	V	D	W	M	X	E	Z	F

Quelle: $W =$ `(Y B D N T X Z C A I K R F V Q J P G L O M H S U W E)`

Tabelle A.13:

Verdrahtung der schnellen Walze auf Grund der Untersuchung der Indikatoren.
Walzenanordnung: 321; Ringstellung: `AAA` ; Grundstellung: `AAE`.

Basis		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	:	H	C	Z	M	R	V	J	P	K	S	U	D	T	Q	O	L	W	E	X	N	Y	F	A	G	I	B
2	:	I	D	A	N	S	W	K	Q	L	T	V	E	U	R	P	M	X	F	Y	O	Z	G	B	H	J	C
3	:	J	E	B	O	T	X	L	R	M	U	W	F	V	S	Q	N	Y	G	Z	P	A	H	C	I	K	D
4	:	K	F	C	P	U	Y	M	S	N	V	X	G	W	T	R	O	Z	H	A	Q	B	I	D	J	L	E
5	:	L	G	D	Q	V	Z	N	T	O	W	Y	H	X	U	S	P	A	I	B	R	C	J	E	K	M	F
6	:	M	H	E	R	W	A	O	U	P	X	Z	I	Y	V	T	Q	B	J	C	S	D	K	F	L	N	G
7	:	N	I	F	S	X	B	P	V	Q	Y	A	J	Z	W	U	R	C	K	D	T	E	L	G	M	O	H
8	:	O	J	G	T	Y	C	Q	W	R	Z	B	K	A	X	V	S	D	L	E	U	F	M	H	N	P	I
9	:	P	K	H	U	Z	D	R	X	S	A	C	L	B	Y	W	T	E	M	F	V	G	N	I	O	Q	J
10	:	Q	L	I	V	A	E	S	Y	T	B	D	M	C	Z	X	U	F	N	G	W	H	O	J	P	R	K
11	:	R	M	J	W	B	F	T	Z	U	C	E	N	D	A	Y	V	G	O	H	X	I	P	K	Q	S	L
12	:	S	N	K	X	C	G	U	A	V	D	F	O	E	B	Z	W	H	P	I	Y	J	Q	L	R	T	M
13	:	T	O	L	Y	D	H	V	B	W	E	G	P	F	C	A	X	I	Q	J	Z	K	R	M	S	U	N
14	:	U	P	M	Z	E	I	W	C	X	F	H	Q	G	D	B	Y	J	R	K	A	L	S	N	T	V	O
15	:	V	Q	N	A	F	J	X	D	Y	G	I	R	H	E	C	Z	K	S	L	B	M	T	O	U	W	P
16	:	W	R	O	B	G	K	Y	E	Z	H	J	S	I	F	D	A	L	T	M	C	N	U	P	V	X	Q
17	:	X	S	P	C	H	L	Z	F	A	I	K	T	J	G	E	B	M	U	N	D	O	V	Q	W	Y	R
18	:	Y	T	Q	D	I	M	A	G	B	J	L	U	K	H	F	C	N	V	O	E	P	W	R	X	Z	S
19	:	Z	U	R	E	J	N	B	H	C	K	M	V	L	I	G	D	O	W	P	F	Q	X	S	Y	A	T
20	:	A	V	S	F	K	O	C	I	D	L	N	W	M	J	H	E	P	X	Q	G	R	Y	T	Z	B	U
21	:	B	W	T	G	L	P	D	J	E	M	O	X	N	K	I	F	Q	Y	R	H	S	Z	U	A	C	V
22	:	C	X	U	H	M	Q	E	K	F	N	P	Y	O	L	J	G	R	Z	S	I	T	A	V	B	D	W
23	:	D	Y	V	I	N	R	F	L	G	O	Q	Z	P	M	K	H	S	A	T	J	U	B	W	C	E	X
24	:	E	Z	W	J	O	S	G	M	H	P	R	A	Q	N	L	I	T	B	U	K	V	C	X	D	F	Y
25	:	F	A	X	K	P	T	H	N	I	Q	S	B	R	O	M	J	U	C	V	L	W	D	Y	E	G	Z
26	:	G	B	Y	L	Q	U	I	O	J	R	T	C	S	P	N	K	V	D	W	M	X	E	Z	F	H	A

Quelle: $W =$ (W Z B L R V X A Y G I P D T O H N E J M K F Q S U C)

Tabelle A.14:

Verdrahtung der schnellen Walze auf Grund der Untersuchung der Indikatoren.
Walzenanordnung: 321; Ringstellung: `AAA` ; Grundstellung: `AAS`.

Basis		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	:	O	L	W	E	X	N	Y	F	A	G	I	B	H	C	Z	M	R	V	J	P	K	S	U	D	T	Q
2	:	P	M	X	F	Y	O	Z	G	B	H	J	C	I	D	A	N	S	W	K	Q	L	T	V	E	U	R
3	:	Q	N	Y	G	Z	P	A	H	C	I	K	D	J	E	B	O	T	X	L	R	M	U	W	F	V	S
4	:	R	O	Z	H	A	Q	B	I	D	J	L	E	K	F	C	P	U	Y	M	S	N	V	X	G	W	T
5	:	S	P	A	I	B	R	C	J	E	K	M	F	L	G	D	Q	V	Z	N	T	O	W	Y	H	X	U
6	:	T	Q	B	J	C	S	D	K	F	L	N	G	M	H	E	R	W	A	O	U	P	X	Z	I	Y	V
7	:	U	R	C	K	D	T	E	L	G	M	O	H	N	I	F	S	X	B	P	V	Q	Y	A	J	Z	W
8	:	V	S	D	L	E	U	F	M	H	N	P	I	O	J	G	T	Y	C	Q	W	R	Z	B	K	A	X
9	:	W	T	E	M	G	V	G	N	I	O	Q	J	P	K	H	U	Z	D	R	X	S	A	C	L	B	Y
10	:	X	U	F	N	G	W	H	O	J	P	R	K	Q	L	I	V	A	E	S	Y	T	B	D	M	C	Z
11	:	Y	V	G	O	H	X	I	P	K	Q	S	L	R	M	J	W	B	F	T	Z	U	C	E	N	D	A
12	:	Z	W	H	P	I	Y	J	Q	L	R	T	M	S	N	K	X	C	G	U	A	V	D	F	O	E	B
13	:	A	X	I	Q	J	Z	K	R	M	S	U	N	T	O	L	Y	D	H	V	B	W	E	G	P	F	C
14	:	B	Y	J	R	K	A	L	S	N	T	V	O	U	P	M	Z	E	I	W	C	X	F	H	Q	G	D
15	:	C	Z	K	S	L	B	M	T	O	U	W	P	V	Q	N	A	F	J	X	D	Y	G	I	R	H	E
16	:	D	A	L	T	M	C	N	U	P	V	X	Q	W	R	O	B	G	K	Y	E	Z	H	J	S	I	F
17	:	E	B	M	U	N	D	O	V	Q	W	Y	R	X	S	P	C	H	L	Z	F	A	I	K	T	J	G
18	:	F	C	N	V	O	E	P	W	R	X	Z	S	Y	T	Q	D	I	M	A	G	B	J	L	U	K	H
19	:	G	D	O	W	P	F	Q	X	S	Y	A	T	Z	U	R	E	J	N	B	H	C	K	M	V	L	I
20	:	H	E	P	X	Q	G	R	Y	T	Z	B	U	A	V	S	F	K	O	C	I	D	L	N	W	M	J
21	:	I	F	Q	Y	R	H	S	Z	U	A	C	V	B	W	T	G	L	P	D	J	E	M	O	X	N	K
22	:	J	G	R	Z	S	I	T	A	V	B	D	W	C	X	U	H	M	Q	E	K	F	N	P	Y	O	L
23	:	K	H	S	A	T	J	U	B	W	C	E	X	D	Y	V	I	N	R	F	L	G	O	Q	Z	P	M
24	:	L	I	T	B	U	K	V	C	X	D	F	Y	E	Z	W	J	O	S	G	M	H	P	R	A	Q	N
25	:	M	J	U	C	V	L	W	D	Y	E	G	Z	F	A	X	K	P	T	H	N	I	Q	S	B	R	O
26	:	N	K	V	D	W	M	X	E	Z	F	H	A	G	B	Y	L	Q	U	I	O	J	R	T	C	S	P

Quelle: $W =$ (I L N X D H J M K S U B P F A T Z Q V Y W R C E G O)

Tabelle A.15:

Anhang B

Bearbeitung eines M4-Spruches

Rufzeichen: ÄDA, Zeit: 14.14 Uhr, Datum: 6.3.1945; Spruchnr.: 36; Länge: 90 Gruppen.

```
CXSO UNVZ NEWM ESUC IIFP RLEE TPNZ LPYJ WDKL LDUJ
URJL BUKF WNKR SPEN ZUPZ LWJF GCHH JMEL KFKP WCMD
RGAF UMZE VOEN UUQG TXIP ZQKP SRAM CEWJ NIFR SCXX
NRCQ TYAB YRDT IRZF VJIJ JGHU GKJU TPPY POFN LLJI
QCOE DQAM EKSY ZSWZ ZJGF ERGG LJTL AWUP HBST LIUP
GJTO BBYC NTST KPBU ESSK EYDR ZDSA DABE TWRU KDHC
XPQL ZCXM YVIV WBBO HVJB KTZW MUTK YJJQ ZVFC EDGH
SQWE ODAO HOBT ESCL AARE EAKH SSQN IPCI XHJW GOWL
WFTZ ZDGP KIXE PATD AXEY JDGF SDUN FUKR CXSO UNVZ
```

Die Bigramme des Indikators CXSO UNVZ werden mit der Bigrammtafel G Kennwort „Quelle“ übersetzt: CX $\mapsto$ IH, SO $\mapsto$ NP, UN $\mapsto$ QV und, VZ $\mapsto$ FW

Im K-Buch wird festgestllt, dass NQF zu Nr. 301 gehört, das ist nach der Zuteilungsliste ein Schlüssel „Triton“= «Shark».

Die Sendezeit und die Frequenz passten zum Sender ÄDA, bestätigt durch Peilungen, Sender Bergen. Es schien sicher, dass es sich um einen Spruch handelte, wie er seit 6 Monaten alle drei Tage abgesetzt wurde, um heimkehrenden U-Booten die Navigationshilfen zur Einfahrt zu geben.

Daher war anzunehmen, dass der Spruch entweder begann:

`es laufen nach periode j bruno j xx eins kk funkfeuergruppe ...`

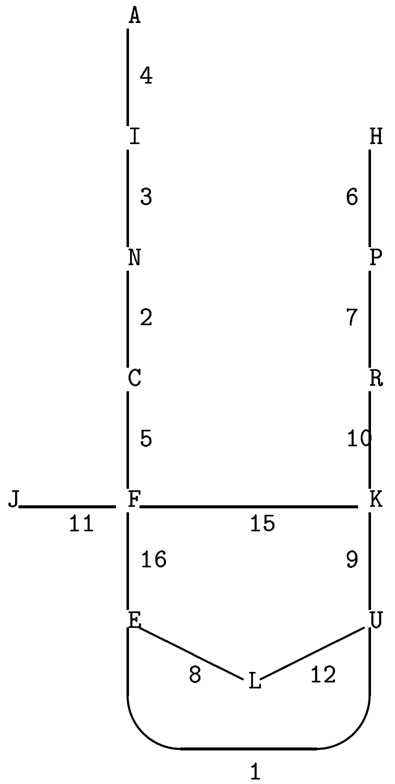
oder:

`eins kk funkfeuergruppe (j) (begen oder bruno) (j) laufen ...`

Damit wurde ein Menu erstellt mit der Struktur

```
U C I I F P R L        U R J L * * K F
e n n a c h p e        k k f u * * f e
1 2 3 4 5 6 7 8        9 1 1 1 * * 1 1
                         0 1 2 * * 4 5
```

Die Zahlen geben die relativen Positionen der Walzen der Bombe an. Beim zweiten Teil ist zu beachten, dass die Positionen 26 Stellen weiter als beim ersten Teil liegen. Daher bedeuten die Nummern 9 bis 12 1 bis 4, aber die mittlere Walze um eine Stelle weitergeschaltet, 14 und 15 bedeuten 7 und 8. (Siehe Kap. 6.2.3.1.10)



Das Ergebnis des Bombenlaufs ist dann:

`eilaufennachperiodejbrunojxxeinskkfunkfeuergeuppeeinseinsamsiebenxmaerzvonein`
`sbisdreigeinszwobiseinsvieryachtxnulvierdreinulbisnulsechsdreinulyneunxeinsnu`
`lbiseinsdwoyzwozwobiszwovgerxzwokkfunkfeuergruppeecnszwvamsiebenrmjerzvoneins`
`bisdreiyachtxnulvierdreinulbisnulsechsbreinulyeinsvierireinulbiseijssechsdrei`
`nulyneunxkkfortkkeinsnulbiseieszwobv`

Die Walzenordnung ergab sich zu:
Umkehrwalze B + Griechenwalze Gamma, 4 5 3 (von links nach rechts)
Die Stecker waren:
`A/X, B/Z, C/Y, D/G, E/T, I/P, J/N, O/Q, R/V` und `S/W`, ungesteckert blieben `F, H, K, L, M, U`
Ringstellung: `M M T`, Grundstellung: `K L G S`

Das Ergebnis lag vor am 7. 3. um 2 Uhr 30, also 12 Stunden und 16 Minuten nach dem Absetzen des Funkspruchs von Bergen.[1]

[1]Das Material stammt aus RIP 425, Seite 62 bis 104. Es wurde von Mr. Erskine zur Verfügung gestellt.

Literatur

Alexander, C.H.O'D.	Cryptographic History of Work on the German Naval Enigma P.R.O. HW 25/1
Allason, R. N. W.	The SIGINT Secrets, Morrow, 1988
Bauer, Friedrich L.	Entzifferte Geheimnisse, Methoden und Maximen der Kryptologie, Springer-Verlag, Berlin, 2000 ISBN 3-540-67931-6
Beesly, Patrick a)	Das «Operational Intelligence Centre» der britischen Admiralität im Zweiten Weltkrieg, In: Marine-Rundschau, Bd. 73, 1976 Teil I: S. 147 - 164; Teil II: S. 368 - 383; Teil III: S. 698 - 707
Beesly, Patrick b)	Very Special Intelligence, Ullstein, Berlin, 1978, ISBN 3-550-07381-X
Bennett, Ralph a)	Ultra and Mediterranean Strategy 1941 - 1945, Hamish Hamilton, London, 1989
Bennett, Ralph b)	Ultra in the West, Hutchinson, London, 1979
Bertrand, Gustave	Enigma ou la plus grand nigme de la guerre 1939 - 1945. Paris: Librairie Plon , 1973
Bloch, Gilbert a)	Enigma before ULTRA, Polish Work and the French Contribution (übersetzt v. C.A. Deavours) In: Cryptologia, Vol. 11, No. 3, 1987, S. 142 - 155
Bloch, Gilbert b)	Enigma before ULTRA, The Polish Success and Check (1933 - 1939) (übers. v. C.A. Deavours) In: Cryptologia, Vol. 11, No. 4, 1987, S. 227 - 234
Bloch, Gilbert c)	Enigma before ULTRA (übersetzt v. C.A. Deavours) In: Cryptologia, Vol. 12, No. 3, 1988, S. 178 - 184
Bloch, Gilbert d)	Enigma Avant Ultra (1930 - 1940), Texte definitif Paris, Septembre 1988
Bloch, Gilbert e)	The Dropping of the Double Encipherment In: Cryptologia, Vol. 10, No. 3, S. 134 - 141
Budianski, Stephen	Battle of Wits Penguin, 2000
Calvocoressi, Peter	Aufbau und Arbeitsweise des britischen Entzifferungsdienstes in Beltchley Park In: Rohwer/Jäckel, S. 88 - 99
Clayton, Aileen	The Enemy is Listening, Hutchinson, London, 1980, ISBN 0-09-142340-6
Cowan, Michael J.	Rasterschlüssel 44 - The Epitome of Hand Field Ciphers In: Cryptologia, Vol. 28, No. 2, 2004, S. 115 -147
Crawford,D.u. Fox,P.(ed)	The Autoscritcher and the Superscritcher: Aids to Cryptanalysis of the German Enigma Cipher machine 1944 - 1946 In: IEEE Annals of the History of Computing, Vol. 14, Nr. 3, 1992, S. 9 - 22
Currer-Briggs, Noel	Some of Ultra's Poor Relations in Algeria, Tunesia, Sicily, and Italy In: Intelligence and National Security, Vol. 2, No. 2, S. 274 - 290, leicht verändert auch in Hinsley/Stripp, S. 209 ff
David, Charles	A World War II German Army Field Cipher And How We Broke It In: Cryptologia, Vol. 20, No. 1, 1996, S. 55 - 76
Davies, Donald W.	The Bombe a Remarkable Logic Machine In: Cryptologia, Vol. 23, No. 2, 1999, S. 108 - 137

Deavours, C. A.a)	Breakthrough '32 The Polish Solution of the Enigma (Includes MS DOS 5-1/4"Diskette for IBM PC) Aegean Park Press, Laguna Hills, California, 1988 Cryptographic Series Nr. 51, ISBN 0-89412-152-9
Deavours, C. A. b)	The Autoscritcher In: Cryptologia, Vol. 19, Nr. 2, 1995, S. 137 -148
Deavours, C. u. Kruh, L.	a) Machine Cryptography and Modern Cryptanalysis Artech House Inc., 1985
Deavours, C. u. Kruh, L.	b) The Turing Bombe: Was it Enough ? In: Cryptologia, Vol. 14, No. 4, 1990, S. 331 - 349
Deutsch, Dr. Harold C.	The Historical Impact of Revealing the Ultra Secret In: Parameters, Journal of the U.S. Army War College, Vol. 7, No. 3, 1977, S. 16 - 32
Erskine, Ralph a)	Naval Enigma: The Breaking of Heimisch and Triton In: Intelligence and National Security, Vol. 3, No. 1, 1988, S. 162 - 183
Erskine, Ralph b)	Naval Enigma: A Missing Link In: International Journal of Intelligence and Counterintelligence, Vol. 3, No. 4, 1989, S. 493 - 508
Erskine, Ralph c)	Letter to the Editor In: Intelligence and National Security, Vol. 3, No. 4, 1988, S. 184
Erskine, Ralph d)	The Soviets and Naval Enigma: Some Comments In: Intelligence and National Security, Vol. 4, 1989, S. 503 - 511
Erskine, Ralph e)	Kriegsmarine Signal Indicators In: Cryptologia, Vol. 20, No. 4, 1996, S. 330 - 340
Erskine, Ralph f)	Naval Enigma: An Astonishing Blunder In: Intelligence and National Security, Vol. 11, No. 3, 1996, S. 468 - 473
Erskine, Ralph g)	From the Archives: U-Boat HF WT Signalling In: Cryptologia, Vol. 12, No. 2, 1988, S. 98 - 106
Erskine, Ralph h)	Kriegsmarine Short Signal Systems - and How Bletchley Park Exploited Them In: Cryptologia, Vol. 23, Nr. 1, 1999, S. 65 - 92
Erskine,R. u. Weierud,F.	Naval Enigma: M4 and its rotors In: Cryptologia, Vol. 11, No. 4, 1987, S. 235 - 244
Fisher, R.A.	Theory of Statistical Estimation In: Proc.Camb.Phil.Soc. Vol.22,1925, S. 700 - 725
Foss,H.R. a)	Reminiscences on the ENIGMA P.R.O. HW 25/10
Foss,H.R. b)	The reciprocal ENIGMA P.R.O. HW 25/14
Fuensana, Soler	Mechanical Cipher Systems in the Spanish Civil War In: Cryptologia, Vol. 28, No. 3, 2004, S. 268 - 273
Gaines, Helen Fouché	Cryptanalysis, Dover Publications, New York, 1956
Gaj, Krzysztof	Szyfr Enigmy, metody zlamania Wydawnictwa Komunikacij i Lacznosci, Warszawa, 1989 ISBN 83-206-0793-0
Garlinski, Jozef	Intercept, The Enigma War, J. M. Dent & Sons, Ltd. London, 1979 ISBN 0-460-04337-4
Glantz, David M. a)	Soviet military deception in the Second World War Cass, London, 1989
Glantz, David M. b)	Soviet military intelligence in war Cass, London, 1990
Golovko, A. G.	With th Red Fleet, Putnam, London, 1965
Good, I.J. a)	Introductory Remarks for the Article in Biometrica 66 (1979) ‹A.M.Turing's Statstical Work in World War II› In: Collected Works on A.M. Turing - Pure Mathematics - ed. J.L. Britton North - Holland, 1992, S. 211 - 223

Good, I.J. b)	Studies in the History of Probability and Statistics XXXVII A.M. Turing's Statistical Work in World War II In: Biometrica, Vol. 66, Nr. 2, 1979, S. 393 - 396
Good, I.J. c)	Enigma and Fish, In: Hinsley/Stripp, S. 149 - 166
Gouazé, Linda Y.	Needles and Haystacks: The Search for Ultra in the 1930's In: Cryptologia, Vol. 11, No. 2, 1987, S. 85 - 92
Goulter, Christina	The Role of Intelligence in Coastal Command's Anti-Shipping Campaign, 1940 - 1945 In: Intelligence and National Security, Vol. 5, No. 1, 1990, S. 84 - 109 In: Hinsley/Stripp, S. 149 - 166
Hamer, David a)	Enigma: Actions involved in the ‹Double Stepping›of the Middle Rotor In: Cryptologia, Vol. 21, Nr. 1, 1997, S. 47 - 50
Hamer, David b)	G–312: An Abwehr Enigma In: Cryptologia, Vol. 24, Nr. 1. 2000, S. 41 - 54
Hamer,Sullivan,Weierud	Enigma Variations: An Extended Family of Machines In: Cryptologia, Vol. 22, Nr. 3. 1998, S. 211 - 229
Handel, Michael (Ed.)	Intelligence and Military Operations, Frank Cass., London, 1990 ISBN 0-7146-3331-3
Heider, Kraus, Welschenbach	Mathematische Methoden der Kryptoanalyse, Vieweg, 1985, ISBN 3-528-03601-X
Hinsley, F.H. (Ed.)	British Intelligence in the Second World War, London: HMSO, Vol. I, 1979, ISBN 0-11-630933-4 Vol. II, 1981, ISBN 0-11-630934- Vol. III,1, 1984, ISBN 0-11-630935-0 Vol. III,2, 1988, ISBN 0-11-630940-7
mit Simkins, C. A. G.:	Vol. IV, 1990, ISBN 0-11-630952-0
Hinsley, F. H. u. Stripp, Alan (Ed.)	Codebreakers, The Inside Story of Bletchley Park Oxford University Press, Oxford, 1993, ISBN 0-19-820327-6
Hirschfeld, Wolfgang	Feindfahrten: Das Logbuch eines U-Boot-Funkers München: Heyne, 1982
Hodges, Andrew	Alan Turing, the Enigma of Intelligence Unwin Paperback, London, 1983, ISBN 0-04-510060-8
Jablonski, David	Churchill, The Great Game and Total War, Frank Cass., London, 1991, ISBN 0-7146-3367-4
Jensen, Willi	Hilfsgeräte der Kryptographie Doktorarbeit, zurückgezogen. Standort: Inst. f. Informatik der TU München
Johnson, B.	Streng geheim, Motorbuch-Verlag, Stuttgart, 1983,ISBN 3-87943-816-1
Jukes, Geoffrey a)	The Soviets and Ultra In: Intelligence and National Security, Vol. 3, No. 2, 1988, S. 233 - 247
Jukes, Geoffrey b)	More on the Soviets and Ultra In: Intelligence and National Security, Vol. 4, 1989, S. 374 - 384
Kahn, David a)	Seizing the Enigma, Houghton Mifflin, Boston, 1991 ISBN 0-395-42739-8
Kahn, David b)	On Codes, MacMillan, New York, 1983, ISBN 0-02-560640-9
Kapera, Zdzislaw J.	Bericht des Obstlt.i.G. G.Langer: Funkaufklärung der Alliierten im Frankreichfeldzug 1940 In: The ENIGMA Bulletin, Ed. by Dr. Z.J.Kapera, No.1, December 1990 Krakow, Poland
Kasparek, C. u.Woytak, R.	In memoriam Marian Rejewski In: Cryptologia, Vol. 6, No. 1, 1982, S. 19 - 25
Kesaris, Paul (Ed.)	Ultra and the History of the United States Strategic Air Force vs. The German Air Force University Publications of America, Frederick, Maryland, 1980

Knox, D.	ENIGMA history 1938 - 1943 P.R.0. HW 25/12
Koss, Mike	The Paper Enigma-Machine In: Cryptologia, Vol. 28, No. 3, 2004, S. 204 - 210
Kozaczuk, Wladislaw a)	Enigma. How the German Machine Cipher Was Broken and How It Was Read by the Allies in World War Two, University Publications of America, Inc., 1984, ISBN 0-89093-547-5
Kozaczuk, Wladislaw b)	Geheimoperation Wicher. Polnische Mathematiker knacken den deutschen Funkschlüssel, (übersetzt v. Th. Fuchs, herausg. v. Jürgen Rohwer) Bernard & Graefe Vlg, Koblenz, 1988, ISBN 3-7637-5868-2
Kozaczuk, Wladislaw c)	Enigma: Wie der Code der Faschisten gebrochen wurde In:Horizont, Sozialistische Wochenzeitung für internationale Politik und Wirtschaft, 1975, Heft 41 - 49
Kröncke, Dr. H.	Das Telegraphengeheimnis und die Chiffriermaschine In: Radio für Alle, 2. Jg., 1926, Heft 9, S. 76 - 78
Kruh,L. u.Deavours,C.a)	The Typex Cryptograph, In: Cryptologia, Vol. 7, No. 2, 1983 S. 145 - 165
Kruh,L. u.Deavours,C.b)	The Commercial Enigma: Beginnings of Machine Cryptography In: Cryptologia, Vol. 26, Nr. 1, 2002, S. 1 - 16
Lewin, Ronald	Ultra goes to war, Hutchinson & Co, London, 1987 ISBN 0-09-134420-4
Lewis, R. P. W.	The use by the Meteorological Office of decyphered German meteorological data during the Second World War In: The Meteorological Magazine, London, Vol. 114, April 1985, S. 113 - 118
Lisicki, Tadeusz	Die Leistung des polnischen Entzifferungsdienstes bei der Lösung des Verfahrens der deutschen „Enigma“ - Schlüsselmaschine In: Rohwer, Funkaufklärung, S. 66 - 81
Mahon, A. P.	The History of Hut Eight 1939–1945 NARA Dokument Nr. 4685, Box ZEMA44
Marks, Philip	Umkehrwalze D: Enigma's Rewirable Reflector Part I, In: Cryptologia,Vol.25,Nr.2,2001,S. 101 - 141 Part II, In: Cryptologia,Vol.25,Nr.3,2001,S. 177 - 212 Part III, In: Cryptologia,Vol.25,Nr.4,2001,S. 296 - 309
Marks,P. u.Weierud,F.	Recovering the Wiring of ENIGMA's Umkehrwalze A In: Cryptologia, Vol. 24, Nr.1, 2000, S. 55 - 65
Meulen, M. van der a)	The Book Cipher System of the Wehrmacht In: Cryptologia, Vol. 19, Nr. 3, 1995, S. 247 - 260.
Meulen, M. van der b)	Werftschlüssel, A German Navy Hand Cipher System, Part I In: Cryptologia, Vol. 19, Nr. 4, 1995, S. 349 - 364
Meulen, M. van der c)	Werftschlüssel, A German Navy Hand Cipher System, Part II In: Cryptologia, Vol. 20, Nr. 1, 1996, S. 37 - 54
Miller, A. Ray	The Cryptographic Mathematics of Enigma In: Cryptologia, Vol. 19, Nr. 1, 1995, S. 65 - 80
Milner-Barry, P. S.	The Soviets and Ultra: A Comment on Jukes' Hypothesis In: Intelligence and National Security, Vol. 3, No. 2, 1988, S. 24 - 251
Morris, Christopher	Ultra's Poor Relations In: Intelligence and National Security, Vol. 1, No. 1, S. 111 - 122; auch, leicht verändert, in Hinsley/Stripp Kap. 24: Navy Ultra's Poor Relations
Paillole, Paul	Notre Espion chez Hitler, Ed. Rob. Lafont, Paris, 1985
Peirce, C.S. a)	The probability of Induction In: Pop. Sci. Monthly, 1878
Peirce, C.S. b)	Chance, Love, and Logic, ed. Morris R. Cohen Harcourt, Brace, New York, 1923
Quirantes, Arturo	Model Z: A numbers-only Enigma Version In: Cryptologia, Vol. 28, No.2, 2004, S. 153 - 156

Reche, Reinhard	Die „Quadratur der Meere“ - zur Umrechnung der Marine-Quadratkarte 1939 - 1945, In: Marine-Rundschau, 1984, Nr. 3, S. 120 - 122
Rejewski, Marian a)	Summary of our methods for reconstructing ENIGMA and reconstructing daily keys, and of German efforts to frustrate those methods (übersetzt v. Chr. Kasparek) Appendix C zu Kozaczuk a)
Rejewski, Marian b)	How the Polish Mathematicians Broke Enigma (übersetzt v. Chr. Kasparek) Appendix D zu Kozaczuk a)
Rejewski, Marian c)	The Mathematical Solution of the Enigma Cipher (übersetzt v. Chr. Kasparek), Appendix E zu Kozaczuk a) Inhaltlich wie d), mit zusätzlichem Beispiel
Rejewski, Marian d)	An Application of the Theory of Permutations in Breaking the Enigma Cipher In: Applicationes mathematicae, Warschau, XVI, (4) , 1980, S. 543 - 559
Rejewski, Marian e)	How Polish Mathematicians Deciphered the Enigma (übersetzt v. Joan Stepenske) In: Annals of the History of Computing, Vol. 3, No. 3, July 1981, S. 213 - 234, Inhaltlich wie b), enthält das Listing eines BASIC - Programms zur Simulation der ENIGMA
Rejewski, Marian f)	Remarks on Appendix 1 to British Intelligence in the Second World War by F.H.Hinsley (übersetzt v. Chr. Kasparek) In: Cryptologia, Vol 6, No 1, January 1982, S. 75 - 82
Rejewski, Marian g)	Mathematical Solution of the Enigma Cipher (übersetzt v. Chr. Kasparek) In: Cryptologia, Vol. 6, No. 1, January 1982, S. 1 - 18, Inhaltlich wie c)
Ribadeau - Dumas	Les decryptements de la machine Enigma des Armees Allemandes Privatdruck, 1987
Rohrbach, Hans	Mathematische und Maschinelle Methoden beim Chiffrieren und Dechiffrieren In: Naturforschung und Medizin in Deutschland 1939-1946, Band 3, Angewandte Mathematik, Teil I, Herausgegeben von Alwin Walther, Verlag Chemie, Weinheim, 1953
Rohwer, Jürgen a)	The Critical Convoy Battles of March 1943, Ian Allen, London, 1977 ISBN 0-7110-0749-7
Rohwer, Jürgen b)	Funkaufklärung und Intelligence in den Entscheidungsprozessen des Zweiten Weltkriegs In: Duchhard, Schlenke: Festschrift, Vlg. Wilh. Fink, München, 1982, ISBN 3-7705-2080-7
Rohwer, Jürgen c)	Ultra, xB-Dienst und Magic, In: Marine-Rundschau, Bd. 76, 1979, S. 637 - 648
Rohwer, Jürgen d)	Axis Submarine Successes, 1939 - 1945, Naval Institute, Cambridge, 1983
Rohwer, Jürgen u. Jäckel, Eberhard (Hrsg)	Die Funkaufklärung und ihre Rolle im 2. Weltkrieg Motorbuch Verlag, Stuttgart, 1979, ISBN 3-87943-666-5
Schick, Joseph S.	With the 849th SIS, In: Cryptologia, Vol. 11, No. 1, 1987, S. 29 - 39
Schwerdtfeger, W. und Selinger, F.	Wetterflieger in der Arktis 1940 - 1944 Motorbuch-Verlag, Stuttgart, 1982, ISBN 3-87943-854-4
Sebag-Montefiore, H.	Enigma: The Battle for the Code Weidenfeld & Nicolson, London, 2000 ISBN 0-297-84251-X
Skillen, Hugh a)	Enigma and its Achilles Heel, Selbstverlag, Pinner, 1992 ISBN 0-9515190-2-6
Skillen, Hugh b)	Spies of the Airwaves, Selbstverlag, Pinner, 1989, ISBN 0-9515190-0-X
Skillen, Hugh c)	Rasterschlüssel, In: The Enigma Symposium 1995, S. 127 - 132 Selbstverlag, Pinner, 1995, ISBN 0-9515190-77

Smith,M.u.Erskine,R.	Action this Day Bantam Press, 2001, ISBN 0593 049 101
Turing,Alan,	Turing's treatise on the Enigma NARA - Dkument, Nr, 964, Box CBCB55
Türkel, D. Siegfried	Chiffrieren mit Geräten und Maschinen Vlg. Ulr. Mosers Buchhandlung, Graz, 1927
Twinn, Peter	The Abwehr Enigma, In: Hinsley/Stripp, S. 123 - 131
Ulbricht, Heinz	ENIGMA - Uhr In: Cryptologia, Vol. 23, No. 3, 1999, S. 193 - 205
Welchman, Gordon a)	From Polish Bomba to British Bombe, The Birth of Ultra In: Intelligence and National Security, Bd. 1, No. 1, 1986, S. 71 - 110
Welchman, Gordon b)	The Hut Six Story. Breaking the Enigma Code McGraw Hill Book Company, 1982, ISBN 0-07-069180-0
West, Nigel	GCHQ, The Secret Wireless War, 1900-1986 Weidenfeld & Nicholson, London, 1986, ISBN 0-297-78717-9
Whitehead, Dvid	Cobra and other Bombes In: Cryptology, Vol. 20, No.4, 1996, S. 289 - 307
Winterbotham, Frederick	Aktion Ultra. Deutschlands Code-Maschine half den Alliierten siegen (übersetzt v. G. Stiller) Moewig Taschenbuch Nr. 4340, 1976
Woytak, Richard, A.	A Conversation with Marian Rejewski, (übersetzt v. Chr. Kasparek) In: Cryptologia, Vol. 6, No. 1, 1982, S. 50 - 60
Y'Blood, W.	Hunter–Killer: US Escort Carriers in the Battle of the Atlantic Annapolis: Naval Institute Press, 1983

Index