TADEUSZ LISICKI

Die Leistung des polnischen Entzifferungsdienstes bei der Lösung des Verfahrens der deutschen »Enigma«-Funkschlüsselmaschine

1. Einführung

Nach dem Ende des Ersten Weltkrieges, 1918, gelang es dem polnischen Dechiffrierdienst ohne weiteres, die russischen und deutschen Schlüssel zu lösen. Es ist kaum bekannt, daß während des russisch-polnischen Krieges 1919–1920, vor allem beim Sieg über die russische Armee im August 1920, die Funkaufklärung eine bedeutende Rolle gespielt hat. Sie hält einen Vergleich mit der Rolle »Ultras« im Nordafrikafeldzug im Zweiten Weltkrieg sehr wohl aus. Während der russischen Offensive im Sommer 1920 kannte der polnische Generalstab aufgrund der aufgefangenen und entzifferten Funksprüche alle von Tuchačevskij an die Armeebefehlshaber herausgegebenen Befehle und wußte, daß Trotzkij diese befürwortete. Auch wurden viele der von den Armee- und Divisionsbefehlshabern gesendeten Sprüche entziffert, so daß der Oberste Befehlshaber der Polen sich ein klares Bild von den Plänen und Möglichkeiten des Feindes machen konnte.

Die deutschen von dem Reichsheer und der Marine benutzten Schlüssel waren leicht zu lösen, und von 1918 bis zur Einführung des »Enigma«-Schlüssels konnten alle Sprüche mitgelesen werden. Der polnische Dechiffrierdienst kannte die im Handel erhältliche Enigma-Maschine, erwarb eine und erhielt aus nachrichtendienstlichen Quellen einige Angaben über ihre militärische Version. Als die Deutschen den »Enigma«-Schlüssel einführten, war es dem polnischen Dechiffrierdienst jahrelang unmöglich, ihn zu lösen. Die üblichen Dechiffriermethoden waren einem Maschinenschlüssel gegenüber machtlos, da die Buchstaben in einem damit verschlüsselten Text gleichmäßiger verteilt waren und es keine Wiederholungen längerer Buchstabenfolgen gab. Eine Ausnahme bildeten die ersten sechs Buchstaben, die häufig wiederholt wurden. Es war offensichtlich, daß diese ersten Buchstaben eine besondere Bedeutung hatten.

Mehrere Jahre lang kam der polnische Dechiffrierdienst nicht voran; der »Enigma«-Schlüssel schien unlösbar zu sein. Als man sich entschloß, »BS4« (die Abteilung für deutsche Schlüssel und Sprüche) zu verstärken, legte man Wert darauf, junge Leute einzustellen, die frei waren von schematischem Denken und über gute Kenntnisse in der Mathematik und der deutschen Sprache verfügten. An der Universität von Posen wurde ein besonderer Kurs für Kryptologen eingerichtet, der von zwanzig Studenten der letzten beiden Jahre der mathematischen Fakultät besucht wurde. Drei von ihnen, M. Rejewski, J. Rozycki und H. Zygalski, stießen im Herbst 1932 zum BS4. So konnte ein Team gebildet werden, dem es in relativ kurzer Zeit gelang, den »Enigma«-Schlüssel zu lösen. Es war ein großer Erfolg für die Kryptologen, und ich möchte kurz beschreiben, wie er zustande kam.

Jerzy Rozicki, einer der vier jungen polnischen Mathematiker, die das Enigma-Verfahren lösten.

Lt. Colonel (ret.) Dr. Tadeusz Lisicki, London, war polnischer Offizier zunächst im polnischen Entzifferungsdienst; später war er in Frankreich und England, in Zusammenarbeit mit den dortigen Entzifferungsdiensten, tätig.

Um mit der »Enigma«-Maschine verschlüsselte Sprüche entziffern zu können, war es nötig, über eine solche Maschine zu verfügen und ihre Einstellungen (Schlüssel) zu kennen. Die Deutschen glaubten, daß der »Enigma«-Schlüssel bei richtiger Anwendung völlig sicher sei; sie waren sich allerdings der Gefahr bewußt, daß im Kriegsfall die Maschine und ihre Schlüssel in Feindeshand fallen könnten. Sie rechneten aber nicht damit, daß man durch die Anwendung neuer Entzifferungsmethoden, unter Ausnutzung einiger Eigenschaften der Maschine, der Schwächen der Betriebsanleitung sowie der Fehler der Schlüßler, den Schlüssel nur anhand aufgefangener Sprüche würde lösen können. Der polnische Dechiffrierdienst machte sich alle diese Gegebenheiten relativ früh zunutze und konnte den »Enigma«-Schlüssel bereits Anfang 1933 lösen. Die deutschen Schlüsselexperten waren allerdings sehr vorsichtig und nahmen während der ganzen Vorkriegszeit Änderungen vor mit dem Ziel, den Schlüssel ständig zu verbessern. Die Polen fanden alle diese Änderungen schnell heraus und entwickelten immer neue Methoden.

Bild 1: Tagesschlüssel

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 nuz 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 Chifffriermaſchine getaſtet, ſondern willkürlich gewählt worden.

2. Die Verschlüsselung

Die Betriebsanleitung vom 8. Juli 1937 legte den Einstellvorgang fest. Auf Bild 1 sehen Sie den Tagesschlüssel für den 4. Mai. Nach diesem Schlüssel mußte der Schlüßler folgende vier Arbeitsgänge ausführen:

Walzenlage:
- Chiffrierwalzen mit der Welle herausnehmen und in der im Tagesschlüssel angegebenen Reihenfolge darauf anordnen, d. h. Walze II rechts, Walze III in der Mitte, Walze I links; dann zusammen mit der Welle wieder einsetzen.

Ringstellung:
- den Ring auf der Walze I auf Stellung 16 (oder Buchstabe P), Ring auf Walze III auf Stellung 11 (Buchstabe K) und Ring auf Walze II auf Stellung 13 (Buchstabe M) bringen.

Grundstellung:
- Deckel schließen und mit Hilfe der vorstehenden Rändelscheiben die Chiffrierwalzen wie folgt einstellen: 1 (A) auf der linken, 12 (L) in der mittleren und 22 (V) auf der rechten Walze; diese Zahlen (Buchstaben) entsprechen der Grundstellung.

Steckerverbindung:
- mit Hilfe der Doppelsteckerschnüre Buchse C mit Buchse O, D mit I, F mit R, H mit U, J mit W, L mit S und schließlich T mit X verbinden.

Nachdem er die Maschine so gemäß dem Tagesschlüssel eingestellt hatte, wählte der Schlüßler willkürlich drei Buchstaben, die dann zum Spruchschlüssel wurden, und tippte sie zweimal ein. Das sind sechs Buchstaben, die im Lampenfeld aufleuchteten. So erhielt er beispielsweise für den Spruchschlüssel XFR die Buchstaben hfi klb als zusätzliche Verschlüsselung; diese schrieb er an den Anfang des Spruches. Danach stellte er die Chiffrierwalzen so ein, daß die Buchstaben XFR in den drei Fenstern erschienen und begann mit der Verschlüsselung des Spruches. Den verschlüsselten Text notierte er und schrieb an den Anfang die Buchstaben des Spruchschlüssels.
Die Entschlüsselung verlief in umgekehrter Reihenfolge.

3. Die Eigenschaften des Enigma-Schlüssels aus der Sicht der Entzifferer

Aus der Beschreibung der Maschine wissen wir, daß die mittlere Walze pro Umdrehung der rechten Walze eine sechsundzwanzigstel Umdrehung machte, d.h. nachdem 26 Buchstaben getippt waren, hatte sie eine Umdrehung vollendet. Daraus ergibt sich, daß nach Eingabe der Buchstaben, die zur zweimaligen Verschlüsselung des Spruchschlüssels nötig waren, in 21 von 26 Fällen, d.h. in ungefähr 81 %, die mittlere Walze sich nicht bewegt und die linke Walze ihre Stellung nicht verändert hatte. Daraus wiederum folgt, daß sie zusammen mit der Umkehrwalze als eine einzige, quasifeststehende Walze betrachtet werden konnten. Diese Tatsache war von größtem Nutzen bei der Entdeckung der inneren Verbindungen der rechten Walze.
Die Anordnung der Walzen auf der Welle konnte geändert werden; das deutsche Verfahren schrieb eine häufige derartige Änderung vor, was zur Folge hatte, daß verschiedene Walzen in die rechte Stellung gebracht wurden. Die Methode, die zur Entdeckung der inneren Verbindungen der rechten Walze führte, ermöglichte es den Kryptologen, auch die Verbindungen der anderen Walzen herauszufinden.
Bis 1938 wurde die Grundstellung für alle Teilnehmer eines bestimmten Netzes für eine gewisse Zeit im voraus festgelegt, und alle Spruchschlüssel wurden von der gleichen Stellung aus verschlüsselt. Die Kenntnis der Grundstellung war zur Entzifferung der Spruchschlüssel notwendig, doch die polnischen Kryptologen arbeiteten eine Methode aus, mit der diese Schlüssel anhand der Textanfänge gelöst werden konnten. Damit wurde die Kenntnis der Grundstellung überflüssig. 1938 änderten die Deutschen den Verschlüsselungsvorgang; der Schlüßler wählte willkürlich eine Grundstellung, setzte sie an den Spruchanfang und nahm erst dann die zweifache Verschlüsselung vor. Während des Krieges wurde die Doppelverschlüsselung durch die einfache ersetzt. Die Doppelverschlüsselung war ein großer Fehler gewesen, den die Polen voll ausgenutzt hatten.
Ein interessantes Beispiel für einen Fehler ist die Lösung des Schlüssels des SD, der für die Handverschlüsselung eines Textes verwendet wurde, bevor dieser mit der Maschine verschlüsselt wurde. Diese Lösung wiederum führte zu der Entdeckung der inneren Verbindungen der vierten und fünften Chiffrierwalze. Als die Sprüche des SD mit der »Enigma« verschlüsselt wurden, konnten die Polen diese nicht mehr

mitlesen, obwohl sie die Tages- und Spruchschlüssel kannten. Man nahm deshalb an, der SD verwende ein besonderes Verfahren, bis in einem der Sprüche das Wort *Eins* auftauchte, während der übrige Text unverständlich blieb. Offenbar hatte der Schlüßler einen handverschlüsselten Text bekommen, der die Ziffer 1 im Klartext enthielt. Da die Maschine keine Ziffern hatte, hatte der Schlüßler das Zahlwort eingegeben. Nun erkannte man, daß der ganze übrige Text vorher chiffriert worden war. Die Lösung des betreffenden Schlüssels war für die Polen dann eine relativ leichte Aufgabe, doch sie hatte noch weitere Folgen. Als das deutsche Heer und die Luftwaffe 1938 die bisher gesperrte vierte und fünfte Walze in Betrieb nahmen und das Verfahren für die Verschlüsselung des Spruchschlüssels änderten, führte auch der SD die zusätzlichen Walzen ein, blieb aber bei der gleichen Grundstellung für den Spruchschlüssel. Dieser Fehler führte dazu, daß die inneren Verbindungen der vierten und fünften Walze nach der gleichen Methode entdeckt werden konnten, die bei der »Enigma« mit drei Walzen verwendet worden war.

4. Die Lösung des Spruchschlüssels

In den ersten Jahren nach der Einführung der Maschine verwendeten die Deutschen das oben beschriebene Verfahren für die Verschlüsselung des Spruchschlüssels. Der Spruchschlüssel jedes Spruches innerhalb eines bestimmten Netzes wurde zweimal mit dem gleichen Tagesschlüssel, d.h. mit der gleichen Maschineneinstellung und der gleichen Grundstellung verschlüsselt, welche den Kryptologen beide nicht bekannt waren. Trotzdem und ohne eine genaue Kenntnis der Maschine war es möglich, den Spruchschlüssel zu lösen. Dabei half der Umstand, daß die deutschen Schlüßler damals oft charakteristische Schlüssel verwendeten, beispielsweise AAA, SSS, QWE usw. Später wurde diese Art der Schlüssel verboten, das Verbot kam jedoch zu spät, denn mit Hilfe der charakteristischen Schlüssel war es den Polen gelungen, die Spruchschlüssel zu lösen.
Nehmen wir einmal an, den Kryptologen lagen 65 Sprüche vor, deren erste sechs Buchstaben die doppelt verschlüsselten Spruchschlüssel sind. (Bild 2)
Zur besseren Übersicht sind die sechs Buchstaben in Dreiergruppen dargestellt, zuerst die erste, dann die zweite Verschlüsselung. Der

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 scv	48.	use nwh	61.	ypc osq
10.	hno thd	23.	nxd qtu	36.	syx scv	49.	vii poh	62.	ypc osq
11.	hxv tti	24.	nxd qtu	37.	syx scv	50.	vii poh	63.	zzy yra
12.	ikg jkf	25.	nlu qfz	38.	syx scv	51.	vii poh	64.	zef yoc
13.	ikg jkf	26.	obu dlz	39.	syx scv	52.	vqz pvr	65.	zsj ywg

AD = (a) (s) (bc) (rw) (dvpfkxgzyo) (eijmunqlht)

BE = (blfqveoum) (hjpswizrn) (axt) (cgy) (d) (k)

CF = (abviktjgfcqny) (duzrehlxwpsmo)

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

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

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

Bild 2: 65 doppelt verschlüsselte Spruchschlüssel und die entsprechenden Zyklen

Klartext beider Gruppen war gleich, also entspricht der erste Buchstabe dem vierten, der zweite dem fünften und der dritte dem sechsten. Ein genauerer Vergleich der Anfänge der Sprüche zeigt, daß, wenn ihre jeweils ersten Buchstaben gleich sind, auch ihre jeweils vierten dieselben sind. Beispielsweise beginnen Nummer 2 und Nummer 3 jeweils mit b, ihre vierten Buchstaben sind jeweils ein c. Viele Sprüche fangen mit dem gleichen Buchstaben an, z.B. Nummer 9 und Nr. 10, Nr. 12 und Nr. 13 usw. Da es in einem Alphabet mit 26 Buchstaben 26x26x26 = 17576 verschiedene Dreiergruppen gibt, müßten Sprüche mit den gleichen Anfangsbuchstaben äußerst selten sein. Dies war aber nicht der Fall, denn es tauchten viele Wiederholungen in den täglich aufgefangenen Sprüchen auf, so daß die Schlüßler offensichtlich Schlüssel wie AAA, ABC usw. verwendeten.

Der erste und vierte Buchstabe des Spruches Nr. 1 sind identisch, es handelt sich um das a. Der Schlüßler hatte einen dem Kryptologen unbekannten Buchstaben gewählt, der zweimal den gleichen Schlüsselbuchstaben ergab, es gab also einen Ein-Buchstaben-Zyklus (a). Aufgrund eines von Rejewski ausgearbeiteten Lehrsatzes wissen wir, daß es deshalb noch einen solchen Zyklus geben muß. Aus Spruch Nr. 35 geht hervor, daß es sich um den Zyklus (s) handeln muß. Aufgrund des Prinzips der Wechselseitigkeit handelt es sich bei dem ersten Buchstaben des Spruches Nr. 1 um ein s und bei dem von Nr. 35 um ein a. Die Ein-Buchstaben-Zyklen nannten die britischen Kryptologen »female« (weiblich).

Geht man bei Spruch Nr. 3 und Nr. 4 ähnlich vor, stellt man fest, daß der erste Buchstabe von Nr. 3 ein b ist, der an der vierten Stelle zu c wird, während bei Nr. 4 c zu b wird. Hier handelt es sich also um einen Zwei-Buchstaben-Zyklus (bc). Ein weiterer Zwei-Buchstaben-Zyklus wird von den ersten und vierten Buchstaben (rw) gebildet.

Wenn man die nächsten Sprüche untersucht, in denen keine Buchstaben der vorhergehenden Zyklen auftauchen, und mit Spruch Nr. 5 beginnt, bei dem d zu v wird, stellt man fest, daß in Nr. 49 v zu p, in Nr. 27 p zu f usw. wird, bis wir bei Nr. 61, wo y zu o wird, und schließlich bei Nr. 26 anlangen, wo o zum ersten Buchstaben des Zyklus, nämlich zu d, wird und damit folgenden Zyklus schließt:

(d v p f k x g z y o)

In ähnlicher Weise erhalten wir noch einen Zehn-Buchstaben-Zyklus, der mit e beginnt, einem Buchstaben, der bisher noch in keinem Zyklus auftaucht. Dadurch erhalten wir:

(e i j m u n g l h t)

Der Wechsel vom ersten zum vierten Buchstaben ist eine AD-Permutation.

AD = (a)(s)(bc)(rw)(dvpfkxgzyo)(eijmunglht)

Gehen wir mit den zweiten und fünften Buchstaben ähnlich vor, erhalten wir das Produkt BE, während wir aus den dritten und sechsten Buchstaben das Produkt CF erhalten. (s. Bild 2)

Wenn wir annehmen, daß die Sprüche Nr. 35 bis 39 die Buchstaben AAA als Schlüssel haben, müssen die Zyklen wie unten auf Bild 2 angegeben angeordnet werden, um die Schlüssel aller Sprüche lösen zu können. Der Schlüssel des ersten Spruches, der in der ersten Verschlüs-

---

auq amn : SSS	khb xjv : LLL	taa exb : PYX
bnh chl : RFV	ldr hde : KKK	use nwh : ZUI
bct cgj : RTZ	maw uxp : YYY	vii poh : EEE
cik bzt : WER	nxd qtu : GGG	vqz pvr : ERT
ddb vdv : IKL	nlu qfz : GHJ	wtm rao : CCC
ejp ips : VBN	obu diz : JJJ	wki rkk : CDE
fbr kle : HJK	pvj feg : TZU	xrs gnm : QQQ
gpb zsv : NML	qga lyd : XXX	xio guk : QWE
hno thd : FFF	rjl wpx : BBB	xyw gcp : QAY
hxv tti : FGH	rfc wqq : BNM	ypc osq : MMM
ikg jkf : DDD	syx scw : AAA	zzy yra : UVW
ind jhu : DFG	sjm spo : ABC	zef yoc : UIO
jwf mic : OOO	sug smf : ASD	zsj ywg : UUU
	tmn eby : PPP	

Bild 3: Entzifferte Spruchschlüssel

selung auq lautete, heißt SSS, da der Buchstabe s beim Ein-Buchstaben-Zyklus unter dem Buchstaben a steht, da im umgeordneten BE-Zyklus u über S und im CF-Zyklus q auch über S steht. Auf gleiche Weise erhalten wir für die übrigen Sprüche die Schlüssel, die Sie auf Bild 3 finden.

Als die Deutschen 1933 die Verwendung der charakteristischen Schlüssel verboten, konnte eine neue, einfache Methode erarbeitet werden, die sich dieses Verbot zunutze machte und auf den oben beschriebenen Zyklen (AD, BE, CF) basierte.

Bild 3 zeigt nicht nur die entzifferten Spruchschlüssel, sondern auch sechs vollständige Schlüsselalphabete und deren Klartexte. Durch ihre geschickte Auswertung und die Anwendung höherer Mathematik gelang es den Polen, die »Enigma«-Maschine nachzubauen und Methoden zur Lösung der Tagesschlüssel zu finden.

5. Die Rekonstruktion der inneren Verbindungen der Maschine

Der Verlauf, den der Strom von der Tastatur zur Lampe nimmt, kann als Gleichung aus dem Produkt der Permutationen ausgedrückt werden. Wenn wir den Buchstaben A zur Bezeichnung der von der Maschine beim Druck auf eine beliebige Taste bewirkten Permutation verwenden, dann ist er das Produkt der Permutationen, von denen jede dem Verlauf des Stroms durch die einzelnen, in Bild 4 gezeigten Abschnitte entspricht, und auch der Permutation, die wir P nennen und die einem Sechsundzwanzigstel einer Walzenumdrehung entspricht.

Wir bezeichneten die durch die Steckerverbindung bewirkte Permutation mit S, die Permutationen der Chiffrierwalzen in der Reihenfolge von links nach rechts L, M und N und die Permutation der Umkehrwalze mit R. Die Permutation A und die Permutationen der nächsten fünf getasteten Buchstaben, B, C, D, E und F, sehen Sie auf Bild 5.

Diese Gleichungen sind dann richtig, wenn wir annehmen, daß die mittlere Walze sich nicht bewegt hat, eine relativ sichere Annahme, da sie sich in 21 von 26 Fällen nicht dreht; dadurch ist es möglich, die Walzen R, L und M als eine einzige, feststehende Walze R zu betrachten.

In den obigen Gleichungen ist die linke Seite unbekannt, nur die Produkte AD, BE und CF sind bekannt.

Um die inneren Verbindungen der Walzen herauszufinden, muß diese Reihe von sechs Gleichungen gelöst werden, eine außergewöhnlich

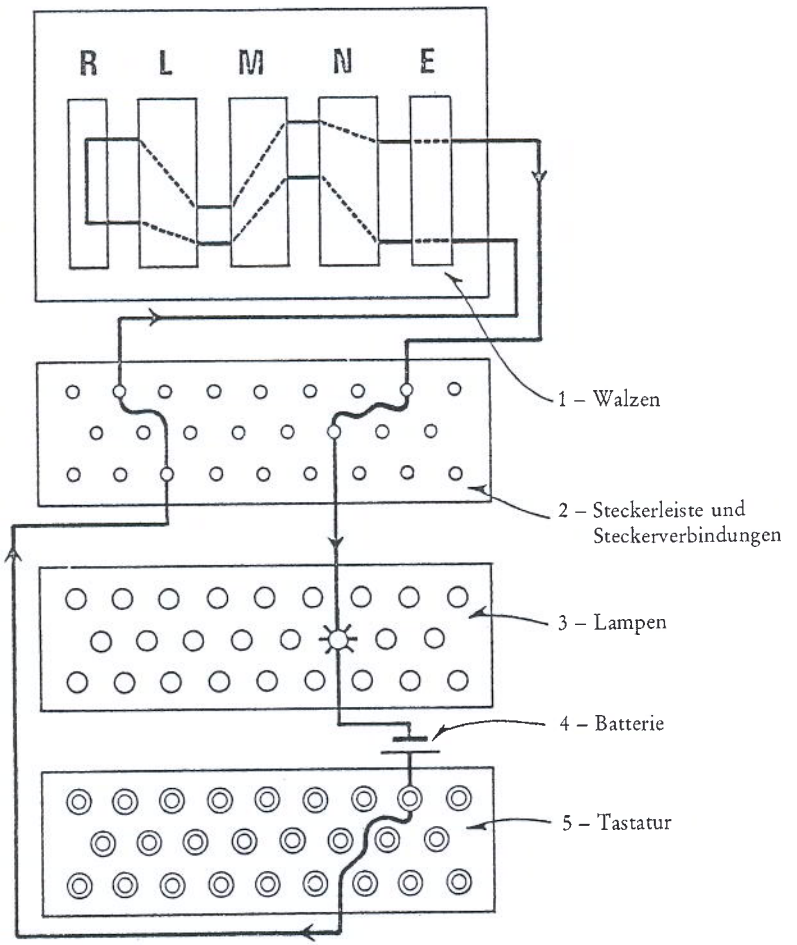

Bild 4: Blockdiagramm der Enigma-Maschine

$A = S\ N\ M\ L\ R\ L^{-1}\ M^{-1}\ N^{-1}\ S^{-1}$

$B = S\ P\ N\ M\ L\ R\ L^{-1}\ M^{-1}\ N^{-1}\ P^{-1}\ S^{-1}$

$C = S\ P^{2}\ N\ M\ L\ R\ L^{-1}\ M^{-1}\ N^{-1}\ P^{-2}\ S^{-1}$

$D = S\ P^{3}\ N\ M\ L\ R\ L^{-1}\ M^{-1}\ N^{-1}\ P^{-3}\ S^{-1}$

$E = S\ P^{4}\ N\ M\ L\ R\ L^{-1}\ M^{-1}\ N^{-1}\ P^{-4}\ S^{-1}$

$F = S\ P^{5}\ N\ M\ L\ R\ L^{-1}\ M^{-1}\ N^{-1}\ P^{-5}\ S^{-1}$

Bild 5: Permutationen der Buchstaben A, B, C, D, E, F.

schwierige Aufgabe, die dadurch vereinfacht wurde, daß der französische Nachrichtendienst uns eine Liste mit allen Schlüsseln für einen Zeitraum von zwei Monaten zur Verfügung stellte. Für diese Zeit kannten wir also die Steckerverbindungen, d. h. die Permutation S. Durch die Lösung dieser Gleichungen erhielten wir die inneren Verbindungen der Chiffrier- wie auch der Umkehrwalzen. Dadurch konnte die deutsche »Enigma«-Maschine nachgebaut werden.

6. Die Rekonstruktion der Tagesschlüssel

Zum Mitlesen eines ganzen Spruches reichte es nicht, über eine Schlüsselmaschine zu verfügen und die Spruchschlüssel rekonstruieren zu können. Es war wichtig, Methoden zu erarbeiten, mit denen die Einstellung der Maschine in Erfahrung gebracht werden konnte, d. h. mit denen man die Tagesschlüssel rekonstruieren konnte. Eine ganze Reihe solcher Methoden, einfache und komplizierte, manuelle und mechanische, billige und teuere, wurden entwickelt, von denen ich nur einige beschreiben möchte.

Um die Lage und Stellung der Walzen und der Steckerverbindungen herauszufinden, bediente man sich einer Kartei, in der die Zahl und Zykluslänge aller möglichen Walzenstellungen verzeichnet waren. Bei drei Walzen handelte es sich um 105456. In den Beispielen für AD, BE und CF beeinflußt die Permutation S nur die Buchstaben innerhalb des Zyklus, der gesamte Zyklus an sich bleibt unverändert. Es genügte deshalb, die Produkte von AD, BE und CF an einem bestimmten Tag mit ähnlichen Produkten in der Kartei zu vergleichen, um die erforderlichen Elemente für den Tagesschlüssel zu erhalten. Das dauerte nur ein paar Minuten.

Um das Verfahren zu beschleunigen, wurde ein sogenannter Zyklometer (Bild 6) gebaut. Er bestand aus zwei miteinander verbundenen »Enigma«-Maschinen, denen die Tastatur fehlte und die nur über die inneren Verbindungen und die Lampen verfügten, von denen einige entsprechend einer doppelten Zykluslänge in einer bestimmten Stellung aufleuchteten.

Am 15. September 1938 führten die Deutschen beim Heer und bei der Luftwaffe ein neues Schlüsselsystem ein. Etwas später, am 15. Dezember, fügten sie eine vierte und fünfte Walze hinzu.

Deswegen mußten Wege gefunden werden, um mit dieser neuen Situa-

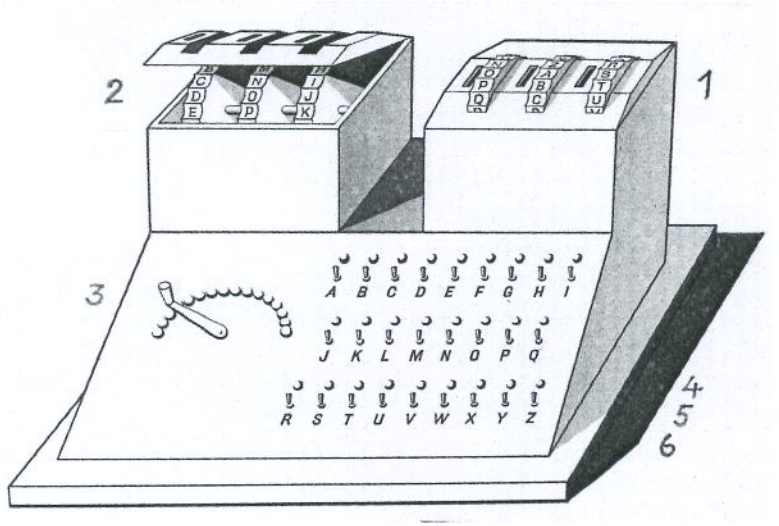

Bild 6: Polnischer Zyklometer: 1 „Enigma"-Walzen mit geschlossenem Deckel, 2 „Enigma"-Walzen mit geöffnetem Deckel, 3 Rheostat, 4 Lampen, 5 Schalthebel, 6 Alphabet
(Rekonstruktion: T. Lisicki)

tion fertig zu werden. Diese Aufgabe wurde schnell gelöst. Eine rein mechanische Methode, die sich auf eine Maschine mit der Bezeichnung »Bomba« stützte, war schon im November 1938 fertig. Die Entwicklung einer zweiten Methode, die auf Lochkarten beruhte, brauchte etwas länger. Wie bereits erwähnt, gelang es dank dem Schlüssel des SD, die inneren Verbindungen der vierten und fünften Walze herauszufinden.

Die neue Verschlüsselungsmethode unterschied sich von der alten darin, daß nicht mehr dieselbe Grundstellung für den ganzen Tag benutzt wurde, sondern jeder Spruch seine eigene, willkürlich vom Schlüßler gewählte erhielt, von der ausgehend er, wie zuvor, den Spruchschlüssel zweimal verschlüsselte. Der Schlüßler schrieb oben auf den Spruch Buchstaben in Dreiergruppen, von denen die erste unverschlüsselt die willkürlich gewählte Grundstellung angab, während die anderen den doppelt verschlüsselten Spruchschlüssel darstellten. Obwohl die Produkte AD, BE und CF nicht mehr gegeben waren, gab es weiterhin eine Beziehung zwischen dem ersten und vierten, dem zweiten und fünften sowie dem dritten und dem sechsten Buchstaben des verschlüsselten Spruchschlüssels, und beide Methoden machten sich diese Beziehung zunutze. Wenn also der erste Buchstabe eines Spruchschlüssels nach der ersten und auch nach der zweiten Verschlüsselung zu W wurde, so handelte es sich um einen Ein-Buchstaben-Zyklus.

Wenn wir nun annehmen, daß der Buchstabe W durch die Steckerverbindungen nicht geändert wurde, so muß jede Stellung der Maschine für W danach untersucht werden, ob innerhalb von drei Buchstaben der gleiche Buchstabe auftaucht.

Anstatt je drei Buchstaben herauszuschreiben und zu prüfen, kann man natürlich auch eine Maschine bauen, die automatisch alle Stellungen sehr viel schneller durchläuft und an der richtigen Stelle stehenbleibt. Es wurden sechs solcher Maschinen, je eine für jede Walzenlage, gebaut und »Bomba« genannt.

Die Maschinen benötigten nur 110 Minuten, um anhand von drei Paaren verschlüsselter Spruchschlüssel mit Ein-Buchstaben-Zyklen (females) die Walzenlage und die Stellung aller Walzen herauszufinden.

Auf Bild 7 sehen Sie die Abbildung einer polnischen Bomba.

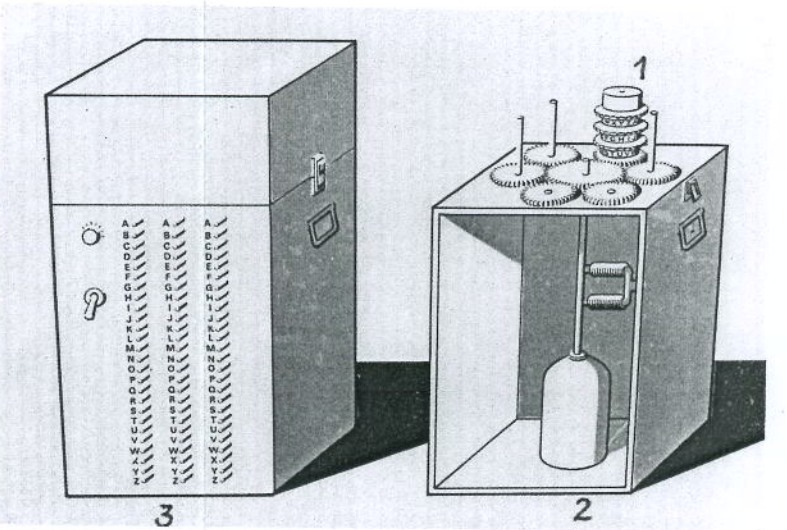

Bild 7: Polnische Bomba: 1 „Enigma"-Walzenlage mit drei Schlüsselwalzen, auf den restlichen fünf äußeren Zahnrädern sind die anderen bei drei verwendeten Walzen möglichen Walzenlagen angeordnet; 2 Elektromotor; 3 geschlossener Kasten mit drei Reihen Schalthebeln.
(Rekonstruktion: T. Lisicki)

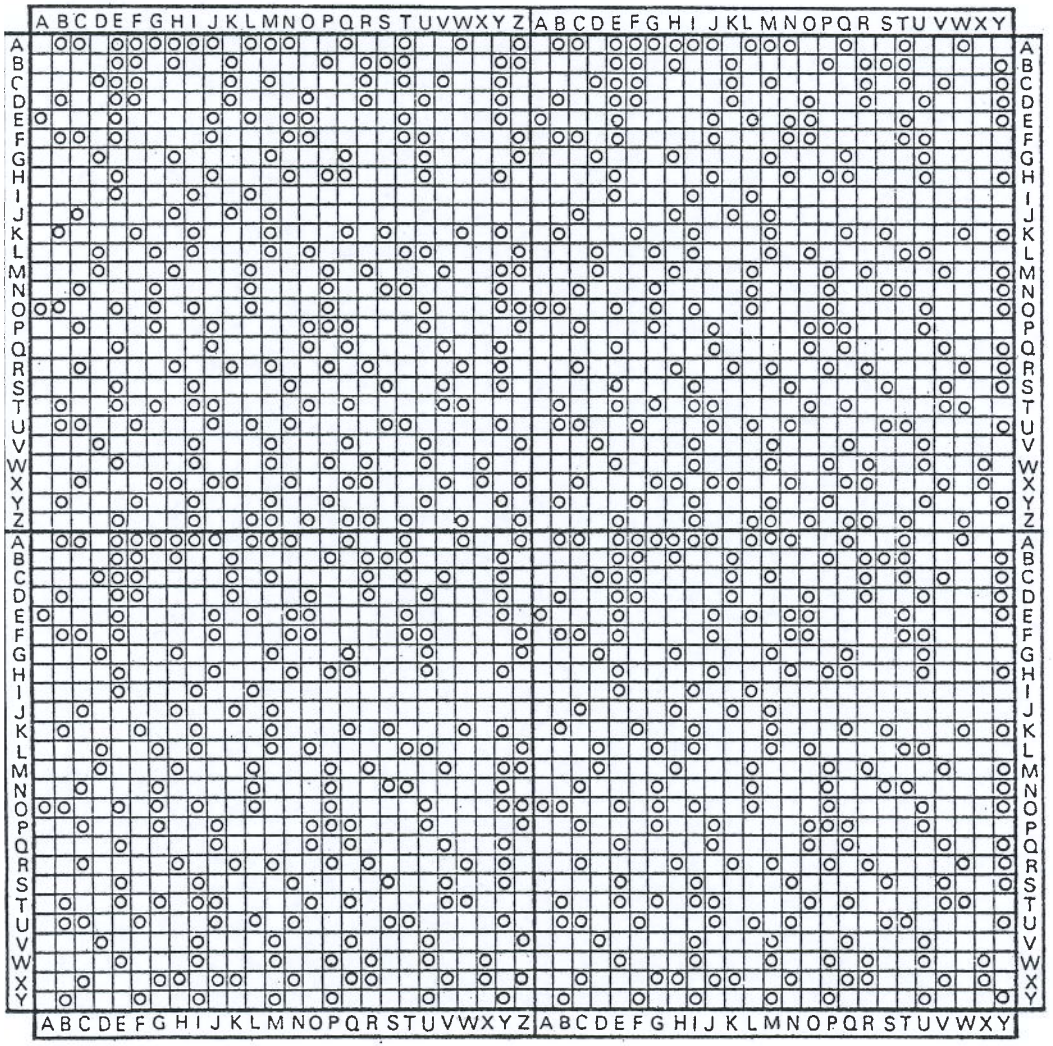

Bild 8: Lochkarte

Mit der Lochkartenmethode erhielt man Ergebnisse, ohne die Steckerverbindungen beachten zu müssen. Sie ging ebenfalls von den »females« aus.
Für jede Stellung der Walze N wurde eine Karte mit 26 x 26 Quadraten, entsprechend aller möglichen Stellungen der Walzen L und M gefertigt. Die Quadrate der »female«-Stellungen wurden gelocht, die anderen nicht. Für jede Walzenlage benötigte man 26 Karten. Wenn beispielsweise an einem bestimmten Tag die Spruchschlüssel sechs »female« Paare enthielten, dann mußten die sechs entsprechenden Karten herausgesucht werden.

Diese wurden aufeinandergelegt und in einer bestimmten Weise angeordnet. Für die praktische Anwendung hatten die Karten 51 x 51 Quadrate (s. Bild 8), damit bei diesem Verfahren kein Kartenteil übersehen wurde. Wenn man sechs Karten von den betreffenden 26 in der richtigen Reihenfolge ordnete, so befand sich ein Loch auf allen sechs Karten an der gleichen Stelle. Die Lage dieses Loches gab die Walzenstellung und die Ringstellung an, und durch einen Vergleich der Buchstaben des Schlüssels und der auf der Maschine konnten auch die Steckerverbindungen herausgefunden werden, d. h. der ganze Tagesschlüssel war bekannt.
Nachdem die Deutschen die Zahl der Walzen auf fünf erhöht hatten, wurden 60 Kartenblocks zu je 26 Karten benötigt.
Im Juli 1939 wurden die Erkenntnisse über die »Enigma« den britischen und französischen Dechiffrierdiensten als polnischer Beitrag zur gemeinsamen Sache übergeben, und je eine von den Polen gebaute »Enigma«-Maschine wurde nach Paris und London geschickt.