~~TOP SECRET CREAM~~

ARMY SECURITY AGENCY

Washington, D. C.

EUROPEAN AXIS SIGNAL INTELLIGENCE IN WORLD WAR II AS REVEALED BY "TICOM" INVESTIGATIONS AND BY OTHER PRISONER OF WAR INTERROGATIONS AND CAPTURED MATERIAL, PRINCIPALLY GERMAN

COMMENTS

VOLUME 2--NOTES ON GERMAN HIGH LEVEL CRYPTOGRAPHY AND CRYPTANALYSIS

Prepared under the direction of the

CHIEF, ARMY SECURITY AGENCY

1 May 1946

WDGAS-14

~~TOP SECRET CREAM~~

Volume 2

NOTES ON GERMAN HIGH LEVEL CRYPTOGRAPHY AND CRYPTANALYSIS

Volume 2

Chapter I The Paradox of German High-Level Cryptography

1. German high-level cryptographic systems were insecure, although brilliantly conceived-- German high-level cryptography was brilliantly conceived (as will be shown in this volume) but more brilliantly conceived cryptanalytic procedures and large expenditures in manpower and machinery by the United States and Brisish Governments, in one of the most dramatic chapters of World War II, accomplished daily solutions of German high-level systems that cost Germany heavily, if they did not, as some believe, bring about actual defeat. For instance:

a. The German Air Force lost the Battle of England in 1940, partly because it entrusted bomber-target information to the insecure Air Force Enigma.[1] Unknown to and even unsuspected by the Germans, their operations from this date on were constantly embarrassed by the cryptographic insecurity of this machine.

b. The German Army suffered terrific casualties and losses of materiel in Africa and on the continent because of blind faith in two of its high level military cryptographic machines: the Army Enigma, and the teleprinter cipher attachment "SZ-42." Both were insecure.[2]

[1]The great debt England owes its cryptanalysts is to be recorded in a history of the Government Code and Cypher School, London, to be available in the fall of 1946. The statement here is based on verbal information from intelligence officers and cryptanalysts of the School, and awaits proper documentation. This history will also include data regarding the German Army and Navy Enigmas.

[2]A written report by Brigadier E. T. Williams, chief intelligence officer to Field Marshall Montgomery, 5 October 1945, to be included in the Government Code and Cypher School history, gives specific examples bearing out this statement.

c. The German Navy lost a staggering number of submarines for a similar reason: insecurity of the Enigma, Navy version.[3]

d. The German Foreign Office employed three main systems, all insecure. Two of them (the Deutsches Satzbuch unenciphered, and the Deutsches Satzbuch enciphered by "Floradora,") were read during the war; the third system (a "one time pad," Army Security Agency trigraph "GEE") was read only in the last six months of war, but gave information of much military value against the Japanese.

2. German military cryptographers had secure cipher devices under development-- It is a paradox that German high-level cryptography was a "practical" failure and at the same time German military cryptographers had so many secure devices in various stages of development.

a. One simple item alone, a "variable-notch" rotor, would probably have prevented Anglo-American attempts at reading the Enigma after 1942, if it had been produced in quantity and installed. This rotor was called "Lueckenfuellerwalze."[4]

[3]The real truth behind these losses has been and still is at this writing (May 1946) so carefully concealed that the following statement by Admiral Doenitz in the Nuremberg trial is of considerable interest: "The Battle of the Atlantic was nearly won prior to July 1942, when German losses were within reasonable limits. But they jumped 300 per cent when Allied aircraft, aided by radar, which came like an epileptic stroke, were used in the fight." He reported 640 to 670 submarines and 30,000 men lost as a result of British and American action. (See IF 259). A captured, unsigned, naval report dated 1944, evidently sent to the Navy High Command regarding cipher security, stated: "... . the high degree of efficiency of the enemy's aircraft Radar, so often surprising, has received remarkable and decisive assistance from directions based on the results of the direction finding service." (See IF 142). It was never realized that cryptanalysis, rather than radar and direction finding, disclosed the positions and intentions of the German submarines.

[4]M 11; I 104 pp 2,3

b. An irregular-drive Enigma that would have defied all presently known methods of solution, was being developed. This was called "Cipher Device 39" ("Schluesselgeraet 39," abbreviated "SG-39").[5]

c. An improved "cipher teleprinter" had been built, installed on several circuits, and used, which prevented easy reading of teleprinter messages in depth; and even if this reading in depth was accomplished, the machine remained secure against known methods of attack as far as all other messages enciphered by it were concerned. This was called "cipher teleprinter T-52e" ("Schluesselfernschreibmaschine T-52e," abbreviated "SFM T-52e").[6]

d. Apparatus was being developed for "cryptizing" a radio teleprinter circuit--that is, for applying a basic cryptographic process to the circuit itself even before any intelligence is superimposed on the emissions. This was called "cipher attachment 42c" ("Schluesselzusatz 42c," abbreviated "SZ-42c"), which was to be used with a continuously operating, crystal-controlled, synchronized teleprinter.[7]

e. A mechanical, portable, keyboard-operated cipher machine, employing an interacting wheel-motion principle applied to Hagelin-type wheels, had been developed and built and partially distributed, which would have been completely secure against reconstruction even if messages were read in depth. This was called "Cipher Device 41" ("Schluesselgeraet 41," abbreviated "SG-41").[8] It was cryptographically superior to its much smaller U.S. Army equivalent device, Converter M-209.

f. Other devices were also in varying stages of development; these included the "Cipher Box" ("Schluesselkasten"), and the "Cipher Disk" ("Schluesselscheibe"), which were two miniature enciphering devices intended for use by secret agents and by the Army.[9]

[5] I 53

[6] I 20, I 31. In this document the term "cipher teleprinter" will be employed consistently to designate a teleprinter in which the cryptographic mechanism is an integral part of and is contained within the machine itself; the term "teleprinter cipher attachment," to designate an auxiliary cryptographic mechanism associated with the teleprinter but not an integral part thereof.

[7] I 57 E 14

[8] I 72

[9] I 20 I 96

The foregoing devices have been studied and are being studied by cryptographers and cryptanalysts at the Army Security Agency, and the general opinion is that the Germans were making rapid strides toward greatly improving their communications security.

The very least that can be said is that they had something different. Their teleprinter devices employed mechanical cipher wheels, as opposed to the U.S. Army and U.S. Navy use of electrically-wired cipher wheels ("rotors"); furthermore, the mechanical wheel arrangements, in their new devices, were highly developed and secure. They also employed interacting wheel motions (wheels mutually controlling one another) for several of their cipher-teleprinters, as well as for their SG-41 (Hagelin-type machine). Mechanical wheels and interacting wheel motions for teleprinter enciphering devices have long been considered by United States cryptographers; our development along other lines has been from choice. None of our present devices uses interacting motion, and the excellent developments of the Germans not only furnish us greater insight into such possibilities, but also increase greatly our store of knowledge.

3. German security studies revealed only theoretical weaknesses of their cryptography-- German military cryptographers failed to realize that their existing Enigmas and teleprinter cryptographic apparatus were insecure. This was because they were unable, in their security atudies, to put forth the costly practical effort required to solve them. Their security studies were theoretical only,[10] since actual traffic was never obtained for such studies.[11] They were completely without practical knowledge of how successfully a careful and determined attempt at traffic analysis can provide daily "cribs" and other data for cryptanalytic attack; and they had not advanced sufficiently in applied cryptanalysis to realize that determined engineering staffs can produce items like the Polish (later French, later English, later American) "bombe," the U.S. Navy "duenna," the Army Security Agency "autoscritcher," or the British "colossus." The flashes of intuition and inspiration that come from doing, as well as theorizing, were denied them.

[10] I 45 pp 4,5
[11] I 31

A report on naval ciphers dated 10 July 1944, apparently written by the Signal Security Agency of the Navy High Command (OKM/4 SKL/II), stated that solution of the naval Enigma was conceivable, based on "the assumption of extraordinary mechanical outlay on the part of the enemy for cryptographic activities.... though we [OKM/4 SKL/II] can conceive of a machine which would be suitable for this kind of work, we have none available or under consideration, since the whole question does not yet appear to justify undertaking such a difficult special constructional problem."[12] The British did undertake this problem, and were rewarded with astounding success.

4. Interrogation of Anglo-American prisoners failed to disclose German cryptographic weaknesses-- Furthermore, TICOM reveals that Germany never became aware of the Anglo-American solution of German high grade systems. Not even a hint of this fact came to them through their agents, their interrogations of Anglo-American prisoners of war, or their cryptanalysis.

It may be said that Germany lost the cryptologic war even before 1939, in Poland. The Poles invented the "bombe," a device which later, in improved form in England and in America, provided daily solutions of the German plugboard Enigma. The "bombe" secret was almost revealed when three deciphered German messages were found by the Germans in Poland in 1939. The Germans became alarmed and conducted many interrogations;[13] the case was re-opened in 1942 and 1943; but at no time did the Germans learn the real secret of the Poles' success. The Germans became convinced that probably the Enigma indicator system had been at fault (as it partly had been) and since it had already been changed in 1940, they were no longer concerned with the suspected solutions.

Also, there were intelligence officers who feared that Enigma traffic was insecure, but their fears were based only on inference and not on direct proof. Thus, when the Navy High Command became alarmed at mounting submarine losses, the increasing effectiveness of Anglo-American airplane radar was blamed, and the Enigma was exonerated.[14]

[12] IF 142

[13] I 127

[14] See footnote number 3 of this volume.

An intelligence officer attached to the Air Force High Command at the time of the landings in North Africa expressed his suspicions to the Chief Signal Officer of the Air Force, a General Martini, and caused him to reduce "his earlier belief in the 100% security to 80% security,"[15] but his evidence was insufficient to cause the Air Force to discontinue use of the Enigma.

Germany was unable to cryptanalyze British and American high-grade systems carrying cryptanalytic operational information and other ULTRA matters between England and America. As a result she had no hint from cryptanalysis that her own high-grade systems were insecure.

It is absolutely clear that United States and British security regulations applicable to ULTRA were so good and so closely adhered to by all concerned that knowledge of our Enigma-solving and teleprinter-solving operations was kept from the Germans. An interrogation of two of the leading German cryptanalysts, Drs. Huettenhain and Fricke of the Signal Intelligance Agency of the Supreme Command Armed Forces (OKW/Chi), revealed only that:[16]

> "One Allied PW in North Africa had said the United States and British operated with a very large joint 'park' of I.B.M. machinery, but this interrogation was never followed up. No personalities whatever were known."

[15] IF 5
[16] I 84 p 6

Chapter II The Enigma Cipher Machine

5. Enigma cipher machine was the backbone of German high-level cryptography-- The Enigma cipher machine, in five different forms, was used by German commercial firms, by the Post Office, the Railways, and miscellaneous other German government departments; by the Supreme Command of the Armed Forces; by the High Command of the Army, and in Army communications down through division; by the High Command of the Air Force, and in Air Force communications down through group and sometimes squadron; by the High Command of the Navy and in Naval communications down through submarine; by Military Intelligence (Abwehr), by the Reich Security Office (Reichssicherheitshauptamt, abbreviated "RSHA"); and by Military Attachés.

The five main forms in which it appeared were called the commercial (or "K") Enigma; the "counter" (or "Zaehlwerk") Enigma, sometimes called the "Abwehr" Enigma or the "G" Enigma; the plugboard ("Stecker") Enigma; the plugboard with (pluggable) reflector-D ("Stecker mit Umkehrwalze D") Enigma; and the Navy Enigma. The plugboard Enigma with "variable-notch" rotors ("Stecker mit Luenkenfuellerwalzen") was to have appeared soon. Another model, Cipher Device 39 ("Schluesselgeraet 39") was under study. See Chart No. 2-1 herewith.

Enigma Model	Used by	Number of rotors	Number of notches per rotor	Type of reflector	Type of end plate	How machine would be solved
Commercial ("K")	Commercial firms Reichspost Reichsbahn. Misc. govt. depts.	3	1	Rotor, not pluggable	Not pluggable	4 or 5 letter crib and catalogue; or rapid analytic machinery. (Bombe, duenna or scritcher not needed.)
Counter ("Zaehlwerk")	Military attache until 1943; then Reich Security Office	3	Multiple but fixed	Rotor. Not pluggable	Not pluggable	1Ø letter crib and catalogue; or rapid analytic machinery. (Bombe, duenna, or scritcher not needed.)
Plugboard ("Stecker")	Supreme Command Army. Air Force	3 from set of 5	1	Fixed plate Not pluggable	PLUGGABLE	Bombe (duenna or scritcher not needed).
Navy Plugboard	Navy standard machine	3 from set of 8 & 1 from 2	5 with 1 3 with 2 2 with Ø	Fixed plate Not pluggable	PLUGGABLE	Bombe, duenna, or scritcher
Plugboard with pluggable reflector (Umkehrwalze D)	Just beginning to be used by Air Force. Proposed for Armed Forces and for Army	3 from set of 5	1	Fixed plate PLUGGABLE	PLUGGABLE	Duenna or scritcher. VERY DIFFICULT.
Plugboard with variable notch rotors(Luecken-fuellerwalzen)	Proposed for Armed Forces, Army, Navy, Air	3 from set of 5 ?	Multiple, CHANGEABLE and therefore non-predictable	Fixed plate PLUGGABLE or not pluggable	PLUGGABLE	Bombe, duenna, or scritcher (if at all possible)
Cipher Device 39 (Schluessel-geraet 39)	Proposed for Armed Forces, Army, Navy, Air	4 variable notch rotors from set of ?	Multiple, changeable; plus Hagelin type drive	Fixed plate PLUGGABLE	PLUGGABLE	Bombe, duenna, or scritcher (if at all possible).

PROGRESSIVE CHANGES IN GERMAN ENIGMA

Chart No. 2-1

6. "Commercial" Enigma was known to be insecure-- It was well known by the Germans that the commercial Enigma was not difficult to solve. They suggested hand methods of "stripping off the fast-moving rotor," which were almost identical with our methods and which involved small prepared catalogues.[20] They suggested statistical methods using rapid analytic machinery.[21] They had also investigated the machine mathematically, from a "group theory" standpoint.[22] The commercial machine had been, until about 1934, sold on the commercial market by the German firm which owned the patents and developed them; but soon after the Nazi accession into power the machine was withdrawn from the market. The Germans furnished these machines to the Croat puppet government.[23] The Germans themselves used it for their post office, their railroads, and other government agencies. Because of its insecurity, every message enciphered by it was supposed to be re-enciphered at a second setting,[24] a procedure which if adopted would have made the messages quite secure. It is doubtful if such procedure was generally carried out, because of the difficulties involved.[25]

7. "Counter" Enigma was known to be insecure-- The "counter" Enigma (so called because it incorporated a letter counter in its machanism) was important because it introduced multiple-notch rotors. In general, the more often enciphering rotors in machines of the Enigma class step, the more difficult solution becomes, and multiple-notch rotors bring about this desirable motion. Even so, the "counter" machine was known to be solvable by short cribs.[26] Regulations were also issued with this machine to double-encipher each message.[27] Only about 100 of the "counter" machines were made in all; they were issued to German military attachés, withdrawn in 1943, and issued to Military Intelligence (Abwehr). Some were also sold to the Dutch government.[28]

[20] I 47
[21] I 45
[22] T 372
[23] I 92
[24] I 92
[25] I 92
[26] I 77
[27] I 77
[28] I 104

8. Plugboard Enigma was believed safe if used properly--Plugboard Enigma was used by the Supreme Command Armed Forces, by the Army, by the Air Force, and, with an additional rotor, by the Navy, as the ubiquitous and "secure" cipher device, able to carry highest-level traffic "if used properly." It was also supplied to the Hungarians, Rumanians, Finns, and Italians.[29] Investigations by Dr. Pietsch, of the Signal Intelligence Agency of the Army High Command (OKH/G d NA), showed the safety margin to be 20,000 letters a day.[30] Dr. Fricke believed that if the instructions on maximum length of messages were followed, "everything would be all right."[31] Yet it was traffic in this Enigma, even when "used properly," which was regularly solved day-by-day by the tremendous Anglo-American cryptanalytic effort.

9. Plugboard Enigma was known to be solvable with "cribs."--It is an astonishing fact that although German cryptographers knew, at least as early as 1943, that it was theoretically possible to solve the German Army plugboard Enigma whenever a proper crib was available,[32] they seemed little concerned about this possibility and failed to realize that a practical solution might be based upon it. This knowledge should have aroused their most vivid apprehensions but did not, because of lack of imagination regarding the possibilities presented by the invention, development, and use of specially designed high-speed analytic machinery.

In 1944, Lt. R. Hans-Joachim Frowein of the Signal Security Agency of the Navy High Command (OKM/4 SKL/II) suggested an International Business Machine (I.B.M.) method of solving the plugboard Enigma, given a twenty-five letter crib.[33] This suggestion was based on a hand method which employed sequential testing, or "scritching," a method which was mechanized by the Army Security Agency and incorporated in the "auto-scritcher." After describing this hand process, Lt. Frowein made the following suggestions:[34]

[29] I 92 p 2
[30] I 78
[31] I 20
[32] D 58 p 18
[33] I 38 pp 3-4
[34] I 38 p 4

> "In practice, Hollerith /I.B.M./ machinery would be used... . With a 3-wheel (Army) Enigma, only 70,000 cards are required... . The enemy could have produced the 70,000 cards at the beginning of the war and this catalogue would have been valid throughout the life of the three-wheel Enigma. The first Hollerith card sorting process would take 200 machine-hours, the second only 8 machine-hours, and so on."

Thus a total of approximately 220 I.B.M. sorter-hours would have been sufficient to test the "crib" to see if it could break the plugboard machine. Another way of stating this, is that 10 sorters could test one crib in one day. This is not rapid, but it is within practical limits. And this suggestion is only the first theoretical answer, not the climax of a comprehensive, practical attempt at solution.

Perhaps the cryptographers of the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) believed that it would be too difficult for an emeny to obtain the cribs necessary for solution by Lt. Frowein's methods. Possibly they were too busy designing improved apparatus which they would put into effect "someday." Certainly there is no indication in the TICOM interrogations or documents that cryptographers of either the Armed Forces or the Army worried about Lt. Frowein's results when the results were shown to them. The Navy, with a four-rotor, more nearly secure Enigma, did take his results somewhat seriously. Lt. Frowein stated:[35]

> "The official reaction to the findings of the investigation was the immediate decision /by the Navy/ that only rotors with two turn-overs should be allowed to be used in the right-hand /"fast"/ position. This /action/ was introduced at the beginning of December, 1944... . The view of the German Army was that their Enigma was theoretically solvable. The four-rotor /Naval/ Enigma was not considered theoretically solvable and the Army were astonished at the Navy's view based on this investigation."

The action taken by the Navy, as indicated above, was so ineffective an answer to the problem raised by Lt. Frowein, that it almost might as well not have been taken. Nevertheless, for his excellent work, Lt. Frowein was awarded the War Merit Cross.

[35] I 38 p 5

10. Theoretical weaknesses of plugboard Enigma were understood.- We may not conclude from the lack of all-out practical efforts to make a worthwhile security study of the plugboard Enigma that the German military cryptographers were in any way mentally inferior to the British and American cryptanalysts who succeeded against this Enigma. Despite that fact that the Germans discovered every weakness the Enigma had, their theoretical studies and conclusions apparently did not impress them. According to Dr. Buggisch of the Signal Intelligence Agency of the Army High Command (OKH/G d NA), the weaknesses of the plugboard Enigma were:[36]

a. Rotor I (the "fast" rotor) moved uniformly.
b. Rotors II and III moved too seldom.
c. The machine needed more than three rotors to be inserted in it at once. That is, the period $26^2 \times 25$ was too short.
d. The machine needed more than five rotors to be issued with it. That is, the number of rotor orders, the permutations of 5 rotors taken 3 at a time (= 60), was too small.
e. The reflector was not pluggable, and the "enemy" could set up the $60 \times 26^2 \times 25$ alphabets of the machine in its unplugged form, possibly proceeding to a solution from there.

Dr. Buggisch was so right! Improvement in any one of the foregoing particulars could easily have pushed the plugboard Enigma beyond the reach of already-straining Anglo-American cryptanalytic fingers, and possibly altered the course of the war. If the multiple turn-over rotors of the "counter" machine had been inserted in the plugboard Enigma, if ten rotors had been issued instead of five, if five rotors simultaneously could have been used in the machine instead of three, if the rotors already in it had been kept more active by suitable motions, or if a pluggable reflector had been universally adopted, regular, day-by-day solution would hardly have been possible.[37]

[36] I 37

[37] Another effective security measure would have been to issue new rotors at regular intervals, or whenever compromise of those in use was suspected. This procedure was evidently not considered favorably by the Germans, who had so many Enigmas in the field and in use elsewhere, that the chance of capture was great, and the number of rotors to be replaced in case of compromise prohibitive. Newly wired rotors were issued at the outset of the war, but these wirings were kept throughout the war without change, on the theory that the Enigma was secure regardless of rotor compromise.

How close the Anglo-Americans came to losing out in their solution of the German Army Enigma is a matter to give cryptanalysts pause.

British and American cryptanalysts recall with a shudder how drastic an increase in difficulty resulted from the introduction by the German Air Force of the pluggable reflector ("Umkehrwalze D," called "Uncle Dick" by the British) in the Spring of 1945. It made completely obsolete the "bombe" machinery which had been designed and installed at so great an expense for standard, plugboard-Enigma solution. It necessitated the development by the U.S. Navy of a new, more complex machine called the "duenna," and by the U.S. Army of a radically new electrical solver called the "autoscritcher." Each of these had to make millions of tests to establish simultaneously the unknown (end-plate) plugboard and the unknown reflector plugging. Only a trickle of solutions would have resulted if the pluggable reflector had been adopted universally; and this trickle of solutions would not have contained enough intelligence to furnish the data for cribs needed in subsequent solutions. Thus even the trickle would have eventually vanished.

Credit must be given to the unknown German Air Force cryptographer, possibly a member of the Security Group of the Signal Intelligence Service (OKL/Gen Nafue/III, Gruppe IV), who brought about the use of "Uncle Dick" throughout the German Air Force in the spring of 1945. It is indeed lucky for the Allies that the cryptographers of the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) did not agree with his belief in the pressing need for additional security. Dr. Fricke said:[38] "It was not considered important, as the plugboard was the real safeguard." Dr. Huettenhain said in effect:[39] "The G.A.F. had introduced the pluggable reflector, but the Army said it was too much trouble."

11. "Variable-notch" rotors would probably have made plugboard Enigma secure-- Daily solution of the plugboard Enigma would probably have been prevented if the Germans had introduced the variable-notch rotor ("Zueckenfuellerwalze") in 1943 as planned.

This rotor was designed to "hold the security line" until the introduction of Cipher Device 39, a Hagelin-type-drive Enigma designed in 1939 (as its name implies) and already past the blueprint stage.

[38] I 29

[39] I 31

The effect of variable-notch rotors in an Enigma would have been to make impossible the foretelling of exact successive rotor settings, when preparing to "bombe" a crib. Assumptions would have to be made as to the presence or absence of turn-overs of the "medium speed" and "slow speed" rotors, at each successive element of text. This would have multiplied the number of trials necessary to test cribs, and thereby reduced the number of solutions to the small trickle which has already been characterized as not being, in all probability, self-sustaining.

The following excerpts from minutes of conferences held by the Signal Intelligence Agency of the Supreme Command, Armed Forces (OKW/Chi) on 15 December 1943 and 18 March 1944, are interesting sidelights:[40]

a. "Concerning improvement of the Enigma, Wa Pruef 7 /Army Ordnance, Development and Testing Group, Signal Branch/ stated that the replacement of all rotors by variable-notch rotors required reconstruction and time for development. It was however possible to exchange one rotor; the necessary variable-notch rotors could be delivered within a reasonable time."

b. "In collaboration with Wa Pruef 7, in view of the introduction of the variable-notch rotor, the keying pressure /required to encipher on the Enigma/ was reduced by about 1000 gr. at the firm of Heimsoeth & Rinke."

Mechanical drawings of the variable-notch rotor are now in the files of the Army Security Agency.[41] Several such rotors have been captured and are available.

12. Cipher Device 39 would have been secure against present attack-- Cipher Device 39 was to be the epitome of Enigma perfection. It was to have everything--end-plate plugboard, pluggable reflector, 4 variable-notch rotors, 3 added Hagelin-type irregular drive wheels, and a simple inter-acting motion. It was to have a keyboard; and it was to print both plain and cipher texts, at a rate of 85 words per minute.

A note in Dr. Huettenhain's files dated 30 May 1944 stated:[42]

[40] D 59 p 11 p 2

[41] M 11

[42] D 59 p 26

"The model built by the Telefonbau u. Normalzeit Company, Frankfurt a. Main is being demonstrated in operation. The machine essentially satisfies all the requirements laid down for it. Wa Pruef 7 /Army Ordnance, Development and Testing, Signal Branch/ has settled what features of the machine require improvement. F.A.N. (?) in Frankfurt a. Main has been completely destroyed. The machine cannot therefore be expected to go into large scale production there for some considerable time. It is therefore intended to get an additional production center at once. The Wanderer Company, which already has wide experience of large scale production, is proposed for this additional production. Dr. Fess of Wanderer's is awaited in Planken for detailed negotiations on the subject of this production.

"According to Wa Pruef 7 /Army Ordnance, Development and Testing Group, Signal Branch/ small scale production is approved.

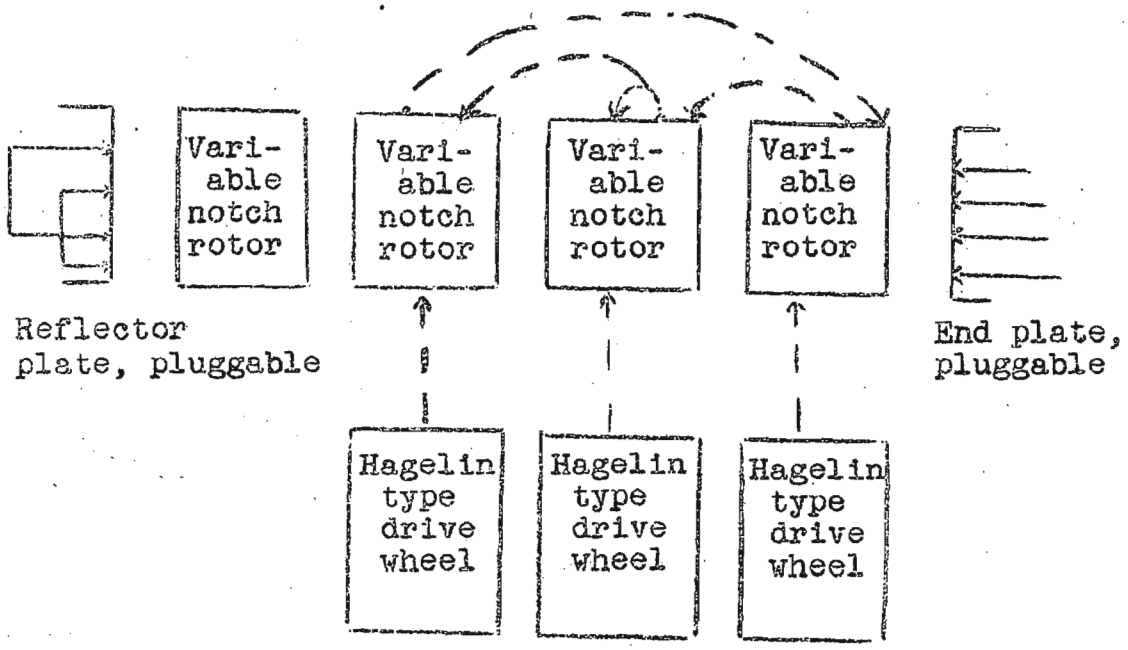
"OKW/Chi sees at the moment no possibility of a break-in, but exhaustive investigations are still in progress.

"On completion of plant at Wanderer it is planned to arrange a final conference there with the units requiring the machines and the special committee. The aim is to begin large scale production by the end of 1944."

None of the test models of Cipher Device 39 has ever been received at Army Security Agency.[43] Excellent descriptions

[43] Two test models of Cipher Device 39 were packed in boxes at Telefonbau u. Normalzeit, Frankfurt, and the boxes "picked up by an Army Corporal on March 22, 1945, for movement to a military depot at Tauberbischofsheim." See I-53 p 3. These were never found. A third, incomplete, machine however was captured and is now at London Signal Intelligence Centre. Captured German Army plugboard Enigmas, commercial Enigmas, counter Enigmas, variable-notch rotors, and pluggable reflector wheels are available at the Army Security Agency museum, however.

exist, however.[44] The main elements of this device may be represented by the following skeleton schematic diagram:



[44] I-53, I-57. It is interesting to note that Cipher Device 39 was originally planned to have been issued in 1939, as its name implies. A TICOM report on an interrogation of Dr. Otto Buggisch of the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) stated: "Geraete 39 and 41 were both in development for years and still had not come out at the end. B /Buggisch/ has the almost inevitable comments about the military non-technicians who blocked things." According to a writing by Dr. Liebknecht, of the Army Ordnance, Developing and Testing, Signal Branch, "This delay was due in part to lack of clarity in the operational requirements, in part due to changes following mathematical researches, but in large part due to pure technical difficulties."

Motion controls of the variable-notch rotors are indicated by broken lines in the diagram. Solid lines to the "end plate" indicate wires from keyboard and tape printers. Note that the first variable-notch rotor never moves during encipherment. Better cryptographic procedure would be not to allow any completely stationary rotor.

13. Enigma development is worthy of study-- To recapitulate, German cryptographers throughout the war used a cryptographic device known as the "plugboard Enigma," which had a high degree of security, but was insecure against determined and costly Anglo-American cryptanalysis. This device was on the threshold of almost complete security, through the introduction of pluggable reflectors and/or the variable-notch rotors. The pinnacle of German Enigma development was reached with the completion of plans for Cipher Device 39 and the building of a very small number of test models. The four rotors and three Hagelin wheels, irregular interacting motions, and dual end plate pluggings of Cipher Device 39 would have produced a machine that, if used properly, would probably have ranked along with our own SIGABA for security.[45]

[45] Cryptanalysts Schauffler and Hauthal of the Foreign Office Cryptanalytic Section (Pers Z S) discussed the construction of a proposed new cipher machine with Willi Korn, engineer of the Enigma firm Heimsoeth and Rincke, Berlin, in February 1942. It was to be called "Machine 42" ("Maschine 42") and was to be, in effect, an Army plugboard Enigma with three additional rotors inserted in front of the plugboard--that is, between the plugboard and the key-and-light bank. The first of these three additional rotors was to step each time a letter was enciphered, and the second and third were to be stepped by notches in the customary Enigma manner. Traffic in such a machine could not have been solved by normal bombe methods, although a special autoscritcher can be conceived of for such reading. The practical difficulties would be tremendous, so that for practical purposes Machine 42 would have been secure. Machine 42 never passed the stage of theoretical development because of engineering and procurement difficulties. See T-5 for details.

Volume 2

Chapter III Teleprinter Cryptographic Apparatus

14. German teleprinter cryptographic apparatus was of two main types.- German cryptographers developed two main types of teleprinter cryptographic apparatus. They were:

a. Cipher attachments, which could be associated with or attached to any teleprinter.
b. Cipher teleprinters, in which the cryptographic mechanisms were integral parts of the teleprinters.

The cipher attachments were called "Schluesselzusaetze." Of these, model SZ-40 (later discarded), and models SZ-42a and SZ-42b were insecure against Anglo-American cryptanalysis. Model SZ-42c, which was designed to "cryptize" the radio circuit as a whole, would probably have been completely secure.

The cipher teleprinters were called "Schluesselfernschreibmaschinen." Of these, models T-52a, T-52b, T-52c (first model), and T-52c (second model) were insecure against Anglo-American cryptanalysis, and were ementually discarded by the Germans as a result of their own security studies; models T-52d and T-52e could not have been solved by any presently-known methods of attack. The T-43 was a "one-time tape" cipher teleprinter and likewise secure if proper tapes were inserted, and if certain electrical elements in the apparatus were properly adjusted.

Various models of all the above machines carried high-level communications for the Foreign Office, the Air Force, the Navy, the Reich Security Office, and miscellaneous government departments; and practically all models were used at some time or other by the Army down through division.

Land-lines carried most of the teleprinter traffic, and land-line traffic was, of course, not interceptible by the Anglo-Americans. Radio links were "beamed transmissions" which were difficult to intercept, yet certain important Army radio links employing such transmissions were intercepted. They included, among others, circuits between Berlin and each of the following: Athems, Salonika, Rome, Bucharest, Belgrade, French ports, Paris, Rotterdam, and Oslo; they also included circuits among corps areas (Wehrkreis) in Germany itself.

From Ultra sources, it is known that solved German teleprinter messages gave information in detail concerning supplies shipped, troop movements, police data, and agent information. Important battle order information was often obtained, and important orders from Hitler.

The information transmitted by German teleprinter cryptographic apparatus was therefore of utmost importance to the Anglo-American government and field forces during the war from an intelligence standpoint. The various machines themselves are still important, as a result of TICOM investigations, for the cryptographic features they involve.

British cryptanalysts gave the generic cover name "fish" to any German teleprinter cryptographic machine, the cover name "tunny" to the cipher attachments of the first type mentioned in paragraph 14, and the cover name "sturgeon" to the cipher teleprinters, the machines of the second type.[49]

15. <u>German teleprinter cryptographic apparatus enciphered individual teleprinter impulses</u>.-- A standard teleprinter of the so-called "start-stop" type transmits seven impulses for each letter or character sent, as follows: a start impulse, a set of five distinguishing impulses or "bauds," and a stop impulse. Each of the five bauds is either "plus" or "minus" depending on the character being sent. (Thus, the set of bauds for "e" is plus minus minus minus minus, and the following sequence of impulses is sent: start, plus minus minus minus minus, stop.) German teleprinter cryptographic apparatus, just as

[49]Captured T-52d/e and SZ-42b apparatus are available in the Army Security Agency Museum.

similar machines of other origin, enciphered such teleprinter transmissions by enciphering these five individual bauds. The apparatus did this by generating a key made up of a lengthy sequence of teleprinter characters, and causing the sets of bauds corresponding to the successive keying characters to be combined, baud by baud, with the sets of bauds corresponding to the successive plain text characters. Combining was done according to a principle invented in 1918 by an American engineer named Vernam, who originated the so-called "Vernam Rule" that a combination of like signs produced a "plus" impulse, and a combination of unlike signs produced a "minus" impulse. The result was, of course, a succession of sets of five bauds corresponding to the cipher characters. In the German teleprinter cipher attachments, these cipher characters were transmitted without further encipherment; in the cipher teleprinters, they underwent transposition of bauds within characters as further encipherment before they were transmitted.

16. German teletype cryptographic apparatus used mechanical wheels.- Mechanical cipher wheels were used in all German teleprinter cryptographic apparatus, except in the one-time-tape cipher teleprinter. Around its periphery, each of these mechanical wheels had small pins which operated a switch (or switches) as the wheels rotated. Operation of the switches gave in effect the "plus" or "minus" impulses needed to form key characters. In the teleprinter cipher attachments SZ-40, -42a, and-42b, the "pin patterns" of each of the wheels, i.e. the sequence of pins with respect to their being in operable or inoperable positions, was changeable simply by manually setting the individual pins into effective or ineffective positions. In the SZ-40 (original model) and in the cipher teleprinters (T series except for T-43) the pin patterns were not variable, and were fixed at the time of their manufacture. The T-43 used tape and no cipher wheels.

17. "Cipher attachments" were insecure.- The German teleprinter cipher attachments, or "tunny" machines, are of importance to Anglo-American cryptographers in showing them what not to do. All of the actually built models of these machines were insecure. Dr. Huettenhain, of the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi), told Dr. Vierling that their "security was good for about two years,"[50] but he evidently had a rather high opinion of the SZ-42a and SZ-42b as used with beamed radio, because he permitted their use past the two-year mark.

[50] E 14 p 6

The SZ-40 (original model) had ten mechanical cipher wheels, with fixed peg patterns. The ten elements produced by these wheels combined in pairs to form one set of 5 elements, and the set was then used as the keying character for the plain text character to be enciphered.[51] Only 40 of these machines were built. Dr. Fricke said that since it had been ascertained that single messages of 1,000 letters sent on the SZ-40 (original model) could be solved, it was decided to introduce a machine with an irregular element in the wheel motion.[52] This was done by introducing the SZ-40 (regular), which consisted of 12 wheels with changeable patterns, divided as follows: 5 "springcaesar" wheels, all of which stepped in unison but irregularly, being driven by a pair of "vorgelege" (control) wheels; and 5 "spaltencaesar" wheels, all of which stepped in unison and regularly, once for each character enciphered. Anglo-American solutions of messages sent on this machine were accomplished by statistical recovery of the pin patterns of the regularly-stepping wheels and the removal of their effects from the cipher texts; this was then followed by recovery of the pin patterns of the irregularly-stepping wheels and the removal of their effects. Dr. Huettenhain believed that solution could be obtained by attacking the motion of the five irregular ("springcaesar") wheels first[53] and therefore suggested the SZ-42a, which gave an additional irregular control to these irregular wheels. This further irregular motion came from two sources: one source was the pattern on the first of the five irregular wheels itself, another was the variation in the fifth baud of the plain-text character "two letters back" in the plain text, i.e., two characters before the character actually being enciphered at the moment. This plain text autokey control was optional; and because it gave rise to many errors it was not used often. The SZ-42b was next developed with a third element contributing to the irregularity, namely, a control by the second regular ("spaltencaesar") wheel.[54] None of these ruses succeeded in preventing Anglo-American cryptanalysis, since the attack was to ignore temporarily the irregularly-moving wheels, and to remove the effects of the

[51] In this respect this machine was identical with that developed by the International Telephone and Telegraph Company in the United States in 1931, employing 10 mechanical wheels and the property of pairing.

[52] I 45

[53] I 31

[54] I 45 p 19

regularly-moving wheels first. This made attack on the irregularly-moving wheels possible. The Germans had evolved elaborate protection for the wrong end of their machine.

18. Proposed SZ-42c with synchronization would have "cryptized" a whole radio circuit.-- The SZ-42c was being designed to "cryptize" a whole radio teleprinter circuit.[55] Teleprinters on this circuit were to operate at all times, transmitting a stream of characters forming an entirely unintelligible "message" whenever bonafide enciphered messages were not being sent. An interceptor would not be able to distinguish any signals representing real messages from those corresponding to unintelligible or random sequences of characters. Therefore the number, length, precedence, classification, and timing of messages would not be known to enemy intercept, and the circuit would be secure against traffic analysis. Dr. Vierling of the Feuerstein Laboratory was developing the crystal controlled synchronizing apparatus, called "gleichlauf," which was to keep the teleprinters synchronized, regardless of radio fading and interference.[56]

The nonsense to be transmitted on the air whenever messages were not being sent would actually be "pure key" generated by the SZ-42c. An enemy would therefore have a great advantage in trying to cryptanalyze the SZ-42c. No one can state accurately what results could have been obtained by an enemy given possession of tens of thousands of consecutive characters of pure key, but the design for the SZ-42c appeared to be secure for normal operation. The five regularly-moving wheels (spaltencaesars) of the earlier models no longer were to move regularly or even together; this would have prevented the methods of cryptanalytic attack theretofore used by the Anglo-Americans. Dr. Huettenhain was probably right in his report as follows:[57]

> "Wa Pruef 7 are at the moment carrying out a reconstruction in which the five righthand wheels are driven separately irregularly. This eliminates a cardinal weakness of the SZ 40 and 42, the regular movement of the Spaltencaesar, and makes methods of reconstructing the pin arrangements impossible."

[55] E 14

[56] E 13

[57] D 59 p 18

A full description of the interacting motions involved in the SZ-42c can be found in TICOM reports.[58] Briefly there were to be 10 wheels. These moved constantly unless interrupted. Interruption of motion of wheels 1, 2, 3, 4, and 5, (which were the springcaesars and which moved in unison) was accomplished by action of wheels 9 and 10; interruption of wheel 6 was accomplished by wheels 8 and 2; of 7 by 9 and 3; of 8 by 10 and 4; of 9 by 6 and 5; of 10 by 7 and 1. If it happened that all wheels became stationary (thus resulting in monoalphabetic encipherment), the machine counted to three, and then wheels 1 through 5 stepped automatically.

The firm of Lorenz, which was developing SZ-42c with electromagnetic drive rather than mechanical, called their model of the SZ-42c machine "SK-44." They also planned SK-45, which was to be identical with SK-44 except for an eleventh wheel; the eleventh wheel was to step the machine past "dead spots," so that the counting device used in SZ-42c for that purpose would not be needed.

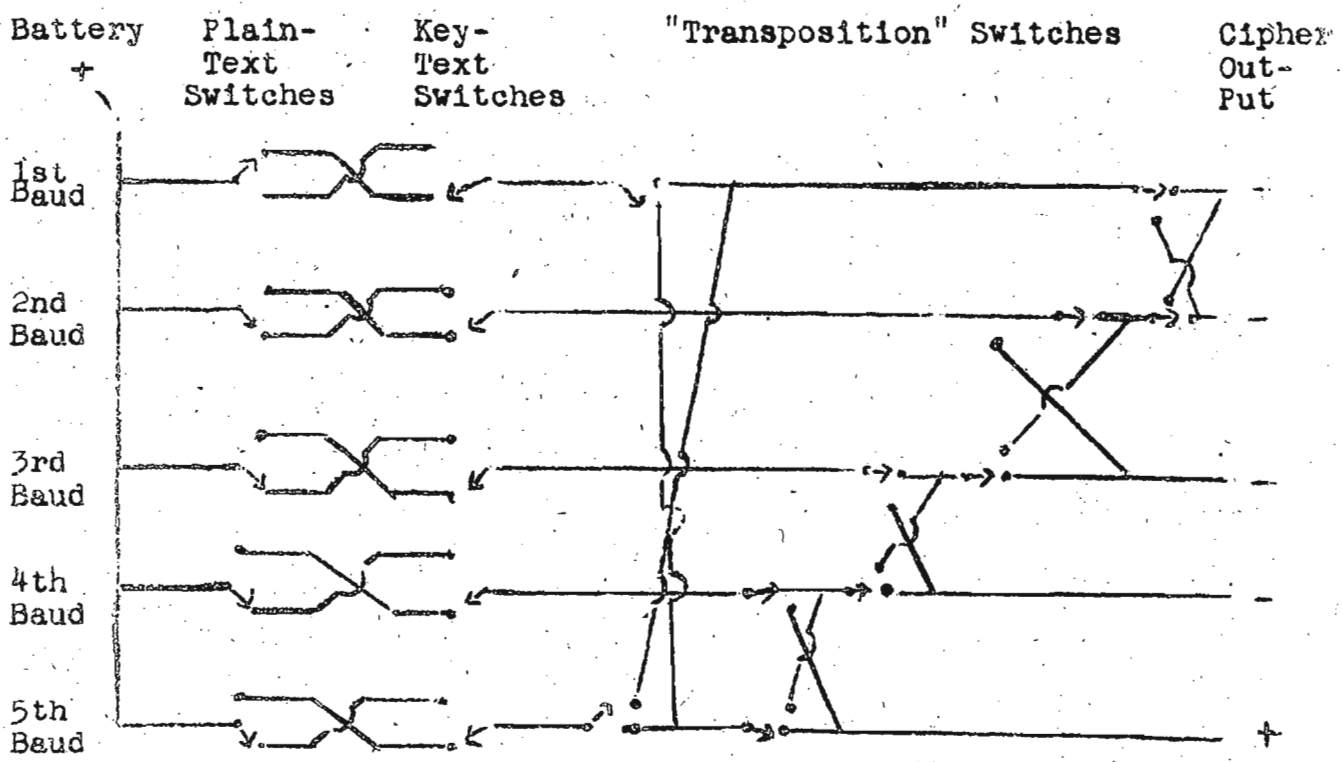
19. Some "cipher teleprinters" were secure.-- There were five main types of cipher teleprinters developed by German cryptographers: T-52 a/b, T-52c (first model), T-52c (regular), T-52d, and T-52e. The T-52d (probably) and T-52e (certainly) were secure against known methods of attack, but were not actually much in use on radio circuits.

All five of the foregoing cipher teleprinters were important because they introduced a new principle into teleprinter cryptography: that of positionally transposing, as a form of superencipherment, the five separate bauds constituting the set corresponding to each cipher character, after the normal or basic encipherment had been accomplished.[59]

[58] I 57, E 14

[59] A similar principle is the subject of a U.S. patant by Mr. William F. Friedman of the Army Security Agency. The German cryptographers, however, brought into actual use the first secret teleprinters to employ these principles in practice.

A schematic diagram demonstrating the principles involved in the two processes of encipherment, substitution and transposition, is shown below:



The foregoing diagram is not electrically accurate, but it is accurate in principle. It indicates, for example, the result of enciphering the plain-text character "e" (plus minus minus minus minus) by the key-text character "blank" (minus minus minus minus minus) and passing the result through a transposition network as shown, with a transposition taking place between the first and fifth bauds. The result is the character "t."

It can be demonstrated that the security of any cipher teleprinter employing the foregoing principles depends upon the manner of generating the key-text characters, the manner of controlling the transposition switches, and in addition whether or not the order of the transposition switches may be changed.

All of the T-52 series of cipher teleprinters had ten mechanical cipher wheels, and the pegs on each of these wheels were set into permanent peg patterns. In the T-52 a/b model, each of the five key-text switches and the five transposition switches was operated by one of the ten mechanical wheels. The ten wheels moved regularly. The transposition switches themselves could not be interchanged. The machine was insecure because the settings of the wheels could be attacked independently of one another and statistically. In the T-52c (first) model, each of the five key-text switches was controlled by a given combination of four of the ten mechanical wheels; each of three of the transposition switches was controlled by a given combination of four of ten mechanical wheels; each of the remaining two transposition switches was controlled by a given combination of six of the ten mechanical wheels. The ten wheels moved regularly, and it is believed that the order of the transposition switches was not changeable. Furthermore, the particular choice the Germans made for the sets of four wheels to be used in controlling the key-text switches resulted in a limited number of substitution permutation combinations, which made solution possible. This effect was partially eliminated in the T-52c (regular model) and for this reason the regular T-52c was harder to solve.[60]

Model T-52d made the order of the transposition switches changeable, and while each key-text switch and each transposition switch was controlled by only one wheel, the wheels themselves stepped irregularly. The movement of each wheel was controlled by the patterns of two other wheels, and interacting controls resulted. Provision was also made for the optional use of an additional plain-text control of the irregular motion. It is seriously doubted if this machine could have been solved, even if pure key was available from reading messages in depth, solely because of the interacting, irregular motion of the wheels.[61]

[60] Inspectorate 7/VI (In 7/VI) discovered that the T-52c was breakable in 1942, and suggested alterations that led to the T-52d. I 78 p 11.

[61] Single messages might have been partially read by a crib matching method suggested by Inspectorate 7/VI (In 7/VI). I 78 p 12.

Model T-52e had wheel motion identical with that in model T-52d. Its order of transposition switches was not changeable, but each of the transposition switches and the key-text switches was operated by the combined pattern of a set of four wheels chosen for it from the ten wheels. The T-52e was therefore also probably secure.

Full details concerning the interacting and irregular wheel motions, the transposition of bauds, and the manner in which wheel patterns were combined to get replication of controls, are given in TICOM publications.[62]

20. Cipher teleprinter model T-43 used one-time tape.-- The T-43 used a one-time key tape to supply the sequence of keying characters, instead of mechanical cipher wheels as in the other T-series models. The T-43 was just as secure against cryptanalysis, therefore, since the key tapes employed consisted of "random characters."

In practice the key tape was generated by the running of a fifty-meter-long loop of random tape over and over through a T-52d machine, with the T-52d punching out the key tape as long as desired. The key tape was not random in a true sense, but it was unpredictable for practical purposes, and secure.

A serious electrical defect in the T-43 was discovered by radio engineers and corrected. This defect actually had rendered the T-43 insecure. It resulted from the fact that at the instant of encipherment the keying character was electrically slightly out of phase with the plain-text character. As a result, minute inspection of the cipher characters on an oscilloscope permitted separation of the composite cipher characters into their plain-text and key-text elements--resulting in a "solution" without cryptanalysis.[63] The moral from the above story is plain: there are more ways than one to read a message.

21. Conclusion: German teleprinter cryptographic apparatus is worthy of detailed study.-- To recapitulate, although the Anglo-Americans were able to read German teleprinter traffic sent on important Army and Air Force links as a daily procedure, because of the insecurity of the SZ-42a and SZ-42b cipher attachments and the willingness of the Anglo-Americans to build the expensive machinery necessary for solution, (such as the British "colossus"), nevertheless the more recently developed German cipher-teleprinters (T- series) were completely secure.

[62] I 45, I 20, I 31

[63] I 45, p 15

The latter units were designed along different lines from any lines taken by Anglo-American development of teleprinter cryptographic apparatus. They therefore make definite contributions to our knowledge. Their main features were:

a. Irregular and interacting wheel motions.
b. Use of baud transposition as an additional protection, superimposing this on the basic substitution process.

Furthermore, the attempted development of a cipher attachment (SZ-42c) for cryptizing a radio circuit, thus protecting it against traffic analysis as well as cryptanalysis, indicated that the Germans were giving serious thought to all phases of the cryptographic problem.

Volume 2

Chapter IV - Cipher Device 41, the Cipher Box, the Cipher Disk, and the "Number Printer."

22. German Cipher Device 41 was a secure Hagelin-type machine-- Cipher Device 41 ("Schluesselgeraet 41") was a mechanical cipher device (Hagelin type) similar to the U. S. Army converter M-209 and was originally intended for use forward of division.[70] The German Army, Air Force, Weather Bureau, and probably others, had ordered a total of eleven thousand machines,[71] but only a small (unknown) quantity had been manufactured and put in use. Cipher Device 41 was remarkable for two reasons:

a. Although it required no electrical power, being operated by a hand crank, it was compact, portable, printed both plain and cipher tapes, and was provided with a typewriter keyboard.

b. The daily wheel settings and pin patterns were protected against reconstruction by cryptanalysis even when "pure key" was available. This was because even though the plain texts of identically-keyed messages could readily be obtained by well-established procedures and the corresponding portion of the keying sequence reconstructed, nevertheless this reconstructed sequence ("pure key") did not provide data whereby the wheel settings and pin patterns could

[70] I 72. The Army Security Agency has a captured Cipher Device 41 in its museum.

[71] D 59 p 23

also be reconstructed. As a consequence, no other messages on the same day could be read. This is not usually the case in other Hagelin type machines, including the U. S. Army converter M-209.

23. Security of Cipher Device 41 lay in interacting, irregular, cipher-wheel motions-- The security of Cipher Device 41 came from the interacting and irregular movements of its cipher wheels.

Here again is demonstrated the German capacity to make secure in practice an otherwise not too secure machine, by employing the principles of interacting and irregular movements of wheels.

The enciphering principles of Cipher Device 41 may be described as follows:

a. It had 6 mechanical Hagelin-type "pin" wheels, "prime" to each other. In cryptographic parlance, the first five of these wheels had "kicks" of 1,2,4,8, and 10 respectively. Wheel 6 made these "kicks" positive or negative.

b. The enciphering cycle (one turn of the hand crank) consisted of three elements, as follows:

"Element 1." This element of the cycle took place if and only if wheel 6 had an active peg in the "motion index position." If wheel 6 had such an active peg, then all the following events occurred: Wheel 1 moved one step. Each of the remaining four wheels moved one step, unless the wheel to its left had an active pin in its "motion index position," in which case each such wheel moved two steps.

"Element 2." A key "kick" was generated, which was the sum of all the kicks of wheels which had active pegs in the "kick index positions." This was so unless wheel 6 had an inactive peg in the "kick index position," in which case the key kick which resulted was equal to "25 minus the sum of the kicks" of the wheels with active pegs. This key kick was in effect the "key text" or "key character" which was "added" to the plain text character in encipherment. Encipherment took place at this point.

"Element 3." This element of the cycle was identical in principle to Element 1, except that it occurred whether or not wheel 6 had an active peg in the "motion index position." The purpose of this element was to insure some change in the wheel positions before the encipherment of the next letter of text, if any.

When one compares the foregoing irregular and interacting motions of the wheels, and the use of occasional negative kicks, with the simple regular motion and simple regular kick addition of the usual Hagelin-type machine, the reason for the far higher order of security of Cipher Device 41 is indeed apparent.

In 1945 the British had intercepted certain traffic enciphered by German agents with Cipher Device 41. Several messages were read because of improper mechanical working of one of the machines. The machine itself, however, was not solved thereby, and remained a mystery until capture revealed its construction.

It is believed by investigators that the mechanical designs of the Cipher Device 41 was poor but that its faults could probably be corrected by improved engineering. Mechanical problems in all likelihood prevented its wider and earlier use by the Germans.

Cipher Device "41-Z" was a modification of the standard model 41. It was designed to encipher ten figures instead of twenty-five letters, for use by the German Weather Bureau.[72]

A model of Cipher Device 41 which would be more compact and would eliminate the typewriter keyboard was also under consideration, for use by front line troops.

24. "Cipher Box" was to replace Enigma-- A mechanical device, made out of aluminum and weighing 1-3/4 pounds, was being developed, which involved cryptographic principles entirely new to German cryptography. It was hoped to use this device to replace the Enigma in the German Army above the level of division![73] It was called the "Cipher Box" ("Schluesselkasten") and made use of the cryptographic principle of sliding strips.[74]

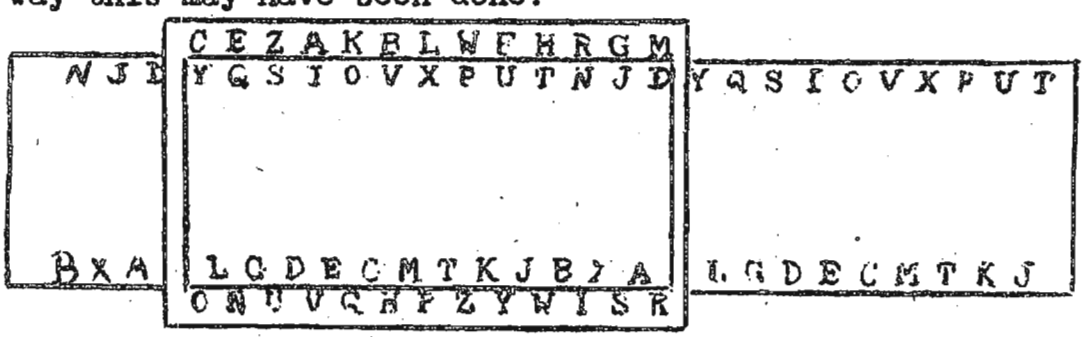
Lt. Col. Mettig, of the Signal Intelligence Agency of the Supreme Command, Armed Forces (OKW/Chi) reported as follows:[75] "Field tests...had been so successful and had brought out the handiness and speed of operation of the machine so clearly, that its introduction into the field army was ordered. As the RSHA (Reich Security Office) had already got in ahead with the order for 70,000 items, mass production was introduced." The mass production was scheduled to have produced at least one thousand devices by October 1945 and to reach a rate of 10,000 per month by January 1946.

[72] D 59 p 25
[73] I 96
[74] I 20
[75] I 96

No Cipher Box has ever been captured, and the descriptions are not sufficiently detailed to do more than reveal the cryptographic principles involved, leaving the mechanics for the imagination. Fricke stated[76] that "it consisted of a small box in the top of which was inserted a slide rule." He described the slide rule as consisting of two mixed alphabets which were written in by pencil with each key change.

Half of the first mixed alphabet was written on the upper base part of the slide rule, the remaining half of the alphabet on the upper slide part of the slide rule. Half of the second mixed alphabet was written on the lower base part of the slide rule, the remaining half of the alphabet on the lower slide part of the slide rule. The two alphabets were so written in that when the halves of the first (upper) alphabet were in phase with each other, the halves of the second (lower) alphabet were out of phase, and vice-versa.

The drawing below illustrates with sample alphabets the way this may have been done:



Encipherment of a letter was accomplished by reading off the letter opposite it on the slide rule. This was to be chosen from whichever alphabet was "in phase" at the time of encipherment. In the foregoing drawing, the cipher equivalent of plain text "I" at the setting shown would be "A" and the cipher equivalent of plain text "A" would be "I." Thus there resulted exactly 26 possible reciprocal enciphering alphabets.

Any sliding-strip device is secure if the successive settings of the sliding strip are unpredictable. Security of the Cipher Box therefore had to rest primarily in the manner of successively setting the slide. Dr. Fricke said this was done as follows:

> "Under the slide were three Hagelin type wheels on separate axes, in a plane perpendicular to that of

[76] I 20

the slide. Each had a different period, around 26. (The pin settings were changeable). The slide was pulled to the right against the action of a spring, and upon release drove the wheels. It did not come to rest until at a reading position of the wheels on one side the pins were all active, or until at another reading position on the other side they were all inactive. There were 26 stopping places possible, but no step zero."[77]

Dr. Liebknecht of the Army Ordnance, Development and Testing Group, Signal Branch (Wa Pruef 7) stated:[78]

> "The tongue (slide) of the instrument was shoved by hand to the right as far as it would go, thereby putting a spring inside the Cipher Box under tension. By means of pressing a blocking notch on the top of the Cipher Box, one causes the sliding tongue to move back varying step lengths into the Cipher Box."

[77] I 20. A cryptograph called the M-40, invented by Inspector Menzer of the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi), also employed three Hagelin-type wheels for alphabet selection. This device was considered reasonably secure but was never adopted. It consisted of a cylinder with 39 horizontal bars arranged around its periphery; the cylinder rotated in steps equal to one plus the sum of the kicks given it by the three Hagelin-type wheels. The Hagelin-type wheels had changeable pins. Normal alphabetic sequences, each starting however with a different letter of the normal alphabet, were permanently inscribed on 26 of the 29 bars; the remaining 3 bars contained "dummy positions." These bars represented the plain components of enciphering alphabets of which the common cipher component was one mixed sequence written in by pencil on a fixed strip, so fastened on the base of the device that the bars of the cylinder could rotate into juxtaposition with it. The device was cryptographically equivalent to a pair of sliding strips, with the plain component a normal alphabet, with the cipher component a mixed alphabet, with the stepping controlled irregularly by Hagelin-type wheels, and with dummy letters thrown into the cipher text whenever a "dummy bar" came into position. See I-118 for fuller details. The Cipher Box was an improvement over the M-40, in that the small slide-rule construction accomplished nearly the same results as the large cylinder construction, the Cipher Box had two "reading positions" for the Hagelin-type wheels instead of just one, and there was provision for two mixed alphabets to be inscribed instead of just one.

[78] I 57 p 9

Nowhere in TICOM was it recorded whether or not the slide was pulled to the right after each encipherment, or only when necessary.

Serious study of this device has not been undertaken as yet at the Army Security Agency. However, the Germans felt that it was most secure. Lt. Col. Mettig stated as follows:[79]

> "The cryptographic security of this machine is very high and was considered superior to that of the Enigma. The safety margin for the daily cipher was calculated in the neighborhood of 40,000 to 50,000 letters, whereas with the Enigma this margin was 20,000 letters."[80]

25. "Cipher Disk" was to be a simplification of the "Cipher Box."-- The Cipher Box, small as it was, was the larger of two miniature cipher devices. The smaller device was called the Cipher Disk ("Schluesselscheibe.") Dr. Liebknecht[81] gave TICOM its best description of this device. He said:

> "Oberinspektor Menzer designed this machine for agents. The machine was not to exceed in size a shoe polish can. The encoding principle was similar to that of the Cipher Box. The equipment (consisted) of a rotatable inner disk and a stationary frame. The disk and frame had to be provided with scrambled alphabets similar to the Cipher Box. In operation the inner disk was rotated against the frame, and thereby in a manner similar to the Cipher Box, put a spring under tension. By means of a pressure and blocking notch, the disk is returned in various step lengths back toward its original position. In contrast to the Cipher Box, in this machine only control (wheels) with fixed notches were to be used. In the design, three control wheels to be set from the outside were to be included. The number of notches was to be determined once and for all for each pair of devices (one for the agent and one for central office). For this, a hand punch was thought of for punching the notches."

[79] I 96

[80] See also D 57 p 4.

[81] I 57 p 9.

According to Mettig:[82]

> "The security investigations on this machine by Dr. Huettenhain and Lt. Dr. Stein proved so successful that it was decided to employ the Cipher Disk as enciphering equipment for forward (Army) units and indeed for forward of Regt HQ."

In Dr. Huettenhain's records was found the following, dated 21 April 1944:[83]

> "The Chiffrier department requires.... 10,000 Cipher Disks and 20,000 sets each of 3 pin disc blanks."

The Army Security Agency has as yet made no serious study of this device, but it is believed that it has only limited security.

26. Foreign Office "Number Printer" produced non-random one-time pads-- A report on German cryptographic machines would not be complete unless it mentioned the "Number Printer" ("Numerierwerk") of the Foreign Office Cryptographic Section (Pers Z Chi). This device printed "one-time pads." These were used to encipher the Diplomatic Code Book (Deutsches Satzbuch); the system was called "GEE" at the Army Security Agency and was solved in the winter of 1944-45.

Cryptanalysts believe that a "one-time pad" is cryptographically 100% secure, if it is made up of random additive or key. The emphasis must be on the "random" as well as on the "one-time." The German Foreign Office Cryptographic Section (Pers Z Chi) overlooked the "random" when they made use of the Number Printer.

The Number Printer looked almost exactly like a large printing "job press." The type bed carried 240 small wheels, similar to the wheels on a rubber date stamp. Each wheel carried a sequence of ten digits around its periphery. The wheels were individually removable and interchangeable, as well as interchangeable in groups. Each time the press operated, it printed a sheet of paper with 240 numbers on it (8 lines of 6 groups of 5 digits). The press could be adjusted to print up to thirty sheets of paper identically, but was usually adjusted to print two sheets identically, one sheet of which became a page in a one-time "send" pad, while the duplicate became a page in the corresponding one-time "receive" pad. Before printing the next set of two

[82] I 96

[83] D 59 p 25

sheets, the machine proceeded to turn all the 240 wheels up one notch except such wheels as were at the moment kept from turning by special mechanical means. The cryptographic laws governing exactly which wheels paused in their movements, when and how often, were extremely simple. In principle, this was accomplished by what might be termed "non-turnover notches." These laws were discoverable by cryptanalysis. The result was that, while each page contained numbers that were random so far as that page alone was concerned, any given position on such a page was related to the same position on all the succeeding pages, and this non-random property permitted reconstructing sequences involved on the printing wheels. Shuffling of the sheets before binding into pad forms, of course, added to the cryptanalysts' difficulties, but did not prevent recovery and almost 100% reading of messages.

No Number Printer has ever been captured, but TICOM documents contain descriptions of early models.[84]

[84] T-1282. Captured files of the Foreign Office show that Number Printer apparatus was purchased from the German firms Maschinenfabrik Otto Krebs, and Clemens Mueller, in 1925, 1927, and 1933. See D-51 p 4. Similar number printer apparatus was offered for sale to the British Government on 14 June 1932 by the English firm Loranco Ltd., Engineers, by a Mr. Lorant, who described the apparatus, showed photographs, and stated that his firm (Loranco Ltd.) had supplied Number Printers to the German Government in 1925, 1928, and 1932. According to Mr. Lorant, the apparatus was for printing given numbers of copies of cipher telegrams, although it became immediately apparent to the British Government representatives that its real purpose was the generating of pages of random additives. Mr. Lorant stated that German Government had printed 2,000,000 pages without a breakdown, and that they kept an additional set of 250 spare wheels from which to choose. The British Government asked Mr. Lorant to submit prices, but apparently subsequently lost interest in his apparatus. The connection between the British firm Loranco Ltd., Engineers, and the German firms, is not known at this time.

VOLUME 2

Chapter V German Ciphony

27. German enciphered speech apparatus was unsuccessful.-- Telephone or radiophone transmission of intelligence, swiftly, accurately, and securely, has been a goal of cryptanalysts for many years. Such speech encipherment is called "ciphony."

German experiments with ciphony were singularly unsuccessful. No satisfactory ciphony method was developed at any time.[90]

Dr. Werner Liebknecht, of the Army Ordnance, Development and Testing Group, Signal Branch ("Wa Pruef 7"), where ciphony experiments were undertaken, stated:[91]

> "If a process giving unintelligible speech was arrived at, then unfortunately it always happened that the speech quality after unscrambling was no longer acceptable; and the process of scrambling was therefore unacceptable."

Speech encipherment experiments were carried out by the following seven German commercial firms from 1937 to 1940:

[90] I 57
[91] I 57

1. Siemens and Halske, Berlin.
2. Deutsche Telefon und Kabelwerke, Berlin.
3. Sueddeutsche Apparate Fabriken, Berlin.
4. A. E. G., Berlin. ("Allgemeine Elektrische Gesellschaft")
5. Telefunken, Berlin.
6. Dr. Vierling, Technische Hochschule, Hanover.
7. Fabrik C. Lorenz Aktiengesellschaft, Berlin, Muelhausen, Thuer.

In 1943 only Telefunken and Dr. Vierling worked on speech enciphering, and from 1944 on, only Dr. Vierling, at his Laboratorium Feuerstein ("Firestone Laboratory") at Ebermannstadt, Germany.

Dr. Vierling's laboratory was captured almost intact by TICOM, because of Dr. Vierling's orders on the eve of surrender that none of his expensive equipment was to be destroyed. Ciphony and other varied electronic researches were in progress at the time of surrender. Two Army Security Agency ciphony engineers were dispatched to Ebermannstadt to exploit the German ciphony research, in conjunction with U. S. Navy and British engineers. As a result of this exploitation, plus interrogations of other German engineers elsewhere, it is believed the German ciphony picture is fully known at least as far as concerns their latest experiments.

Six main ciphony methods had been developed by German engineers. These methods were called:

a. Frequency inversion.
b. Noise superimposition.
c. Time scrambling.
d. "Little Building Block."
e. "Big Building Block."
f. Triple wobbling.

Each method in turn promised to prove less unsuccessful than its predecessor.

28. Experiments showed frequency inversion insecure.-- Methods of frequency inversion usually require that speech frequencies (from 250 cycles per second to 2,750 cycles) be beat against a "carrier" frequency of about 3,000 cycles. The resultant frequencies are the differences in frequencies; these differences are transmitted. Thus, a low speech frequency of say 300

cycles would be transmitted as a high frequency of 2,700 cycles (or 3,000 cycles minus 300 cycles) whereas a high speech frequency would be sent as a low one.

The German inverter apparatus, which evidently worked along such lines, was "a large equipment of the size of a field telephone (installation) used in the field since the outbreak of the war. This set was considered safe and encouraged careless and insecure conversation. In reality it was possible with an ordinary receiver to re-establish the impulses normally. The equipment was, therefore withdrawn from units in 1942."[92]

There are no other important references to frequency inversion, and as it is considered insecure by most engineers everywhere, it is likely that no further experiments were carried out by the Germans along simple inversion lines.

29. Noise superimposition gave bad quality.-- Methods of noise superimposition require that the superimposed noise frequencies cover the speech frequency band width, so that the noise can mask out the speech. At the receiving end a noise is applied exactly equal to that applied at the sending end,, exactly 180 degrees out of phase, so that the noise component is cancelled and clear speech remains.

C. Lorenz, Berlin, experimented with this method from 1937 to 1939, and found that frequency distortion over transmission lines was too great, as well as that faulty noise cancellation gave poor speech quality.[93]

From 1939 to 1943, after exhaustive experimentation, Telefunken (Berlin) determined that it would be impossible to cancel the noise correctly, and the speech quality would never become acceptable.

In spite of this, an ultra-high-frequency radio link between Athens, Crete, and Derna continued noise superimposition tests. Results from these tests were also disappointing.[94]

No further details of the experiments are available.

[92] I-96

[93] I-57

[94] I-57

30. "Time scrambling" was insecure.-- Methods of time scrambling require that the speech at the sending end be recorded immediately (usually magnetically on a steel tape) as a means of storing it for encipherment; encipherment results from breaking up the stored speech into small elements (of 60 milliseconds duration in the case of the German devices) and transposing them. The transposed elements are then transmitted by radio or wire to the receiving station which stores them, retransposes them, and puts them into the receiving telephone as speech. These principles, for instance, formed the basis for the U. S. Army's AN/GSQ-1, or SIGJIP.

The first German experiments in "time scrambling" required a long "time-delay" in order to store sufficient speech for transposition, and still did not result in completely enciphered (unintelligible) speech.[95]

In order to reduce the amount of time-delay needed to accomplish complex enough transpositions to result in unintelligibility, Siemens (Berlin) attempted to divide the speech into three frequency bands, and scramble each band separately. Dr. Liebknecht said as follows: "Despite the large bulk of this equipment (each station weighed about 100-150 kilograms) this process did not deliver completely unintelligible speech. The device was never manufactured."[96]

Possibilities of time-scrambling were brought to the fore again in late 1944, when an American Mustang airplane was shot down and found to include in its equipment an American time-scrambling radio-telephone apparatus (SIGJIP). According to Lt. Col. Mettig of the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi):[97]

> "The technical experts believed that with the availability of necessary equipment, it would be possible to solve this apparatus in 10 minutes. The traffic was picked up on a sound track, photographed and through the regular division of the track it was possible for an expert to read the conversation. As a result, there was

[95] I-57
[96] I-57
[97] I-96

a controversy over the development of a German version of the Mustang apparatus. Forward units were of the opinion that it was impossible to carry out any tactical interception of such traffic since they would require a large quantity of special equipment. Consequently they felt the Mustang type could safely be used until a more practical machine was developed. The decision on this matter was never taken."

Time-scrambling devices were called "Tigerstedt" devices by German cryptographers (after a Swedish inventor named Tigerstedt). Dr. Fricke, of the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi), offered the following information concerning the American Mustang device:[98]

"He had seen an American machine on the Tigerstedt principle taken from a Mustang. It had a magnetophone band which revolved between nine heads which scrambled the speech horizontally (i.e. in time). This type of machine was rejected in Germany because you had to wait in between utterances for the machine to act. He himself did not think 750 milliseconds was very long to wait, but he supposed if a German major was talking to a general, the latter would find it desirable to cut him off abruptly with a reply."

There is no indication in the interrogations that Tigerstedt devices were ever adopted and used by the Germans.

31. "Big Building Block" proved too difficult to control. -- Since German ciphony experiments indicated that too much time would be required to develop secure ciphony apparatus, plans were developed for the independent construction of a machine which could be built quickly as a "stop-gap." The first of these attempts resulted in the "Building Block" ("Baustein"), later renamed the "Big Building Block" ("Der Grosse Baustein") after it was discovered that a second and still simpler device (called the "Little Building Block") would be needed.

The "Big Building Block" used the principle of "ring wobbling." "Ring wobbling" was the name given to a process

[98] I-20

by which the voice frequencies were shifted up and down the frequency scale. When they were shifted up, the frequencies at the top were electrically taken out of the spectrum and put back in at the bottom of the scale; when they were shifted down, the frequencies at the bottom were electrically taken out of the spectrum and put back in at the top of the scale. The process was called "ring," because what went off at the top came back around to the bottom, and vice versa. It was called "wobbling" because the frequencies wobbled or shifted, by being modulated on a "wobble frequency" "carrier." American engineers call the process "re-entrant wobbling."

Obviously such a system needed a wobbler--an agent to control the amount of the wobbling of the wobble frequency. In the case of the "Big Building Block" the wobbler was to have resulted from an autokey. The enciphered voice itself, operating through a time delay circuit, 100 to 200 milliseconds later, provided the key for enciphering the following voice.

We have on record the following epitaph:[99]

> "The experiment resulted in such difficulties in control of the receiving equipment that the experiment up to the present has led to no conclusions."

32. "Little Building Block" combined noise superimposition and frequency inversion.-- The "Little Building Block" ("Der Kleine Baustein") was intended to be a low-security speech scrambler for land-line use only.[100] It was to be secure against the human ear only. It combined noise superimposition and frequency inversion. Speech frequencies of from 300 cycles per second to 1,300 cycles per second were accepted by the filter system. These were inverted alternately by a 1,700 cycles per second carrier resulting in a frequency band from 1,400 cycles to 400 cycles; and by a 2,700 cycles per second carrier, resulting in a frequency band from 2,400 cycles to 1,400 cycles. The alternations in choice of carrier for inversion occurred about three to six times per second, depending upon the volume level of the speech. Into whichever of the frequency bands the speech was not inverted, noise was superimposed. Thus if inverted

[99] I-57

[100] I-57; E-9

speech occurred in the 400-1400 cycle band, noise occured in the 1400-2400 cycle band; and vice versa. Note that the noise was not superimposed at the same frequencies as the speech, as in the noise superimposition method described first; therefore, it could be eliminated by simply being electrically ignored at the receiving end, provided, of course, the receiver had the appropriate apparatus. The receiver then would proceed to re-invert the speech, rendering it intelligible.

This apparatus was under test by Dr. Vierling at the close of the war; but only a single one-way circuit had been constructed for the tests.[101] Evidently switching imperfections, bad filter networks, and scarcity of electrical parts, prevented its development. The apparatus was not complete when captured, but diagrams are available.[102]

33. Hopes centered on synthetic speech enciphered by "triple wobbling."--German engineers recognized as early as 1939 that synthetic speech might prove easier to encipher than actual speech. Experiments were begun which resulted in the development of a synthetic speech apparatus called "Anna" by the German engineers, and patterned closely after the American "Vocoder," patented by Homer Dudley of Bell Telephone Laboratories. The German apparatus, "Anna," divided actual speech into eight separate frequency bands, by means of filter networks. It produced eight carrier frequencies, to correspond to the eight speech bands; and when the energy level of any speech band varied, the amplitude of the corresponding carrier frequency varied in proportion. These carrier frequencies, plus two more carriers each of which represented variations in the pitch of the speech fundamental and whether or not the speech was "voiced" or "whispered," formed the set of ten carriers which was then to be enciphered.

"Triple wobbling" was the method proposed for the encipherment. By this process, the composite set of carriers (ranging in frequency from 450 to 2110 cycles per second) was passed through a single stage of ring wobbling much as in the "Big Building Block;" the output from this stage of wobbling

101 E-9

102 E-9

was split by filters into halves, and each was separately ring-wobbled; these two outputs were combined and passed through a third stage of ring wobbling. The signal was then passed through a fixed carrier modulator which restored the scrambled signal to a transmittable frequency range.

The following are important to note: Wobbling was to have been done three separate times; wobbling was to have been controlled by a specially built cipher machine, and not by an autokey system as in the "Big Building Block."

Dr. Liebknecht said:[103]

> "A triple wobbling project is still under way at the Feuerstein Laboratory, but it is also very complicated. Through this system, condensers were to be turned under the influence of teletype impulses from the SZ-42 enciphering device, and thus the wobbling is to be brought about. Until now the results from triple wobbling have not been very satisfactory. The speech quality after dewobbling was very bad."

Excellent descriptions of the speech filters et-cetera appear in the TICOM reports.[104] It is believed by Allied investigators that "triple wobbling" would not have proved satisfactory unless much research could have been carried out, especially in filter designs. Nevertheless, German hopes of successful ciphony apparently centered on synthetic speech enciphered by "triple wobbling."

34. Conclusions: Germans had no usable ciphony machines.--Unless new evidence is unearthed the conclusions are: Germany had no usable ciphony machines; and Germany probably would not have had any usable ciphony machines even if the war had gone on several more years.

[103] I-57

[104] E-9, E-10, E-11

VOLUME 2

Chapter VI - German "I.B.M." and Rapid Analytic Machinery

35. German "I.B.M." equipment paralleled ours.-- Electric accounting machines using punch cards, called "Hollerith" throughout Europe and simply "I.B.M." (after International Business Machines Corporation) in America, are a primary yardstick of cryptanalytic progress. By this yardstick the Germans measured up well.

A chart comparing the I.B.M. equipment of the principal German cryptologic bureaus with that of the Army Security Agency (U.S. Army) is shown herewith as Chart No. 2-2. (See next page.)

From the chart it may be seen that the estimated total number of I.B.M. machines used by the German non-Navy bureaus was less than the total employed at Army Security Agency; but if the Army Security Agency machines devoted exclusively to the attack on Japanese Army systems are not counted, than the German non-Navy machines in general probably exceed the Army Security Agency machines.

Four key punches, 2 sorters, 1 collator, 2 reproducers, 1 multiplier, and 1 tabulator, represent

I.B.M. PUNCH CARD ("HOLLERITH") EQUIPMENT OF THE SIX PRINCIPAL GERMAN CRYPTOLOGIC CLEARINGHOUSES COMPARED WITH THAT AT ARMY SECURITY AGENCY

	OKM/4 SKL/III (Navy)	Pers ZS and Chi (Foreign Office)	FORSCHUNGS-AMT (Goering's Research Bureau)	OKW/Chi and OKH (Supreme Command and Army)	OKL (Air)	German Non-Navy	ARMY SECURITY AGENCY (U.S. Army)		
	Cryptanalysis Cryptography	Cryptanalysis Cryptography ?	Cryptanalysis	Cryptanalysis Cryptography	Cryptanalysis Cryptography	TOTAL at least	TOTAL	General c.anals. Cryptography	Jap Army Code Solution only
Punches and verifiers	30	20	10*	40	20	90	109	35	74
Reproducers	6	2	1	8*	2*	13	52	10	42
Sorters	7	10	4	30*	5	49	85	27	58
Collators	1	2	0	4*	?	6	39	13	26
Multipliers	3	1	0	0	?	1	4	1	3
Interpreters	0	0	0	0*	?	0	7	1	6
Tabulators, all types	7	6	3	2	3*	14	47	10	37
Special Equipment	2 tape-to-card readers	1 comparator counter. 1 selective	?	?	? tape-to-card readers	-	-	11 card operated typewriters 2 presensing gang-punches	4 tape-to card readers. 4 presensing gang-punches. Also special attachments**
Personnel	80	45*	15*	150*	50*	260	1100	300	800
References	I-146 I-158	I-1 I-22	I-25 I-58 I-96 I-113 I-67	I-20 I-127 I-152	I-119	-	-	-	-

*Estimated

**See Chart No. 2-3, following page 50.

Chart No. 2-2

the total of captured I.B.M. equipment belonging to the German signal intelligence organizations; these were captured at Zschepplin; they belonged to the Foreign Office Cryptanalytic Section (Pers. Z S). Their wires were all ripped out and plugboards missing. They were studied briefly by TICOM Team 1 and then destroyed by dynamite.[109] Therefore, practically all our knowledge of German use of I.B.M. must come from the TICOM interrogation reports, and these discuss I.B.M. but scantily. Nevertheless, scattered remarks indicate the used to which the I.B.M. machines were put by the Germans, and under what conditions. These technical uses were almost identical with those at Army Security Agency. The important excerpts from the interrogations are given below:

a. Dr. Buggisch, of the Signal Intelligence Agency of the Army High Command (OKH/G. d NA), stated as follows concerning the use of I.B.M. by his agency:[110]

> "Some of the bigger I.B.M. machines were always being provided with special new wirings for special cryptanalytic purposes, as for non-carrying addition and subtraction in code work. Most of the tasks, however, consisted of the usual statistics (digraphs, trigraphs, "chain" statistics, "column" statistics, and of simple figure calculations, e.g. in work on Hagelin Machines). But, as a rule, no tasks were undertaken which could not have been carried out by hand by perhaps 100 people in a reasonable time."[111]

b. Evidently Army code problems (usually problems of finding messages in depth) were turned directly over to the I.B.M. section. An interrogation report stated:[112]

> "A new (Russian) code came in October 1941, and depths were less thereafter. Buggisch and other mathematicians were withdrawn from this work in November 1941, and he states that the problem was handed over largely to the I.B. M. section."

[109] I-1
[110] I-67
[111] At the Government Code and Cypher School the basis was 20 to 25 persons.
[112] I-58

c. A complaint by Dr. Buggisch on the way I.B.M. mishandled some of its more specialized statistics was recorded in one report as follows:[113]

> "The breaking of cipher texts (without crib) is possible when the pin arrangement of the pin wheels can be discovered from column statistics of the cipher text....The calculation is carried out with an I.B.M. machine provided with special wiring. As mistakes were frequent and the time required was considerable, the construction of special calculating machines for this purpose was proposed."

(It so happens that I.B.M. is not well adapted to solution of the Hagelin machine, as the Army Security Agency, U. S. Army, has itself found out. The number of operations required to furnish all necessary statistics by the I.B.M. method allows for too many handling errors.)

d. A further reference to the German Army use of I.B.M. is made with reference to a double transposition used by the Allies in Italy in February 1945. Such messages included times of origin in their plain text, with such times of origin first enciphered by digraphs involving infrequent letters. (These enciphering alphabets never changed.) The whole messages were then subjected to the double transposition encipherments. The times of origin were seldom more than half an hour before the times of sending, so the Germans had information they could "crib into" the cipher text, once they had broken the digraphic substitution. These cribs were at least four letters long, and in short messages could almost always be placed accurately. Corporal Clemens Schuck of Inspectorate 7/VI (In 7/VI) stated as follows:[114]

> "A four letter entry would thus be obtained. Such a combination would be run through all the possible widths on the I.B.M. machines. The time required to break these messages was one to five days, depending on the number of men and machines available."

[113] I-137

[114] I-80

e. Some of the I.B.M. machines the Army had were evidently not working too well. The following was learned from Dr. Fricke, when he discussed the making up by the German Army of some of its own keys and tables:[115]

> "Daily changing trigraphic substitution tables were introduced (by the German Army). They were made at first by I.B.M.....The section moved to Weimar late in the war, and there the machines were so old and out of repair that they made too many mistakes in the tables."

As a result, Fricke had the tables handset by a printer. This later method proved more efficient.

f. Specialist Voegele, discussing the use of I.B.M. by the Signal Intelligence Agency of the Commander in Chief of the Air Forces (Chi Stelle Ob d L), stated as follows concerning June 1942 Allied air traffic:[116]

> "The breaking of strip traffic was subject to time lags of two months before the receipt of I.B.M. machinery, but only two to four weeks afterwards."

According to another report by him I.B.M. was used in "brute-forcing," or the discovery of depths by double repeats.[117]

g. I.B.M. was used in a "brute force" method applied to the British Naval Cypher "to find double repeats at intervals up to 10," by the Signal Intelligence Agency of the Navy High Command (OKM/4 SKL/III), according to Oberregierungsrat Tranow and Graduate Engineer Schmalz.[118] I.B.M. was also used by them to provide "a catalogue of differences, repeats, and double repeats," and most interestingly, "reciphering of captured subtractor groups." By this last was meant that captured additive was applied to known high-frequency unenciphered code groups, to obtain a catalogue of likely enciphered code groups against which messages could be tested--a key finding technique often used at Army Security Agency.

[115] I-20

[116] I-119

[117] I-152

[118] I-146

h. A "baby brute force" (index of single hits between messages known to be from approximately the same part of the additive tables) was also carried out by I.B.M. in connection with British codes.

i. Senior Specialist Tranow and Graduate Engineer Schmalz stated as follows:[119]

> "Five per cent of our I.B.M. capacity was devoted to producing our own cipher systems. We constructed reciphering tables, substitution tables, and the Signal-Tafeln, e.g., reciprocal 2-letter tables, 3- and 4-digit figure tables. The number of cards needed for each substitution table was one set, for 2-letter tables was 26 x 26, and for the 3- and 4-figure tables was 1,000 and 10,000 respectively."

36. Rapid Analytic Machines were built on simple and effective lines.--Just as in the United States, cryptanalysts in Germany felt the need in special cases for more rapid means of searching, comparing, and otherwise statistically treating code and cipher texts than hand and I.B.M. methods could offer. They developed a series of teleprinter tape devices, employing photocell readers, which accomplished these tasks speedily, inexpensively, and very practically. Such machines may be called "rapid analytic machinery." They differed from rapid analytic machinery developed in the United States in that in general they employed teleprinter (paper) tapes, rather than celluloid film. However, it is true that the first German film device was in process of construction; it was almost identical to our "Tetra-Tester," and had an estimated speed of search of 10,000 letters per second, as against the actual speed of the Tetra-Tester of 5,000 per second.

In comparing the states of development of German rapid-analytic machinery with American, it might be said (loosely) that the German scientists were a year and a half behind the Americans. Development of rapid analytic machinery was done almost entirely by the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi), and this mainly as a result of security studies. The special Cipher Security Section was formed

[119] I-146

within OKW/Chi in 1940, later being put under control of Dr. Huettenhain. Interrogation of Dr. Huettenhain revealed:[120]

> "By 1941 it had become clear that machines would be necessary for the dual - offensive and defensive - task of research, but engineers were not obtained until 1942, when the following were appointed: Two graduate engineers: ROTSCHEIDT (formerly with Siemens) and JENSEN (who came directly from school), both telecommunications experts. (These are now thought to be in the South); three working engineers, TODT, SCHAEFFER, and KRACHEL (with a Technical High School Training), who were decidedly subordinate to Rotscheidt and Jensen; and twenty-five mechanics.
>
> "They decided to use I.B.M. wherever possible, but it was found that I.B.M. machinery was not suitable for all problems, and auxiliary deciphering machines were developed as the occasion arose. Special problems were laid before the engineers, and they were told 'This is what I want to do, how would you do it?' The machines which resulted were built in a more generalized way than the immediate problem demanded so that they could be of use again."

As a result the following special machines were developed:

a. Digraph "weight" recorder.
b. Polygraphic coincidence counter.
c. Statistical "depth increaser."
d. Differencing calculator (non-recording).
e. Differencing calculator (recording).
f. Likely additive selector.
g. Simple counting apparatus.
h. Proposed repeat finder.

Chart No. 2-3 herewith, compares these rapid analytic machines, developed by the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi), with those owned by the Army Security Agency.

[120] I-31

37. Rapid analytic machines developed by Armed Forces cryptanalysts described.--The main features of the rapid analytic machines developed by the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) were as follows:

a. Digraph "weight" recorder.--The "Bigramm Suchgeraet," or "digraph search apparatus," was a device for making frequency evaluations of digraphs and recording the evaluations. It cost approximately $5,800.00[121] and was the most expensive rapid analytic machine owned by the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi).

It was used to solve the Japanese two-letter transposed code (J-19, or "Fuji") "and the machine would find a solution in less than two hours."[122] It did the work of twenty people, according to Dr. Huettenhain.[123] "The machine was once used for work on an English meteorological cipher, figure traffic employing a stencil, when Huettenhain liaised with the Air Force Weather Service. They were allowed to use the machine."[124]

The digraph "weight" recorder consisted of: two teleprinter tape "reading heads," a relay-bank interpreter circuit, a plugboard "weight" assignor, and a recording pen and drum.[125]

Each head read its tape photoelectrically, at a speed of 75 positions per second.

The interpreter took the two impulses from the reading heads at any given moment, and translated them from two separate letter impulses into one digraphic impulse, which it sent to the plugboard.

The plugboard contained 676 jacks on its left side, representing digraphs; these could be wired at will to any jack in any one of five different sets of jacks on the right side of the plugboard, these sets representing "weights." Thus on the plugboard, any digraph could

[121] D-60

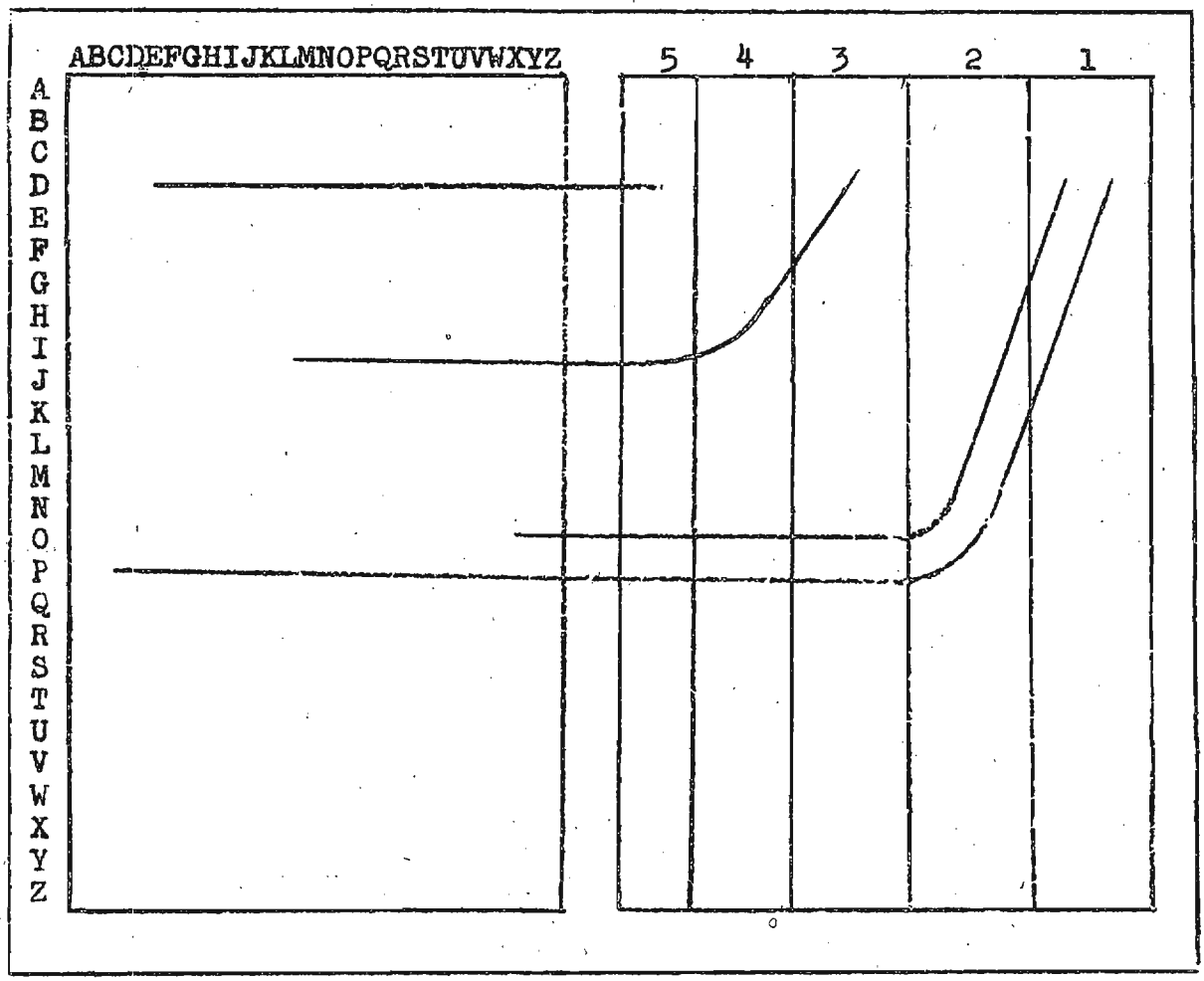
[122] I-31

[123] D-60

[124] I-31

[125] I-37

be assigned any integral weight from 1 to 5 by simply plugging the digraph to the weight; unplugged digraphs had the value zero. A sketch of the plugboard follows:



In the foregoing sketch, for illustration, the digraph DE was given the weight 5, the digraph IL the weight 3, the digraphs PC and OX were each given the weight 1. All other digraphs had the weight 0.

The recording device was in effect an undulator. It consisted of a paper drum revolving at an even rate under a pen which in turn moved on a spindle across the drum. As a result the line traced by the pen was a cylindrical spiral. Undulations occurred in this spiral however, wherever a digraph occurred with a weight other than 0. The heights of the undulations varied directly

with the weights assigned the corresponding digraphs.

This device was said to have made solution of a single transposition easy. Such solution is a familiar process to most cryptanalysts, requiring much trial and error. A message under study must, in effect, be broken into likely columns and these matched against each other, with the resulting digraphs being examined for their "goodness" to determine whether or not such matches are probable. If, for instance, the message is broken into sixteen columns, there are 1,307,674,368,000 (factorial 15) possible matches, but these are attacked of course by successive steps: that is, one column is tried against each of the other fourteen and the most probable combination selected before proceeding further; with this pair as a basis, another of the remaining thirteen columns is selected to add to the left or right of the initial pair, and so on.

It is assumed that the German digraphic weight recorder was used in the following manner to solve such single-transposition problems:

Two duplicate teleprinter tapes were punched, corresponding to the message to be solved, each tape then being formed into a loop and one loop being made one space (or more) longer than the other, so that as they revolved through the tape reading heads they would "slide" relative to each other. Digraphic weights, probably logarithmic in nature, were then plugged up on the plugboard and the machine started. The result would be an undulatory graph indicating, digraph by digraph, for every possible juxtaposition of the whole message against itself, the probability of a "good match" at each point along its length. Careful investigation of this graph would thus show visually (by dense areas of tall undulations) those positions where "good" matches occurred, and the limits in length of each such good match--that is, the length of the columns involved.

The German digraph weight recorder was therefore quite different from the Army Security Agency's "electro-mechanagrammer," which also was designed specifically to solve the Japanese J-19 code. The American machine ran a deck of I.B.M. cards representing the message under study through an I.B.M. tabulator, with a specifically chosen section of the message (representing a definite column) wired up on the plugboard; digraphs were weighted

with ten logarithmic probability values (ranging from 0 through 9) and totals were printed, rather than individual weights being recorded separately as in the German digraphic weight recorder. The American machine took about four minutes per section to calculate and print the results. If the sections of text chosen from any given message were well chosen from a cryptanalytic viewpoint, the American machine proved much faster than the German machine, because the print of totals was easier for the cryptanalyst to analyze than just the individual values listed by the German machine; but if the sections of text were not well chosen and no true columns were included in the choice, then the German machine had the advantage, since it recorded all possible juxtapositions quickly, and all true matches were included in the data.

The German digraph weight recorder could also be used to advantage to locate coincidences between messages. The digraphs aa, bb, cc, ... zz, could be plugged up to the value 1 and all other digraphs left unplugged. Then when two message tapes would be run against each other, coincidences would be shown by the undulator. Such an arrangement would be especially valuable in revealing interrupted repetitions.

b. Polygraph coincidence counter.--The "Saegebock," or "Sawbuck," was a machine for recording the frequency of polygraphs occurring within one message, or for counting polygraphic coincidences between messages.[126] It was especially useful for work on periodic substitutions. Polygraphs could be of any size up to and including decagraphs. The machine cost approximately $1,200.00.[127]

The apparatus consisted of two teleprinter-tape "reading heads," a "calculator" (not described), and ten different "recorders."

Each head read its tape photoelectrically and had a speed of 75 positions per second. Each recorder comprised a pen which recorded dashes on a paper strip 20 inches wide, making a short dash whenever the recorder received an impulse from the calculator. The short dashes combined to form dashes of varying lengths. One recorder was assigned to "count" single letters, another to "count" digraphs, another to "count" trigraphs, and so on, up to ten.

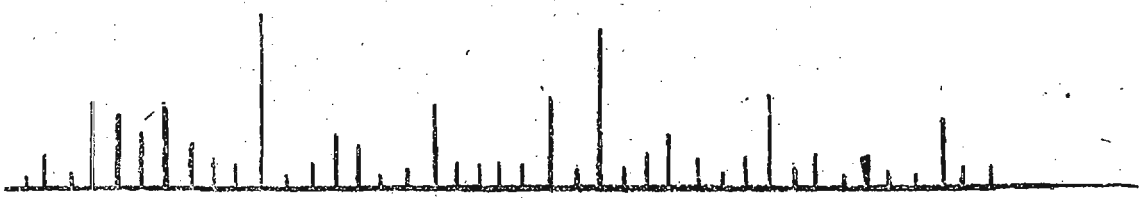
[126] I-37, I-31. The Germans adopted cover names for many of these devices, and these names were apparently not selected at random; but like ours, were derived from characteristics of the devices. The cover name "Saegebock" was probably so derived.

[127] D-60

The machine worked as follows: if it was desired to record the number of polygraphic coincidences occurring within one message, two duplicate tapes corresponding to the message, were prepared as described above in connection with the digraph weight recorder, the looped tapes then being inserted in the two reading heads and the machine started. During the first revolution of the loops, each recorder would make a short vertical stroke every time a coincidence of the length assigned to that recorder occurred between the tapes. Thus, if there were ten digraphic coincidences between the tapes during the first revolution, then recorder number two made ten small strokes, each above the other, so that a line ten units high resulted; if there were four trigraphic coincidences, then recorder number three made four strokes, and so on.

All the recording pens then returned to the zero position and the paper in all the recorders moved along one step automatically, to be set for the next revolution of the tapes, wherein the tapes were of course at a different juxtaposition.

A polyalphabetic substitution of period seven being studied might therefore have given a chart of single letter coincidences at the different justapositions of the tapes, much as follows:



Highest single letter coincidences in this sample are indicated at intervals of seven, the causal interval.

To record the number of polygraphic coincidences between two different messages, a tape would be punched for each message, and similar procedure followed with these two different rather than duplicate tapes, as in the first case.

Drs. Huettenhain and Fricke did not identify the specific cryptographic systems the polygraphic coincidence counter was designed to attack. Dr. Huettenhain stated, however:[128]

[128] I-31

"The problem was to determine the periods in short periodic substitutions by finding the distances between repeats in a message....It (the counter) could also be used to find two enigma messages in depth."

The foregoing machine was one of a class called "Fasen Suchgeraet (Perioden)," or "Phase search apparatus (Periods)."

c. Statistical "depth-increaser."--The "Turmuhr," or "Tower clock," was a device for testing a sequence of thirty consecutive cipher letters statistically against a given "depth" of similar sequences, to determine whether the former belonged to the given depth.[129] It was used "primarily for work on the U.S. strip cipher, when cribbing which was generally employed was impossible."[130] It cost approximately $1,000.00.[131]

The apparatus consisted of a single teleprinter tape reading head (speed 1 1/2 symbols per second); a storage means, by which any one of five different scores could be assigned, on a basis of frequency, to each of the letters in the 30 separate monoalphabets that resulted from the 30 columns of depth; a distributor that rotated in synchronism with the tape stepping, and selected which set of 30 scores was to be used as basis for evaluating the successive cipher letters; and a pen recording device.

The machine was used somewhat as follows:

First, several sections of cipher text, believed from statistical study to be enciphered with the same set of strips and on the same generatrix, were superimposed properly. As a result, the letters within columns fell into successive and separate monoalphabets with characteristic frequencies. A new section of 30 letters of cipher text would have to "match" these alphabets, that is, show a greater than random number of coincidences with them, before it could be added to this depth. The machine was used to test the goodness of such a match. Weights were assigned each letter in each of the basic thirty alphabets, depending on the frequencies therein, and these weights were "stored" in the machine. A message under study was punched on tape; the tape was run through the

[129] I-20, I-37

[130] I-31

[131] D-60

machine; the machine read the cipher text in sequences of thirty; for each sequence it applied the proper weights to each of the letters by choosing the weights from the thirty alphabets in succession; it recorded the total weight for each sequence by strokes of the recording pen. A long resultant stroke meant a great total weight; a sequence giving a long resultant stroke probably therefore belonged to the basic set of superimposed sequences.

Dr. Huettenhain and Dr. Fricke, of the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi), in describing the statistical depth-increaser stated that it had a photoelectric reading head.[132] In view of the also-stated speed of 1 1/2 symbols per second, which is reasonable considering the probable slowness of the distributor, a photoelectric head hardly seems likely, and it is believed that actually a standard teleprinter reading head was used. They stated that "provision is made for 5 different scores," which seems reasonable, although a written description of the machine found in Dr. Huettenhain's papers indicated that 20 scores were possible. which seems unreasonable.[133] Drs. Huettenhain and Fricke also stated:

> "The cipher text passages already recognized as on the same key are stored in the calculating apparatus of the 'tower clock' as a basis on which to start; and in such a way that for each of the substitution alphabets the elements receive different scores according to the frequency of the cipher texts.."

It is believed this storage was done by hand after collection and examination of the cipher text, rather than mechanically by a huge and unnecessary bank of relays, as might be inferred from their statement.

The machine was named "Tower clock" because it ticked after each set of calculations. Presumably it could be operated by the cryptanalyst himself.

d. Differencing calculator (non-recording) and additive tester.--This machine (German name not known) was a manually-operated device designed to assist additive recovery in superenciphered code problems, by speeding the differencing of depths of super-enciphered code groups

[132] I-37

[133] D-60

and the trial of likely additives thereon.[134] It cost approximately $40.00.[135] It was identical in its function to the U.S. Navy "CXDG-CNN-10ADW." often called the "N.C.R. differencing calculator." The German version had a capacity of thirty 5-figure groups, as against the N.C.R. capacity of twenty. The German device was much slower to operate, though far simpler in construction.[136]

The German differencing calculator consisted of five small metal rods arranged vertically and side by side. Down each rod were 31 small metal "rollers," each roller carrying on its periphery the sequence of figures 0, 1, 2, 3, ... 9. A skeleton sketch of the machine, with its cover removed, is shown, on the following page, just as drawn by Dr. Huettenhain.[137]

The top roller of each rod was fastened permanently to its rod; each of the lower thirty rollers was rotatable independently on its rod so that it could be set at will to any of its ten possible positions. Each of the five rods revolved at will, carrying all of its thirty-one rollers around with it simultaneously. The apparatus had a lid which when closed revealed only the one figure at the center of each roller. (In the sketch, if the lid had been closed, the five rollers across the top would have indicated the five-figure group "00000," the next row of five rollers would have indicated the group "13870," the next row, "44651," and so on.)

Differencing a depth of 5-figure enciphered codegroups was a simple process with this machine. The five rods were locked into position with the top (fixed) row of rollers reading "00000." Then the first enciphered code group in the depth was set up on the next row of rollers (marked row "1" in the sketch) then the second enciphered code group was set up on row "2;" the third enciphered code group on row "3," etc., until all the enciphered code groups were set up. Then the five rods were unlocked.

To subtract the first enciphered code group (appearing in row "1") from all the others, all one now had to

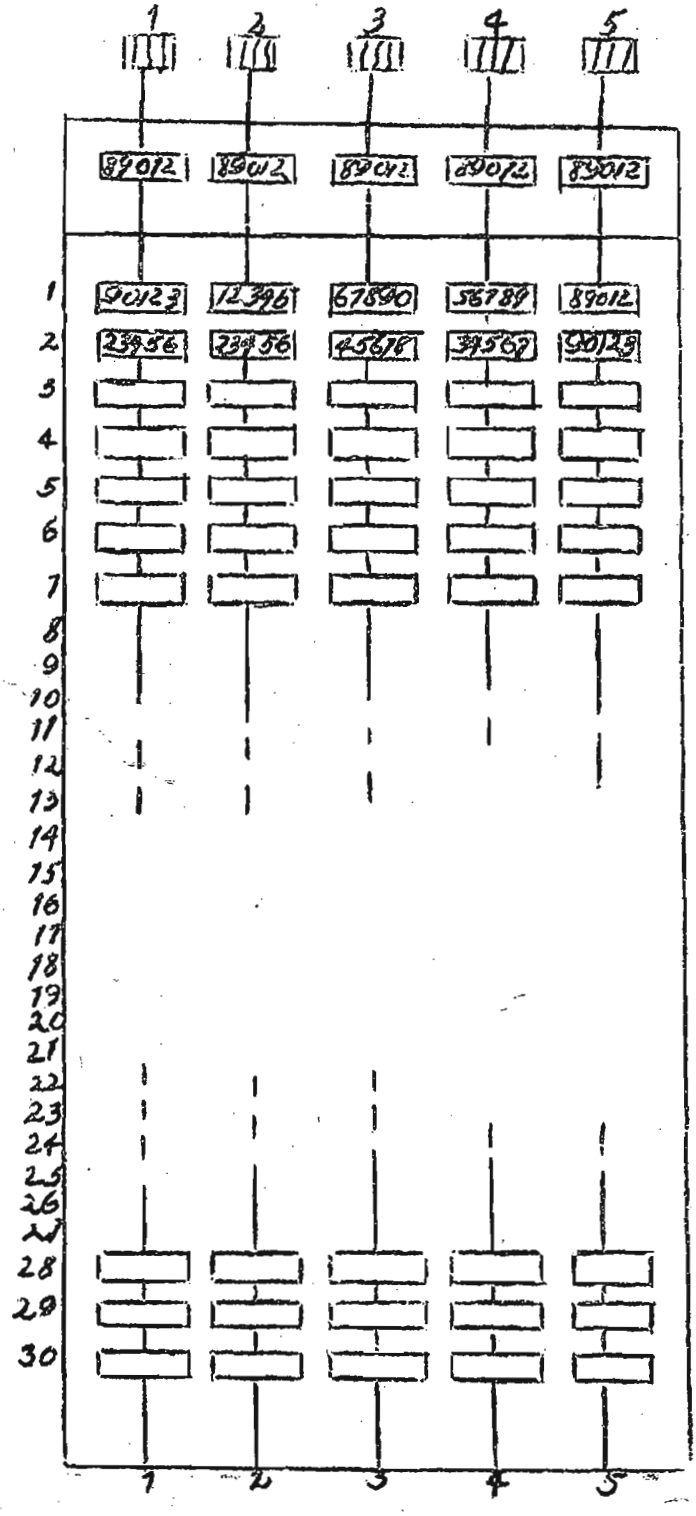
[134] I-37

[135] D-60

[136] Army Security Agency constructed a differencing calculator in 1943 identical in principle to the German device. It was a rough model and was not perfected because the N.C.R. devices were made available. It is now in the Army Security Agency museum.

[137] I-37

German Differencing Calculator, Non-Recording



do was to rotate each of the five rods until the rollers in row "1" read "00000." The numbers appearing in all the lower rows now represented "differences." These differences could now be looked up in "difference tables," and the most probable unenciphered pairs of code groups they represented be noted down for trial--an analytic process familiar to all cryptanalysts. To "try" one of these likely unenciphered groups with the aid of the machine, all one had to do was to rotate the five rods until it appeared in the window instead of the enciphered code group supposed to be representing it; immediately all other rows represented the consequences of the assumption, and the very top row (above the row marked "1") represented the enciphering "additive."

This device could be operated by the cryptanalyst himself at his own desk.

e. Differencing Calculator (recording).--This machine which the Germans probably called the "Differenzen Rechengeraet," or "Difference Calculating Apparatus," was designed to compute a "flag of differences" for a set of enciphered code groups and to record this flag.[138] It consisted of two teleprinter tape photoelectric reading heads, a set of calculating relays, and a recording electric typewriter. The speed of the whole machine was limited to 7 symbols a second by the typewriter speed, with time out for carriage return and line feed. It cost approximately $800.00.[139]

This machine worked as follows: the figure groups between which differences were to be made were punched onto a tape. A duplicate of the tape was made, with one blank group additional. The two tapes were formed into loops and placed into the reading heads, so that the first group of the duplicate tape and the second group of the original tape were ready to be read at the same time. The machine was then started. The calculating relays computed the difference (modulo 10) between the two groups and the typewriter recorded it; the two tapes then stepped simultaneously, and the difference between the second and third was computed and recorded; then between the third and fourth; and so on. On the second time around, since the duplicate tape was one group longer than the original, the "offset" was automatically changed so that the first group was now differenced with the third group, the second with the fourth, and so on. In this way every group was

[138] I-37

[139] D-60

eventually differenced with all other groups. The "flag" actually came out as a rectangle (rather than as a triangle). That is, the difference between the first group and the second was recorded, as also was the difference between the second and the first (a complementary difference). This gave an opportunity to ignore all "minor" differences and consider only "major" ones.

A second version of this machine was built, in which one tape was left in strip form and one tape used as a loop. The strip tape moved through the reading head for one group only; this group was read and stored in the computor; the loop tape revolved; the computor subtracted the stored group from each group in turn of the revolving tape; when the revolving tape made one complete revolution the strip tape moved up to its second group; this second group was stored in the computor and subtracted from every group of the revolving tape; and so on until each group had been subtracted from every other one.

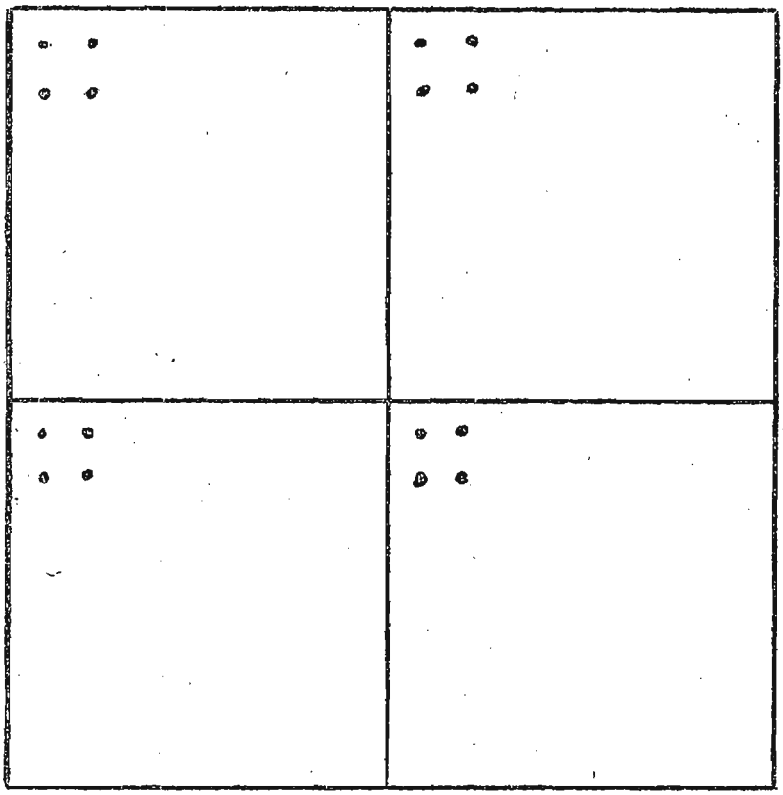
f. Likely-additive selector.--The "Witzkiste," or "Brainbox," was an exceptionally simple device for removing additive from a column of super-enciphered code groups arranged in depth. It could be used with any four-digit (or smaller) enciphered code, the frequency of whose unenciphered code groups had been discovered from previous removal of additives.[140] Five-digit codes had to rely on the differencing calculators previously described. The cost of the "Witzkiste" is unknown, but believed less than $50.00.

Suppose, for example, a four-digit code was under study, and that the following three unenciphered code groups were known to be high-frequency groups, from the removal of additive from previous depths: 0032, 0033, and 6748. Then if enciphered code group "0000" appeared in a new depth, it very likely resulted from additive 0078, 0077, or 4362. Similarly, if enciphered code group "0001" appeared in the same depth, it very likely resulted from additive 0079, 0078, or 4363. (Note that additive 0078 has been indicated twice.) Any other enciphered code group in the depth would also have a set of three likely additives associated with it. A tally of these additives would show highest frequency for the most likely additive for that depth.

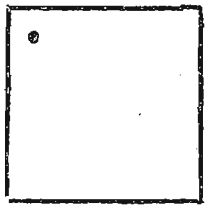
[140] I-37

The "Witzkiste" was a device for tallying such likely additives photographically. In essence it consisted of a "lattice-frame," with each cell therein representing one of the different possible additives from 0000 to 9999; a black-enameled glass plate which fitted under the lattice-frame and was removable; a light source behind both; and a camera in front. For the specific code used in the example in the preceding paragraph, the glass plate would have had the black enamel scratched off at positions 0078, 0077, 4362 (the likely additives for "0000"). Whenever enciphered code group "0000" appeared in a depth, the glass plate would be placed between the lattice and the light source, and the lattice photographed. Only additive positions 0078, 0077, and 4362 would be photographed because only in those spots could light appear. In case enciphered code group "0001" appeared in the depth, the same glass plate would be placed between the lattice and the light source, but moved one position over, and the lattice would be photographed -- on the same piece of film. Only additive positions 0079, 0078, and 4363 would be photographed this time. But since 0078 would now have been photographed twice, it would appear darker when the film was developed. Thus the one glass plate could be slid around and made to tally likely additive for any one of the ten-thousand possible enciphered code groups that might be encountered in a depth; and the additive whose position was darkest, after development of the film, was the most probable one; that is, statistically, it was likely to be correct.

The "Witzkiste" was complicated slightly by the fact that additive-encipherment addition is non-carrying (that is, modulo 10). In order to make the same glass plate and lattice do for all enciphered code groups, in view of the non-carrying addition, the glass plate had to be sixteen times as large as it would have been with normal addition (each additive scratch having to be entered in 2x2x2x2 different positions instead of one) and the lattice frame had to be four times as large. This can be explained to a mathematician by saying that to accomplish four-digit addition modulo 10, the lattice-frame was spread out double size in two dimensions to eliminate carry over, and the scratches on the glass were doubled in each of four ways to make the system re-entrant. Such a glass plate for one additive would have looked as follows:



instead of
as follows:



In the two drawings the black spots represent holes scratched in the black enamel of the glass plate to represent just one additive. In actual practice, many additives of course would be represented.

With the "Witzkiste" made as above, testing for most likely additive was rapid and simple and as described. Final photographs could be printed out on print paper, or projected onto a screen for study.

g. Simple counting apparatus.--This is best described in the words of Dr. Huettenhain as follows:[141]

"By means of simple counting apparatus it is possible quickly to work our statistics, when there are not more than 100 different elements.

"100 counting machines (Post Office counters) are put side by side. The text for which statistics

[141] I-37

are to be worked out is punched on a tape. The perforated strip is read and the symbol in each case put on the corresponding counter. The counters are read off and their position photographically recorded.

"In practice this apparatus was used with success within the scope of the investigations into the security of our own systems."

Cost was approximately $600.00.[142]

h. Proposed "repeat finder."--This ultra-high-speed machine, planned and in production but not yet finished, was designed to study from 20 to 25 messages for repetitions of five or more characters. Each message could be 500 letters (or figures) in length. Thus study of approximately 10,000 letters of cipher text could be undertaken at any one time.

Dr. Huettenhain stated as follows:[143]

"The 10,000 letters were recorded one after another as 5-unit alphabetical symbols onto an ordinary film. A duplicate was made. Both strips were now to pass at high speed in front of a reader working without inertia [i.e., a photocell reader]. In the event of the two strips being completely identical for at least 5 letters, this passage would be likewise registered without inertia.

"The strips were to pass before the reading device at a speed of 10,000 symbols per second. Accordingly, not quite three hours would have been required to work through 10,000 letters. (10,000 x 10,000 = 100,000,000 comparisons.)

"It was also intended at first to record repeats that occurred thus, not yet how the passages read and exactly when (sic) they were ...."

The American rapid analytic machine most nearly comparable to the foregoing proposed device, is the "Tetragraph Tester," developed by Eastman Kodak Company

[142] D-60

[143] I-37

for OP-20-G, and manufactured for both OP-20-G and the Army Security Agency. This American device uses film; the speed past the film gate is 5,000 letters per second; and photocells ("readers working without inertia") are used.

It is unfortunate that more technical data are not available on the German device. Information concerning drive mechanisms, photocell operation, electronic counters, provision for accurate registration, and means to prevent film shrinkage while drying, all of which are of utmost importance in the building of any modern photo-electronic analytic machine, would be useful. Even the dark room procedures to be used would have been of extreme interest.

38. German Army and Foreign office experimented with rapid analytic machinery.--Dr. Buggisch gave an interesting comment on the ill-fated attempt of Inspectorate 7/VI (OKH/In 7/VI) to build rapid analytic machinery, to-wit:[144]

> "The limited width of the I.B.M. card was soon found to be inconvenient, particularly in counting out of repeats for the purpose of lining-up 2 cipher texts. The obvious solution appeared to be in this case to work with perforated strips and 5-unit alphabet. Orders were given at the beginning of '43 (?) for the construction of such a machine. As, however, Section VI only had a completely inadequate workshop at its disposal, and by that time it was already impossible to get any more tools, etc., an agreement was made with the Hollerith [I.B.M.] firm that a few rooms, together with workshop machines, tools, etc., in factory buildings at Lichterfelde Ost should be placed at the disposal of Section VI. An engineer of the name of Schiessler of the Hollerith firm was placed in charge of this newly set-up workshop; he was dressed up as a technician(Lieutenant grade), and was given a special section of his own. He was, in my opinion, pretty unsuitable for solving the problems set and, anyway, as far as his specialist knowledge was concerned, not even remotely comparable to the undermentioned gentlemen of OKW/Chi. The repeat counting machine

[144] I-67

was ready in the autumn of '43 (or winter 43/44). It worked on a mechanical-electrical principle, the speed was not very high (I think a maximum of 40 pairs of letters a second), and there was somehow an 'idling period' (Leerlauf) which was very inconvenient. It is worth noting that, when this apparatus was completed, none of the specialist department doing practical cryptanalysis had any use for it, so that the question was justifiably raised why such an apparatus had been built at all. I do not think that it was ever used for practical tasks.

"In the winter of '43/44, the workshop began to be engaged on the construction of various mechanical aids, but they cannot be described as cryptanalytic machines. Thus, for example, a machine was made which automatically punched on Hollerith cards the Russian T/P traffic taken on perforated strips with 5-unit alphabet. Plans were made, too, in the spring of '44 for machines which were to perform certain calculation tasks such as arose during work on Hagelin Machines; but those were not cryptanalytic machines either, but special calculating machines. I do not know whether work was ever started on the construction of these machines -- the order was probably issued -- because I went to an entirely different department in June '44 and was given quite different tasks. In short, Ag N/NA had until June '44, and in all probability subsequently, no cryptanalytic machine which could be used for the practical solution of any codes or ciphers.

"Things were different at OKW/Chi. There was no I.B.M. department there (as far as I know), and perhaps for that very reason they felt, more than in Ag N/NA, the necessity of developing and constructing special devices..."

Dr. Buggisch stated later that the machines developed at the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) were very satisfactory, however.

At the Foreign Office Cryptanalytic Section (Pers ZS) the "Automaton" was successfully developed for mass

deciphering of American strip cipher messages. This was not properly a rapid analytic machine (though it used a statistical principle) but was actually a rapid deciphering machine. Dr. Rohrbach, of the Foreign Office Cryptanalytic Section (Pers Z S) gave the following information concerning it:[145]

> "As was to be foreseen at the outset, the total material [American State Department messages sent in the strip cipher "C-2"] could not be deciphered by hand on account of its immense size. The number of available qualified workers with sufficient knowledge of English was too small for that. Deciphering...through moving the strips by hand required 6 - 7 minutes on an average, so that the work...would have taken a whole year, provided that 4 collaborators had worked on it 8 hours daily. It was, therefore, of the utmost importance that the automaton should be available for the decipherment of the material at the time when all keys had been worked out. It is not possible to describe the machine more explicitly within the scope of this report, but we should like to say briefly the following about the method of its working:
>
> "The decipherment...consists of two operations: (1) arranging the strips so that the cipher text letters are made to lie in a row, (2) selecting the line containing the true reading out of 25 parallel lines. The adjustment of the strips that move up and down, so that the true reading can be read horizontally, is accomplished by the machine quite automatically, as the cipher text is touched by hand on the keyboard of a typewriter, or taken by means of a sensing device from the I.B.M. cards that had already been punched. Finding the true reading is simplified by the fact that...the most frequent letters in the English language (about 80% of true reading) are printed in a heavy tone, the others in a light tone. A line consisting of 15 letters chosen at random would contain 6 bold ones on an average, while the true reading line of 15 letters with 12 bold ones on an average stands out distinctly...The 30 strips necessary for the decipherment of a double line are arranged side by side in two groups of 15 each for the line;

[145] I-89

if the left-hand group is in the first movement, the right-hand one is in the second movement and vice versa. During the time when the clerk copies the true reading from the indicated line on the typewriter, the machine prepares automatically the adjustment of strips for the next line and performs it at the touch of a key. In this way the decipherment of a double line requires barely half a minute on average. By means of this machine the total material could be deciphered within a month."

Volume 2

Chapter VII. German Cryptanalytic Methods

35. German cryptanalysis was generally against "medium grade" systems.--Germany's cryptanalytic successes were in what might be termed "medium grade" or "medium security" systems.[149] These systems consisted for the most part of codes, either enciphered or unenciphered, the solving of some of which required perserverance, intelligence, and linquistic ability, but certainly very little of what might be called "higher cryptanalysis." And in their solution of these relatively easier systems, they developed no important cryptanalytic methods not already used by the Anglo-Americans.

[149] See Chart No. 1-2, Vol. 1 of this report.

In higher cryptanalysis, and especially in the field of high-grade machine ciphers, the record of what German cryptanalysts did not accomplish is a long one. Although they were successful with the Japanese "red" machine, they did not solve its successor, the "purple" machine. They did not solve the United States Army Converter M-134c (SIGABA), Converter M-228 (SIGCUM), the Teleprinter Cipher System using double-tapes (SIGIBS) nor, of course, its successor, the One-time Tape System (SIGTOT), nor the United States Navy equivalents thereof, nor the joint Army-Navy-British Combined Cipher Machine (CCM). If they were even aware of the existence of the Anglo-American highsecurity ciphony system (SIGSALY) is very doubtful, as not a single reference to it is to be found in any TICOM document. They did not solve the British Typex machine. They apparently did not read traffic sent in the Russian B-211, nor the French modified B-211. In their security studies they certainly did not develop and probably were not aware of practical methods of solving their own plugboard Enigma, or their teleprinter cipher attachments.

It cannot be said that this failing was necessarily due to inability or ignorance. Perhaps, Japan being Germany's ally, Germany felt it was not worth while to expend the great energy necessary to solve the difficult Japanese "purple" machine.[150]

[150]The German cryptanalytic failure in the case of this machine and the fact that this failure probably led higher authority to conclude that the machine was secure against cryptanalysis had immeasurably disastrous consequences upon the German war effort. Since the machine was regarded as secure, very important information was constantly being given Japanese representatives in Europe without reservation, and this information was promptly forwarded to Tokyo by the Japanese, using the machine. Thus, from approximately February 1941, when the United States gave the British the solution to the "purple" system, until the very end of the war in both hemispheres, Anglo-American intelligence had the benefit of authentic, accurate, and timely information about conditions within Germany and the occupied countries, German intentions, results of bombing, war potential, etc. This fact was the central fact in the reluctance of the American high command to have any public investigation and disclosure of the secret facts and events preceding the Japanese attack on Pearl Harbor.

Perhaps German inability to read Anglo-American high-grade systems should be credited to our successful cryptography rather than to their cryptanalytic incompetence, for certainly our security studies showed these systems to be secure. Had these studies proved otherwise the systems would either have been modified or discarded. But in order to make valid studies of cryptographic security there must be cryptanalytic competence; and had the Germans been competent in this respect they would have realized the extent and significance of their cryptographic insecurity. However, this, too, must be added: as regard the German security studies on the German plugboard Enigma, which revealed to them no practical method of solving it, who can say that either British or American cryptanalysts would have thought of the "bombe" as a practical answer, if Polish cryptanalysts had not invented or devised the first crude apparatus from which the final "bombe" was developed?

Whether the Germans deserve praise or censure, the fact remains that their cryptanalytic methods had no very bright highlights. Their ciphony breaking was not advanced. Enciphered teleprinter messages were solved only by finding "depths" and processing them by long known procedures. Only the easiest (commercial type) Enigma was solved in actual attempts to solve enemy traffic. Solutions of messages enciphered by Hagelin machines of the M-209 type were accomplished only where messages in depth were found as a precondition. Additively superenciphered codes were solved the way additive codes usually are solved in America, but the U. S. Army and the U. S. Navy highly specialized machinery, specifically designed for the purpose of expediting the processing of Japanese military, naval, and air secret communications (all superenciphered codes) had no counterparts in German cryptanalytic organizations.

The cryptanalytic highlights, such as they are, are discussed in the paragraphs to follow, in order to make them a matter of record.

36. Washington-London commercial radiotelephone network conversations were solved by analysis of Spectrograms.-- Conversations over the commercial radiotelephone circuits between London and Washington were monitored, solved, and recorded by the German Post Office Research Laboratories in Eindthoven, Holland, and also by the press monitoring group (Gruppe VI) of

the Signal Intelligence Agency of the Supreme Command, Armed Forces (OKW/Chi) located at Ludwigsfelde, about 25 miles south of Berlin.[151] Some of the participants in these conversations are worth noting: Prime Minister Churchill and Anthony Eden when the latter was in Washington; the Minister of War Transport, and his representative; the same Minister and the British Shipping Mission; the Foreign Office and the British Embassy; the Dutch government representatives in both cities; the Russian embassies; the United States Embassy and the State Department. These radiotelephone circuits were enciphered by a "frequency scrambling" principle, according to Mr. K. Vetterlein, of the German Post Office.[152] The speech frequencies 450 cycles wide and the small blocks were rearranged in positions within the speech frequency spectrum, to give the finally enciphered speech.

Simple frequency scrambling of speech can usually be solved by examining the spectrographic records of the enciphered speech, cutting out the "blocks" of frequencies with scissors, rearranging them by sight into proper order, and pasting them back together. This reveals the "pattern" or key used. Simpler yet, if the scrambling pattern has a sufficiently long duration, the rearranging can be done electrically, with the ear for a guide. On the Washington-London commercial radiotelephone circuit, scrambling and recombining of frequencies was by a pattern that remained fixed for 20 seconds, and then changed into another such pattern. There were only 36 such patterns in all, and then the whole procedure repeated. Thus the grand cycle was twelve minutes. The German Post Office had no apparent difficulty in solving this system. They built a five-bank rotary switch with 36 positions, drove it with a synchronous motor so as to step every 20 seconds, repeating every 12 minutes, and controlled this operation accurately over 24 hour periods with a quartz-crystal-controlled oscillator. Once the German engineer wired this switch correctly to match the patterns, they were able to monitor transmissions 100% and receive the speech instantaneously in the clear, so that they could record the

[151] I 84, I 88, I 118, I 190

[152] I 88 p 2

* FREQUENCY SPECTRUM WAS BROKEN INTO FIVE SMALL BLOCKS OF

speech traffic magnetically on steel tapes. The pattern cycle was rearranged by the American Telephone and Telegraph Company (that is, the enciphering keys changed) only several times between April 1942 and April 1945; after each change it took German Post Office engineers "only a few hours" to reconstruct the new patterns and their sequence.[153] Oscillographs, spectrographs, magnetophone recorders, and quartz-crystal oscillators for time control were available for this work, but well trained ears were said to have played the most important role in the solution. While this commercial ciphony system was known to be insecure by the United States and British authorities, and therefore secret matters were normally kept in other channels, it is nevertheless important to our cryptographers and engineers alike to know that the Germans did solve it. Their total ignorance of even the existence of SIGSALY transmissions has already been mentioned.

37. Early Russian ciphony was solved by analysis of spectrograms.--Radio telephone conversations between Moscow, Leningrad, Irkutsk, Alma Ata, and Tscheljabinks, involving Russian Army and People's Commisariats, up until 1943, were enciphered by two simple methods which were said to be easily solvable by German engineers at the Army Ordnance, Development and Testing Group, Signal Branch (Wa Pruef 7), according to Corporal Karrenberg, of the Signal Intelligence Agency of the Army High Command (OKH/G d NA).[154] These two methods of Russian enciphering were:

a. Inversion, employing superimposed modulation of several audio frequencies; and,
b. Distortion, by artificial raising of amplitudes of speech harmonics.

German scientists were able to solve these two simple enciphering methods by recording the enciphered speech, making spectrograms from the recordings, and analyzing them. Evidently the voice engineers could see the results of the inversion and distortion, on careful inspection, and could readily identify the frequencies and methods used for encipherment. They tried it only a few times, according to Karrenberg, but were successful at will. At the beginning of 1944, however, the

[153] I 88 p 2

[154] I 173 p 18

simple enciphering methods were dropped by the Russians, radio telephone traffic networks themselves were changed, and no further entry was gained by the Germans.

Dr. Buggisch of the Signal Intelligence Agency of the Supreme Command, Armed Forces (OKW/Chi) studied spectrograms of this later unsolved Moscow-Madrid radiophone traffic at the Army Ordnance, Development and Testing Group, Signal Branch Laboratories (Wa Pruef 7) where he became convinced that Russian ciphony then involved time scrambling, with the length of the individual time segments being 10 milliseconds each, and a synchronizing pulse occurring every .6 second.[155] The number of "pickup heads" used by the Russians to obtain this time scrambling was reported in one interrogation to be three[156] and in another to be four.[157] German engineers were unable to learn any more than this from the spectrograms. They could reconstruct fragments of speech, they thought, but "the validity of the solution did not satisfy Dr. Huettenhain's critical sense," when shown to him.[158] Dr. Huettenhain, who consulted with Dr. Buggisch, believed that some form of one-time strip might have been used to key the time transposition, as he could find no period whatever in the encipherments.

38. Some Anglo-American teleprinter messages were read.--How much Anglo-American teleprinter traffic was read by the Germans is not too clear from the TICOM reports, but it is doubtful if they ever solved any teleprinter enciphering machines themselves.

a. Dr. Huettenhain denied that his agency, the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) did any work at all on the United States teleprinter traffic, although he admitted that the German Army Ordnance, Development and Testing group, Signal Branch (Wa Pruef 7) passed intercepts to his agency.[159]

[155] I 73

[156] I 73

[157] I 31

[158] I 31

[159] I 31, p 19

b. Dr. Voegele stated that from April to October 1944 his agency, the Signal Intelligence Agency of the Commander in Chief of the Air Force (Chi Stelle, Ob d L) intercepted plain-text American teleprinter messages which concerned aircraft movements between American and North Africa, but he mentioned no other non-Morse.[160]

c. Corporal Karrenberg stated that his agency, the Signal Intelligence Agency of the Army High Command (OKH/G d NA), had a section (Gruppe VI, Referate 2A) which "undertook preliminary evaluation of British and American wireless teleprinter and automatic Morse traffic," and another section (Gruppe VI, Referate 2 B) which "picked up the traffic evaluated in Referate 2A," [161] and that another section (Referate I B) charged with cryptanalysis of Russian secret teleprinters also "worked on British and United States (non-Morse) systems."[162] But he made no references to any actual reconstruction of American or British teleprinter cryptographic apparatus.

d. Russian teleprinter cryptographic apparatus may have been solved by Goering's "Research" Bureau in 1943, according to Dr. Buggisch of the Signal Intelligence Agency of the Army High Command (OKH/G d NA).[163] Dr. Buggisch knew no more details. Traffic was supposed to have stopped soon after, and the machine evidently went out of use. He reported that the Army did some work on a Russian teleprinter cryptographic machine, read a few depths, obtained about 1400 letters of pure key, but went no farther. Corporal Karrenberg, mentioned above, said that Russian enciphered teleprinter messages, when sent in depth, were read by anagramming, and the corresponding keying characters recovered, but the machine itself was not solved.[164] Russian teleprinter links of which he had any knowledge were from Moscow to the Russian armies, and there were about eight in all. Reading of the depths indicated the messages contained operational and reconnaissance information. Examination of the sections of key obtained from the readings in depth led Karrenberg to the conclusion that the Russian enciphering device was similar in construction to the German teleprinter cipher attachment SZ-42 with

[160] I 112 p 5

[161] IF 123 p 11

[162] I 149 p 2

[163] I 64 p 2

[164] I 169

a "motor" wheel or "motor" wheels arranged somehow to give a cycle of 43. None of his surmises was investigated to ascertain its validity, it being claimed that the traffic was too scanty to effect a solution.[165]

39. Swiss Enigma rotor wirings were solved by cribs; other Enigmas were compromised.--The Swiss diplomatic Enigma ("K" type) was read regularly, probably by the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi), although Dr. Huettenhain, who revealed this solution, did not state definitely that it was his agency which accomplished it. The Swiss changed their Enigma rotor wirings every three months, but the changes were not effected on the Berne-Washington link at the time they were made on the Berne-London link. As a result, duplicate messages sent by the Swiss to Washington and to London during the periods of changeover provided the "break" necessary to learn the new wirings.[166] The Croat enigma, used for both diplomatic and military traffic, was read regularly by Inspectorate 7/VI (IN 7/VI). This was no credit to the cryptanalysts involved, however, as their problem was particularly easy: (1) they had obtained the rotor wirings from Konski and Krueger (Berlin) who made the rotors; (2) there was no end-plate plugging involved; (3) the rotor orders were not changed by the Croats; (4) the "ringstellungen" (devices enabling the notches and alignment indicator letters to be "slid" in relation to the rotors) remained fixed; and (5) there were only 100 initial rotor alignments used by the Croats each month.[167]

An excellent treatise on Enigma ("K" type) solution was found in the files of the Foreign Office Cryptanalytic Section (Pers Z S). It involved obtaining many messages in depth, reading these messages by solving the successive (monoalphabetic) columns of superimposed text, and then applying the resultant cribs to recovering the wirings of the rotors. These methods are well-known to Anglo-American cryptanalysts.[168]

[165] I 169

[166] I 31

[167] I 84 p 3

[168] T 372

British Typex was the object of study by Dr. Buggisch, of the Signal Intelligence Agency of the Supreme Command, Armed Forces (OKW/Chi). He showed British Typex to be an Enigma type machine, by statistical study of 10,000 letters of cipher text, but was unable to go further.[169] No German cryptanalytic agency was able to solve it.

40. Traffic in Converter M-209 was solved only by depths.-- Traffic in U. S. Army Converter M 209, used by our field forces (including the Air Forces) and the U. S. Navy, was under study more or less constantly by the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) by the Signal Intelligence Agency of the Army High Command (OKH/G d NA), by the Signal Intelligence Agency of the Air Force High Command (OKL/Ln abt 350 and its predecessor Chi Stelle Ob d L), and by the Signal Intelligence Agency of the Navy High Command (OKM/4 SKL/III). Many theories were developed for statistical solution of M-209 messages, though none was successful. Solutions depended entirely upon reading messages in depth, recovery of key therefrom, then obtaining absolute settings, and reading the remaining messages in the same day's traffic. Items of interest throughout the TICOM reports concerning these solutions are as follows:

a. Dr. Huettenhain of the Signal Intelligence Agency of the Supreme Command, Armed Forces (OKW/Chi) stated that M-209 depths were found by using "Fasensuchgeraet," a rapid analytic machine, probably the "digraphic weight recorder" described in Chapter VI of this volume.[170]

b. Dr. Buggisch of the Signal Intelligence Agency of the Army High Command (OKH/G d NA) gave a statistical formula to be used with I.B.M. machines for aiding in finding M-209 pin patterns.[171] This consisted of writing the cipher text out "on the width" of one of the wheels, and applying a form of "phi" test to the resulting alphabets. Alphabets having distributions which showed the least randomness were supposed to be indicative of inactive pins. Dr. Buggisch did not state that he was ever able to make the test work, and it is believed at the Army Security Agency from long experience with similar tests that this particular one certainly would not have worked.

[169] I 66

[170] I 31

[171] I 137

c. Lt. Muentz, of the Signal Intelligence Agency of the Navy High Command (OKM/4 SKL/III) developed a statistical theory for solving Converter M-209 as used by the U. S. Navy, based on the frequent use of "Z" as a word separator.[172] This never worked on actual traffic.[173] Amtsrat Schultze, of the same Agency, developed a theory on how to guess plain text from a statistical study of the cipher text, but he was never able to make it work.[174]

41. B-211 machines were solved in theory only.--German successes with the French (modified) B-211 Hagelin and the Russian B-211 were practically non-existent. Dr. Huettenhain said a French (modified) B-211 was captured, and believed that an 8 to 10 letter crib could solve the wheel settings, pin settings, and pluggings, if the cipher wheel wirings were known. A Russian B-211 was also captured and a theoretical solution devised, but since no traffic was received this solution was never tested in practice.[175]

42. Additive super-enciphered codes were solved in the "usual" way.--No great new cryptanalytic methods were developed by German cryptanalysts to assist in solving additive super-enciphered codes. They were solved as such codes usually are: by superimposing identically-keyed texts (by virtue of identical indicators and by means of repetitions), removing the additive from the depths, and reconstructing, from the resultant relative code values, the basic code--unless the code book is already known.

a. An example of the foregoing type of solution by the Germans is noted in the case of their cryptanalysis of the British War Office Cypher, a 4-figure super-enciphered code used between Army, Corps, and Division, which was read during the campaign in North Africa in 1940.[176]

[172] I 50

[173] I 6

[174] I 147

[175] I 58

[176] I 51

b. Another example is the Turkish 4-figure diplomatic code enciphered by repeating additives,[177] which was solved without regard to indicators simply by superimposing sections of messages at the period of the additive (in this case a period of 20) thereby obtaining enough depth to eliminate the additives and reconstruct the code.[178]

c. The German Navy's solutions of British naval codes (including "British Naval Cypher No. 3") are perhaps the most completely described solutions of the foregoing type in TICOM publications.[179] These solutions extended from before 1939 to the end of the war. Before 20 August 1941, when the indicator groups were not super-enciphered, messages were lined up in depth by indicators, and additives were eliminated therefrom by the use of "difference tables" or by guessing stereotyped texts. Some of the codes themselves were solved by cryptanalytic reconstruction, and some were captured. When the Merchant Marine code indicator systems became difficult, in 1942, messages were lined up in depth by other methods. One such method was that colloquially called "brute force," that is, pairs of messages were sought wherein at least two code groups in one message, separated by a definite interval, coincided with at least two code groups in the other message, separated by the same interval. Such messages were likely to have been enciphered with the same sections of additive, especially if the interval was not over 10, according to the Germans. However, they considered "brute force" unreliable and used it as little as possible. Whenever sections of additive were already known, messages were set against these sections by a technique quite familiar to the Army Security Agency. This consisted of applying all of the individual additive groups of a known section to 15 or 20 of the usually most frequently occurring unenciphered code groups, and obtaining thereby a set of enciphered code groups most likely to occur in messages enciphered with the known additive section. If two or more such likely enciphered code groups occurred in a message, at an

[177] Army Security Agency trigraph, "TUK"

[178] I 103

[179] I 93, I 146, I 147

interval matching the interval between the groups of additive from which they were derived, then it was very likely that the rest of the message could be deciphered from that point on in the section of known additive. The ordinary cryptanalytic aids, such as difference tables (made by German cryptanalysts usually from the 300 highest-frequency code groups), known and frequently-used addresses, spelling groups, figure groups, and place names, as well as stereotyped texts, aided them in aligning messages and eliminating additives. By such means, depths of only two were often read-- in fact, if the two messages were routine reports, "they were read without exception."[180]

When the British Navy introduced the "S.S. Frame" in December 1943,[181] German cryptanalysts were able to analyze correctly the new cryptographic system being employed, and were able to read messages superenciphered in this new system for one month. The German cryptanalysts were able to superimpose a few messages in depth, which permitted them to recover several sequences of additive; they discovered that parts of one sequence of additive at times overlapped parts of other sequences, albeit out-of-phase and very irregularly; by using this knowledge to test new assumptions, and after much trial and error, they were able to recover and reconstruct a complete set of number tables; they also solved the weak December 1943 indicator system, which relied only on random co-ordinates to indicate the stencil position; and as a result of these activities they obtained a fair understanding of the British "S.S. Frame". They complained:[182]

[180] I 93 p 2

[181] In one type of Stencil Subtractor Frame, a stencil of 100 irregularly located apertures, each aperture 4-digits wide, is placed on a card of randomly chosen numbers, 48 by 68 digits in size, at any one of 100 settings determined by a specific key, and the 4-digit groups that appear in the apertures of the stencil provide additive. Parts of additive obtained at any one setting of the stencil will not properly "overlap" additive obtained at another adjacent setting, because of the irregular spacing of the stencil apertures. Thus satisfactory depths that can be found in such a system are obtained only from identically keyed messages.

[182] I 93 p 25

"We discovered that we had formerly had on the long subtractor system 1,500 starting points over a 10 day period; whereas we now had 10,000 different starting points on one daily table."

On 1 January 1944 the British changed their basic codes as well, and soon thereafter began to use "doubly enciphered indicators" for the "S. S. Frame". The Germans, with almost no depths possible, and with the basic code book unknown to them, could no longer read the traffic. Senior Specialist Tranow, of the Signal Intelligence Agency of the Navy High Command (OKM/4 SKL/III) stated:[183]

"We came to the conclusion that we could not recover a system of this kind within six months, without having the basic book. However it was clear to us that if we were able to capture the book, we should then be able to break this system in a very short time. We provided our own proof for this.... We constructed synthetic messages of our own on the pattern of the British originals. We began the first trial with 200 messages a day and broke all of them within three weeks.... We then carried out a second trial with 100 messages. The staff was much more practiced and succeeded with a smaller number of messages in a shorter time."

So far as is known, however, they did not "capture the book" or continue solving the system.

d. The Polish government in London used an additive superenciphered code for Military Attaché messages, which was read regularly by the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) until about 1943 when the Poles changed their methods of obtaining the additives. The Poles had introduced their version of the British "S.S. Frame," at the suggestion of the British Government; their stencils had from 28 to 40 randomly placed apertures, rather than 100 as in the British version. The German cryptanalysts, having the Polish code book from their previous solutions, were able, with it and with depths obtained by I.B.M. searches for repeats, to reconstruct additives, discover the irregular positions of the stencil apertures, and reconstruct the stencils, and read the messages.[184]

[183] I 93 p 25. Even with the indicators amply enciphered, much headway was made by German cryptanalysts in recovering relative starting points. See D 25.

[184] I 118, I 31

43. Mihajlovic double-transpositions were solved by anagramming.--Yugoslavian double-transpositions (Draza Mihajlovic traffic) were solved by Corporal Herzfeld of Inspectorate 7/VI (In 7/VI), in from one to three days.[185] In each message, the same key was used for the two transposition matrices, and the matrices were usually incompletely filled. The width of the transposition matrices were assumed by Corporal Herzfeld each time"with some degree of accuracy," based on his previous experience with messages of the same length and on the same networks. This was of course a great advantage, since it permitted a marking off in the cipher text of the approximate columns of the second transposition matrix. The words "GENERAL DRAZA MIHAJLOVIC" which nearly always appeared as a signature, made an excellent crib because several of the letters were infrequent, and because these words could be written in as the final rows of the first transposition matrix. With the dimensions of the matrices chosen by good guessing, and with both the complete columns of the second transposition matrix and the final rows of the first transposition matrix delineated, the German corporal then tried to match elements of his cipher text with elements of his crib, and by anagramming recover plain text and the key. The methods used were not unusual.

44. Solutions of American Strip ciphers involved statistical analysis.-- Cryptanalytic successes against American strip ciphers were obtained by at least three German agencies. Dr. Rohrbach, cryptanalyst of the Foreign Office Cryptanalytic Section (Pers Z S), who claimed that his group of six cryptanalysts solved the United States State Department strip cipher ("0-2") in 1943 without any previous knowledge concerning the general system, required over a year for solution. The State Department strip cipher "0-2" which he solved did not employ strip elimination, but it did make use of the principle of "split generatrices"--that is, 30 strips were chosen out of a possible 50 strips each day and arranged in a channel board according to the daily key, and messages were then enciphered by successively setting up 30 letters of plain text across one line of the strips, each time reading off 15 letters of resultant cipher text from the first half of another line, chosen at random,

[185] I 69 p 23; I 52

and the remaining 15 letters of cipher-text from the last half of a third line, chosen at random. Dr. Rohrbach's methods of solution were recorded in a detailed paper written by him at the request of TICOM interrogators,[186] and they were similar to the statistical methods suggested as a general solution by United States Army cryptanalysts in 1934. Messages were punched on I.B.M. cards, repeats were found which indicated that intervals of 15 and 30 were significant, the material was sorted into "families" (Dr. Rohrbach defined a "family" as a collection of homogeneous cipher material based on use of the same generatrix in the enciphering process) and the larger "families" were solved, as similarly-keyed polyalphabetic cipher sequences, by analyzing the material "column by column." The alphabets recovered permitted reconstruction of many of the strips, and with their aid the remaining "families" and strips were solved. Although Dr. Rohrbach indicated in his writing that he had had no previous knowledge of the general system when he started his solution activities in November 1942, it is a fact that the Foreign Office Cryptanalytic Section (Pers Z S) had received photographic copies in 1941 from the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) of a set of instructions for an earlier American strip cipher ("0-1") and "4 series of strips by means of which a number of messages could be deciphered."[187] Files of the Foreign Office Cryptanalytic Section (Pers ZS) captured in 1945 also contained photographs of two Tables of Numerical Keys for the same earlier State Department strip cipher ("0-1"). The advance knowledge of the general system given by this compromise, and the stereotyped beginnings that Dr. Rohrbach indicated in his paper were present in State Department traffic ("0-2") (such as "Strictly confidential from Murphy.... ") together with the State Department's reuse of each daily key an average of 9 times throughout the year (only 40 different strip arrangements were provided for 365 days traffic) should have made the solution much easier for Dr. Rohrbach than he found it.

[186] I 89

[187] DF 15 p 5.

Dr. Huettenhain of the Signal Intelligence Agency of the Supreme Command, Armed Forces (OKW/Chi) stated that his agency worked on American diplomatic strip systems, and that they were not aided in their work by any captures, but succeeded through cryptanalysis only.[188] This statement is also at variance with the record, already mentioned, of compromised strips being handed over from the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) to the Foreign Office Cryptanalytic Section (Pers Z S). The techniques used by Dr. Huettenhain are not recorded, but his Agency considered American strip ciphers of sufficient importance to build a special rapid analytic machine (the "statistical depth-increaser") for facilitating statistical solutions.[189]

According to Dr. Ferdinand Voegele, Chief Section B, of the Signal Intelligence Agency of the Air Force High Command (OKL/LN abt 350), a strip cipher of the United States Army Air Force South Atlantic Ferry Command was solved before 1943. He wrote:[190]

> It was quite evident from the cipher text that there was a break after each 15 letters.... Accordingly an analysis was made on the basis of groups of 15 letters with the assistance of I. B. M. machines. A depth of 80 passages of parallel construction was needed to reconstruct the 100 strips, 30 of which were valid in any one day.... The system was read as long as it was used.
>
> "In 1943 a new difficulty presented itself. While 30 strips were still valid on any one day, the encipherer could arbitrarily remove any five of the strips to encipher any one message... . After about six weeks, some of these messages were also deciphered. However, at the same time the volume of this type of traffic began to decline, so that finally the analysis work had to be discontinued."

Techniques employed by Voegele and his assistants are not known. Decipherment "after about six weeks" of some of the later messages, when strip elimination was employed, may have been accomplished by the skilful use of cribs. It is interesting to note that soon after strip elimination had been introduced, "the analysis work had to be discontinued."

[188] I 84

[189] See Chapter VI of this volume. It will be recalled that another device, the "automaton", was also developed by the Foreign Office Cryptanalytic Section (Pers Z S) for rapid deciphering of a large backlog of strip traffic.

[190] IF 175 p 15.

Major Dr. Rudolph Henze, head of the cryptanalysis group of the Signal Intelligence Agency of the Army High Command (OKH/G d NA) reported solution of an American "strip" cipher the intelligence of which was "mixed military and diplomatic," and which, from the description of the system, and its indicators, was actually enciphered by Army cipher device Type M-94 rather than by any of the strip cipher devices.[191]

This was technically not a mistake in terminology by Dr. Henze, since the aluminum disks of the M-94 may be considered to be strips from a cryptanalytic viewpoint.[192] A soldier, Werner K. H. Graupe (rank unknown) reported that he cryptanalyzed an American "strip" cipher (actually the M-94) carrying Iceland and Carribean area traffic, while he was presumably in Inspectorate 7/VI (In 7/VI) in Berlin.[193] He used cribs, with the help of synoptic tables, to determine the "strip" (disk) orders, and stated that he later believed I. B. M. methods were developed to eliminate impossible keys. According to the interrogator, Graupe "knew of what he called a 30-strip system, but stated very definitely that it had never been solved." Lt. Col. Mettig, who was the commanding officer of Inspectorate 7/VI (In 7/VI) from November 1941 through June 1943, stated[194] "..it was eventually recognized that the main cipher procedure used by the Americans was the strip method whereby 25 variously arranged alphabets were vertically laid out one alongside the other. In the workshop of In 7/VI mechanical aids were constructed and with the help of the I. B. M. section and by noting the addresses and signatures, the various alphabets were recreated."

[191] I 113

[192] Dr. Voegele, the Air Force cryptanalyst, considered North Atlantic Air Force M-94 traffic as being "strip." See I-112.

[193] IF-107. Inspectorate 7/VI was a predecessor of the Signal Intelligence Agency of the Army High Command (OKH/G d NA).

[194] I 78 p 10

To summarize: German cryptanalysis of both the strip cipher and the M-94 apparently developed no exceptional methods, although it did result in the construction of two special rapid cryptanalytic machines, the "statistical depth-increaser" and the "automaton," described in chapter VI.

45. Conclusion.--German cryptanalysis was very successful on low grade systems, not only because the German cryptanalysts were sufficiently skilled to take advantage of the presence of low security traffic, but also because of the failure on the part of Anglo-American commanders to realize the extent to which the Germans were able to go in taking advantage of insecure practices.

German medium-grade cryptanalysis was extensive and worthwhile, as can be seen from the Cryptanalytic Successes chart, Chart No. 1-2, Volume 1 of this report; but no outstandingly different or unusual cryptanalytic methods were developed by the Germans in their medium grade solutions.

German cryptanalysis was not outstandingly successful against systems of high-security. This may have been not only because Anglo-American high-security systems were actually of high-security, and were to some extent insolvable to Anglo-American cryptanalysts as well, but also because the German cryptanalysts never became technically proficient enough to undertake even the solution of the less difficult of the high-security systems.

TAB A

Volume 2

Tab A

General Information and References

Abwehr - See "Military Intelligence."

Army Ordnance, Development and Testing Group, Signal Branch (Wa Pruef 7). This organization developed, engineered and tested Signal Corps equipment. It also did some non-morse interception. It is described in Volume 8 of this paper.

A.E.G., Berlin. ("Allgemeine Elektrische Gesellschaft"). German commercial firm which worked on speech encipherment.

Air Force Weather Service (Wetterdienst der Luftwaffe). This service was charged with cryptanalysis of enemy meteorological ciphers.

Allgemeine Elektrische Gesellschaft. German Commercial firm which worked on speech encipherment.

Buggisch, Staff Sgt. Dr. Otto. Cryptanalyst of Inspectorate 7/VI (In 7/VI). Expert on German cryptographic apparatus, and on ciphony matters.

D-25. "S.S. Frame Indicator System." A TICOM publication.

D-51. "Translation of Miscellaneous Documents from Pers Z S Archives." A TICOM publication.

D-57. "Notes and Minutes of High-Level Mettings held at OKW/Chi-- Cryptographic and Administrative." A TICOM publication.

D-58. "Description of Facsimile Intercept Recorder." A TICOM publication.

D-59. "Notes on Cipher Security and Minutes of Meetings held at OKW/Chi." A TICOM publication.

D-60. "Miscellaneous Papers from a File of RR Dr. Huettenhain of OKW/Chi." A TICOM publication.

Deutsche Telefon und Kabelwerke, Berlin. German Commercial firm which worked on speech encipherment.

DF-15. TF 20 "A Group" Reports (American Systems).

E-9. "Detailed Feuerstein Technical Project Report Ref. No. 2 Little Baustein." A TICOM publication.

E-10. "Detailed Feuerstein Technical Project Report. Ref. No. 3: Artificial Speech and Encoding." A TICOM publication.

E-11. "Detailed Feuerstein Technical Project Report, Ref. No. 4: Three-Fold Wobbulation and Mechanical Wobbulator Generators." A TICOM publication.

E-13. "Detailed Feuerstein Technical Project Report Ref. No. 6: Synchronous cipher system for teletype-writers--Gleichlauf." A TICOM publication.

E-14. "Detailed Feuerstein Technical Project Report, Ref. No. 7: Investigation of SZ Cipher Machines at Feuerstein Laboratory." A TICOM publication.

FA. See: Goering's "Research" Bureau.

Fabrik C. Lorenz Aktiengesellschaft, Berlin, Muelhausen, Thuer. Firm which worked on speech encipherment and developed teleprinter enciphering devices.

Fess, Dr. ..... Member of Wanderer Co.

Feuerstein Laboratory .... Electronic research laboratory owned and managed by a Dr. Oskar Vierling. This is described in Volume 8 of this paper.

Fricke, Dr. Walter, Technician, grade of Lieutenant. Head of Section IIb of the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi). Specialized in the production of codes and ciphers.

Foreign Office, Cryptanalytic Section (Pers Z S) and Foreign Office Cryptographic Section (Pers Z Chi). These made up one of the six principal German cryptologic organizations. These are described in Volumes 1 and 6 of this paper.

Frowein, Lt. R. Hans-Joachim. Assigned temporarily to the Signal Security Agency of the Navy High Command (OKM/4 SKL/II) in 1944 to make security studies on the Enigma. He had no previous experience with this machine and yet developed a workable solution.

German Weather Bureau (Reichswetterdienst). This service was charged with cryptanalysis of enemy meteorological ciphers. It was part of the German Air Force, and maintained close liaison with the Signal Intelligence Agency of the Commander in Chief of the Air Force (Chi-Stelle, Ob d L).

Goering's Research Bureau (Reichsluftfahrtministerium Forschungsamt, abbreviated FA). This was one of the six principal German cryptologic organizations, and is described in Volumes 1 and 7 of this paper.

Heimsoeth & Rinke. German firm engaged in manufacture of Enigma rotors and parts.

Herzfeld, Corporal Heintz Wolfgang. Member of Gruppe IV, Signal Intelligence Agency of Army High Command (OKH/GdNA); formerly member of British, Italian, and Balkan sections of Inspectorate 7/VI (In 7/VI).

Huettenhain, Specialist Dr. Erich. Principal cryptanalyst of the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) from 1939 to end of war.

I-1. "Report of TICOM Reporting Team No. 3. A TICOM publication.

I-6. "Interrogation of Lt. D.R. Muentz of the OKM 4/III." A TICOM publication.

I-20. "Interrogation of Sonderfuehrer Dr. Fricke of the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi)." A TICOM publication.

I-31. "Detailed Interrogations of Dr. Huettenhain, Formerly Head of Research Section of OKW/Chi, 18th-21st June 1945." A TICOM publication.

I-37. "Translation of Paper Written by Reg. Rat. Dr. Huettenhain of OKW/Chi on Special Apparatus Used as Aids to Cryptanalysis." A TICOM publication.

I-38. "Report on Interrogation of Lt. Frowein of OKM/4 SKL/III, on His Work on the Security of the German Naval Four-wheel Enigma." A TICOM publication.

I-45. "OKW/Chi Cryptanalytic Research on Enigma, Hagelin, and Cipher Teleprinter Machines." A TICOM publication.

I-47. "P/W Situation Report." A TICOM publication.

I-50. "Paper Written by Lt. Muentz of OKM/4 SKL/III on Statistical Solution of the M-209 Hagelin Machine." A TICOM publication.

I-51. "Interrogation Report on Uffz. Herzfeld, Heintz Worfgang, and Translation of a Paper He Wrote on the British War Office Code." A TICOM publication.

I-52. "Papers Written by Uffz. Herzfeld on Mihailovic and Tito Ciphers." A TICOM publication.

I-53. "Construction of Schluesselgeraet 39." A TICOM publication.

I-57. "Enciphering Devices Worked on by Dr. Liebknecht at Wa Pruef 7." A TICOM publication.

I-58. "Interrogation of Dr. Otto Buggisch of OKW/Chi." A TICOM publication.

I-64. "Answers by Wm. Buggisch of OKH/Chi to Questions sent by TICOM." A TICOM publication.

I-66. "Paper by Dr. Otto Buggisch of OKH/In 7/VI and OKW/Chi on Typex." A TICOM publication.

I-67. "Paper by Dr. Otto Buggisch of OKH/In 7/VI and OKW/Chi on Cryptanalytic Machines." A TICOM publication.

I-69. "Summary of Cipher Information on Jugoslav Traffic Provided byUffz. Herzfeld (Appendices to TICOM/ I-52)" A TICOM publication.

I-72. "First Part of the Report by Wm. Buggisch on S.G. 41." A TICOM publication.

I-73. "Translated Version of Homework done by Wm. Buggisch." A TICOM publication.

I-77. "Translations of Joint Report made by Drs. Huettenhain and Fricke on the "Zaehlwerk" Enigma Machine." A TICOM publication.

I-78. "Interrogation of Oberstlt. Mettig on the History and Achievements of OKH/AHA/In 7/VI." A TICOM publication.

I-80. "P.O.W. Interrogation Report--Obgefr. Clement Schaack Insp. VII/6 (OKH)." A TICOM publication.

I-84. "Further Interrogation of R.R. Dr. Huettenhain and Stf. Dr. Fricke of OKW/Chi." A TICOM publication.

I-88. "Report on Interrogation of ME. K. Vetterlein of the Reichspost Laboratorium on German Interception of Transatlantic Speech Circuits." A TICOM publication.

I-89. "Report by Prof. Dr. H. Rohrbach of Pers Z S on American Strip Cipher." A TICOM publication.

I-92. "Final Interrogation of the Wachtmeister Otto Buggisch (OKH/In 7/VI and OKW/Chi)" A TICOM publication.

I-93. "Detailed Interrogation of Members of OKM/4 SKL/III At Flensburg." A TICOM publication.

I-96. "Interrogation of Oberstlt. Mettig on the Organisation and Activities of OKW/Chi." A TICOM publication.

I-103. "Second Interrogation of Reg. Rat Hermann Scherschmidt of Pers Z S Auswaertiges Amt. on Turkish and Bulgarian Systems." A TICOM publication.

I-104. "Report on Berlin Targets by Major Heller of G.S.I.(S) 21 A.G., B.A.O.R." A TICOM publication.

I-112. "Preliminary Interrogation of Reg. Rat. Dr. Ferdinand Voegele (Chi Stelle, Ob d. L) and Major Ferdinand Feichtner (O.C. of LN Regt. 352, Etc.)" A TICOM publication.

I-113. "Interrogation of Major Dr. Rudolph Hentze, Head of Gruppe IV (Cryptanalysis), General der Nachrichtenaufklaerung." A TICOM publication.

I-118. "Joint Reports by Reg. Rat. Dr. Huettenhain and Sdf. Dr. Fricke, Written at C.S.D.I.C. on or about 28th August 1945." A TICOM publication.

I-119. "Further Interrogation of Reg. Rat. Voegele and Major Feichtner on G.A.F. Sigint." A TICOM publication.

I-127. "Interrogation of Oberstlt. Mettig of OKW/Chi." A TICOM publication.

I-137. "Final Report Written by Wachtmeister Otto Buggisch of OKH/Chi and OKW/Chi." A TICOM publication.

I-146. "Detailed Interrogation of Members of OKM/4 SKL/III At Flensburg." A TICOM publication.

I-147. "Detailed Interrogation of Members of OKM/4 SKL/III At Flensburg." A TICOM publication.

I-149. "Report by Uffz. Karrenberg and Colleagues on Allied Cypher Machines." A TICOM publication.

I-152. "Second Homework and Report on Further Interrogation of RR Voegele." A TICOM publication.

I-169. "Report by Uffz. Karrenberg on the Bandwurm." A TICOM publication.

I-173. "Report by the Karrenberg Party on Russian W/T." A TICOM publication.

I-190. "Extracts from Report on Interrogation of Dr. Hans Wilhelm Thost." A TICOM publication.

IF-107. "Interrogation of P.O.W. Werner Graupe by interrogators of Signal Intelligence Division, ETOUSA.

IF-123. "Consolidated Report on Information Obtained from the Following: Erdmann, Grubler, Hempel, Karrenberg, Schmitz, and Suschowk." A publication of the Combined Services Detailed Interrogation Centre, number CSDIC. (UK) SIR 1717.

IF-142. "Naval Cipher and W/T Procedures. Marineschluesseldienst und Marinefunkverfahren." A British Naval Intelligence Division publication, number TR/PG/17626/NID.

IF-175. Seabourne report, Volume XIII. "Cryptanalysis Within the Luftwaffe SIS." 24 November 1945.

IF-259. "Radar Most Decisive Weapon, Won Ocean Fight Says Doenitz." United Press Article in the Washington Post 10 May 1946.

In 7/VI. See Inspectorate 7/VI.

Inspectorate 7/VI (OKH/In 7/VI). Central Cryptanalytic Agency of The Army High Command for Non-Russian Traffic 1942-1943.

Jensen, Graduate Engineer. Member of Section IVb of the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) which dealt with the development of cryptanalytic machinery.

Karrenberg, Corporal Erich. Cryptanalyst of Signal Intelligence Agency of Army High Command (OKH/GdNA) who studied Baudot traffic.

Konski and Krueger, Berlin. Firm which manufactured rotors for the Enigma.

Krachel, ... Working engineer who came to Signal Intelligence Agency of the Supreme Command of the Armed Forces (OKW/Chi) in 1941 to help Rotscheidt and Jensen in research on cipher machines.

Kunze, Dr. Werner. Head of mathematical cryptographic subsection of Pers Z S.

Liebknecht, Graduate Engineer Dr. Werner. Chief of section IIIh of Army Ordnance, Development and Testing Group, Signal Branch (Wa Pruef 7). Maintained technical liaison with Dr. Huettenhain of the Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi).

M-11. Five drawings of the Lueckenfuellerwalze.

Martini, Lt. General Hermann. Chief Signal Officer, German Air Force.

Menzer, Senior Inspector. Chief of Section IIc of Signal Intelligence Agency of the Supreme Command of the Armed Forces (OKW/Chi) which dealt with the development and production of special ciphers for government departments, industry, and the Main Reich Security Office (RSHA), developing of deciphering aids for agents.

Mettig, Lt. Col. Head of Inspectorate 7/VI (In 7/VI) from Nov. 1941 to June 1943; second in command of Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) from Dec. 1943 to April 1945.

Military Intelligence (Abwehr). Military intelligence and counter espionage section of the Supreme Command of the Armed Forces (OKW). After 20 July 1944, this section was taken over by RSHA.

Muentz, Lt. ..... Member of the Signal Intelligence Agency of the Navy High Command (OKM/4 SKL/III) who worked on the Navy Hagelin Machine--M-209.

OKH/GdNA. See Signal Intelligence Agency of the Army High Command.

OKL/LN Abt 350. See Signal Intelligence Agency of the Air Force High Command.

OKW/Chi. See Signal Intelligence Agency of the Supreme Command Armed Forces.

OKM/4 SKL/II See Signal Security Agency of the Navy High Command.

OKM-4 SKL/III See Signal Intelligence Agency of the Navy High Command.

Pers Z Chi. See Foreign Office Cryptographic Section.
Pers Z S. See Foreign Office Cryptanalytic Section.
Pietsch, Specialist Dr. ..... Head of mathematical section of Inspectorate 7/VI (In 7/VI)
Rohrbach, Dr. Hans. Group head in Mathematical and cryptanalytic subsection (Kunze) of Foreign Office Cryptanalytic Section (Pers Z S). Also Math Professor at University of Prague.
Rotscheidt, Graduate Engineer. Appointed in 1941 to Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) for Research in offensive and defensive warfare in cipher machines. Telecommunication expert.
Reich Security Office. Reichssicherheitshauptamt, abbreviated RSHA.
Reichsluftfahrtministerium Forschungsamt. See Goering's "Research" Bureau.
Reichswetterdienst. See German Weather Bureau.
Schaeffer ..... Engineer who came to Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi) in 1941 to help Rotscheidt and Jensen in research on cipher machines.
Schmalz, Graduate Engineer. Head of Hollerith section of Signal Intelligence Agency of the Navy High Command (OKM/4 SKL/III).
Schuessler. Engineer of I.B.M. Firm in charge of section workshop at Erfurt (section 4 of Gruppe IV, GdNA)
Schuck, Corporal Clemens. Cryptanalyst of Inspectorate 7/VI who worked on SLIDEX and M-209.
Schultze, Amtsrat. Cryptographer of OKM/4 SKL/III. An expert on the Hagelin machine.
Security Group of the Signal Intelligence Service (OKH/Gen Nafue/III, Gruppe IV). This service did security studies on German Air Force traffic.
Siemens & Halske, Berlin. German commercial firm which worked on speech encipherment.
Signal Intelligence Agency of the Air Force High Command (OKL/LN Abt 350). This was one of the six principal German cryptologic organizations. This agency is described in Volume 5 of this paper.
Signal Intelligence Agency of the Army High Command (OKH/GdNA). This was one of the six principal German cryptologic organizations. It is described in Volume 4 of this paper.

Signal Intelligence Agency of the Supreme Command Armed Forces (OKW/Chi). This made up one of the six principal German cryptologic organizations. It is described in Volume 3 of this paper.

Signal Security Agency of the Navy High Command (OKM/4 SKL/II) and Signal Intelligence Agency of the Navy High Command (OKM/4 SKL/III). These made up one of the six principal German cryptologic organizations.

Sueddeutsche Apparate Fabriken, Berlin. German Commercial firm which worked on speech encipherment.

Stein, Lt. Dr. Head of the section of Gruppe IV of OKW/Chi which concerned itself with security investigations for new procedures and all investigations on inventions.

T-372. "The Enigma by Dr. Rudolf Kochendoerffer, from Scientific Writings of Foreign Office Cryptanalytic Section 8 Dec. 1941." A captured German document in possession of TICOM.

T-1282. A set of miscellaneous Foreign Office papers, in possession of TICOM.

Telefonbau U. Normalzeit Co., Frankfurt am Main. Firm which built test models of Cipher Device 39.

Telefunken, Berlin. German commercial firm which worked on speech encipherment.

Todt, ... Engineer who came to OKW/Chi in 1941 to help Rotscheidt and Jensen in research on cipher machines.

Tranow, Specialist ..... Head of English Cryptographic section in OKM-4 SKL/III.

Vetterlein, Mr. K. Supervised the monitoring service in Holland for trans-Atlantic monitoring of telephone conversations.

Vierling, Dr. Oskar. Specialized in communications equipment reaearch. Was owner and chief engineer of the Feuerstein Laboratory.

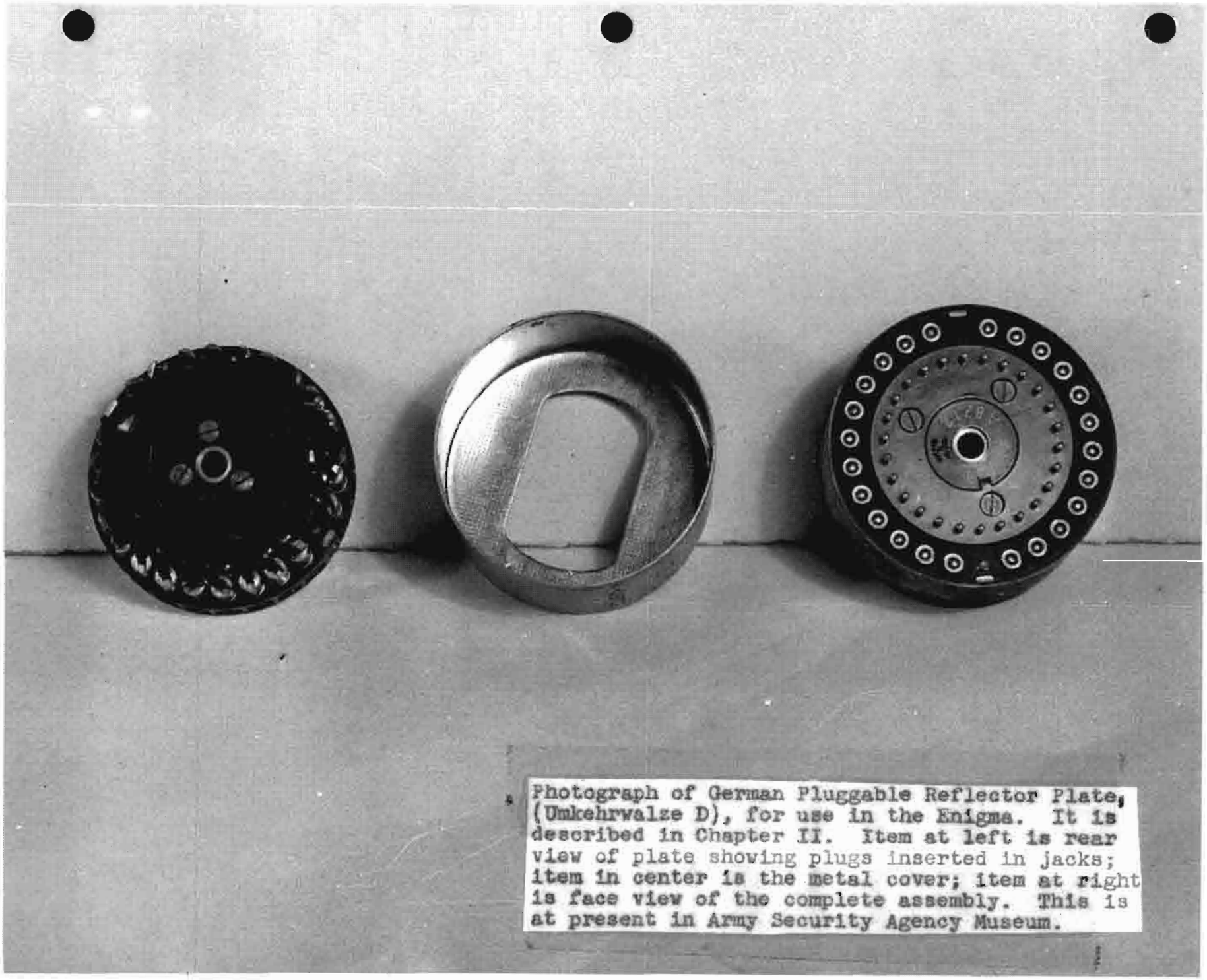
Voegele, Specialist Dr. Ferdinand. Chief of Section E of the Signal Intelligence Agency of the Commander in Chief of The Air Force (Chi-Stelle Ob d L) and principal cryptanalyst in the German Air Force.

Wa Pruef 7. See Army Ordnance, Development and Testing Group, Signal Branch.

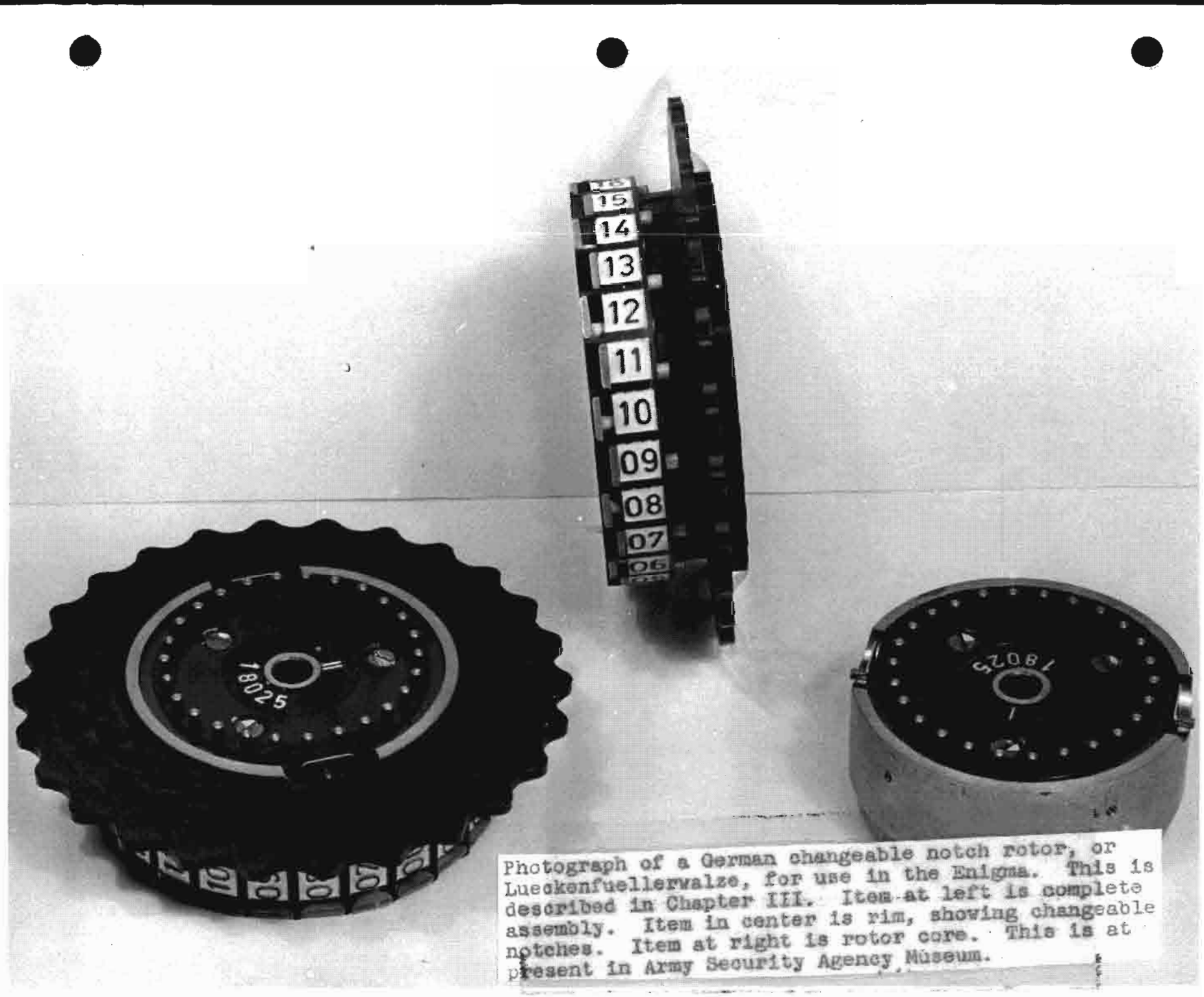
Wanderer Co. This firm was to have manufactured Cipher Device 39 on large scale production.

Wetterdienst der Luftwaffe. See Air Force Weather Service.

Photograph of German Plugboard Enigma, described in Chapter II, at present in Army Security Agency Museum.

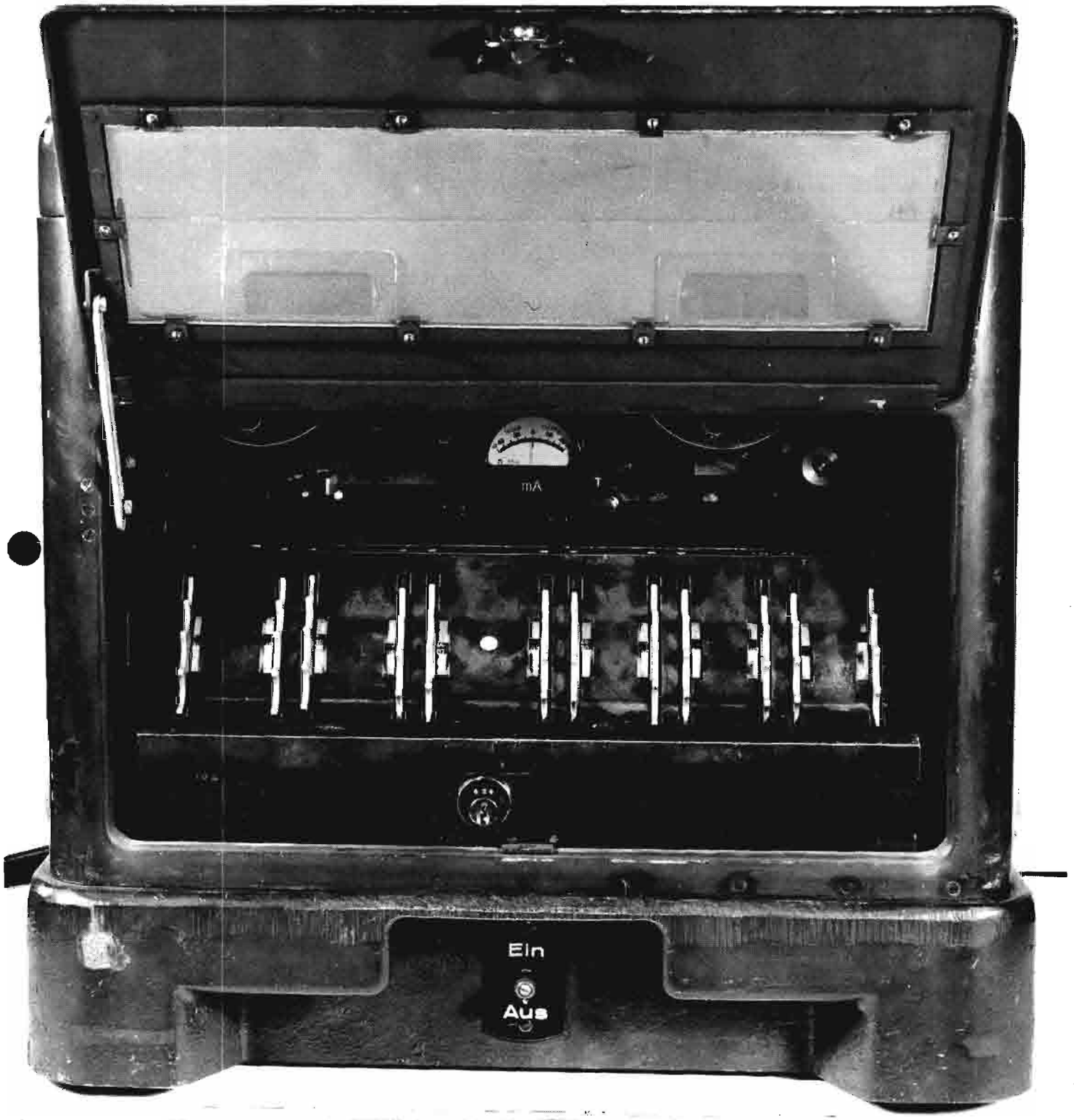


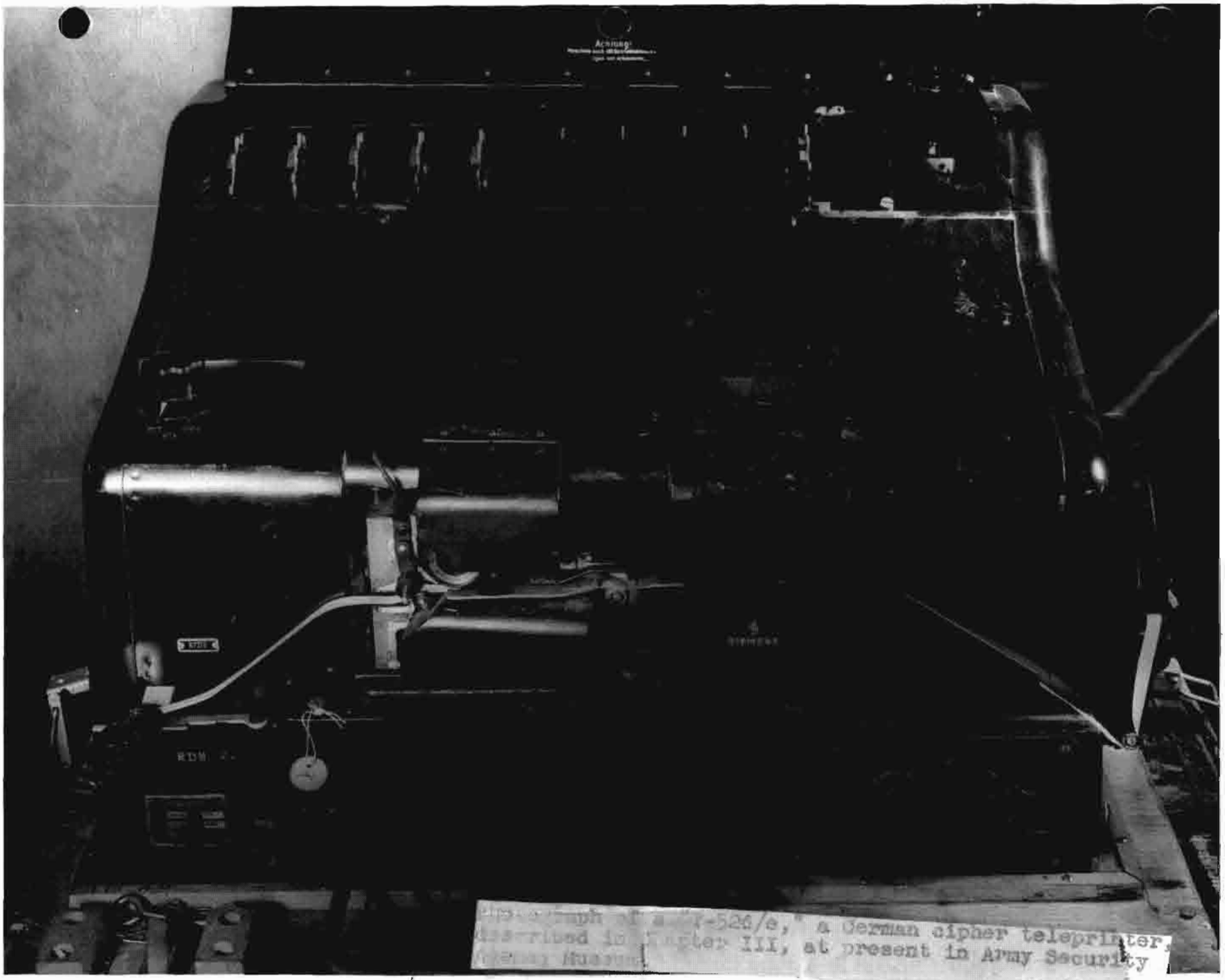
Photograph of German Pluggable Reflector Plate, (Umkehrwalze D), for use in the Enigma. It is described in Chapter II. Item at left is rear view of plate showing plugs inserted in jacks; item in center is the metal cover; item at right is face view of the complete assembly. This is at present in Army Security Agency Museum.



Photograph of a German changeable notch rotor, or Lueckenfuellerwalze, for use in the Enigma. This is described in Chapter III. Item at left is complete assembly. Item in center is rim, showing changeable notches. Item at right is rotor core. This is at present in Army Security Agency Museum.

: 3560816





graph of a T-52d/e, a German cipher teleprinter described in Chapter III, at present in Army Security

Photograph of German Cipher Device 41, described in Chapter IV, at present in Army Security Agency Museum.

COMPARISON OF RAPID ANALYTIC MACHINERY - OKW/CHI AND A.S.A.

GERMAN (OKW/CHI) RAPID ANALYTIC MACHINERY					AMERICAN (A.S.A.) RAPID ANALYTIC MACHINERY				
NAME	PURPOSE	MAKEREADY REQUIRED	SPEED	DATE ACQUIRED	NAME	PURPOSE	MAKEREADY REQUIRED	SPEED	DATE ACQUIRED
DIGRAPHIC WEIGHT RECORDER ("BIGRAM SUCHGERAET")	SLIDING WHOLE MESSAGE AGAINST ITSELF; LISTING THE WEIGHTS OF THE RESULTANT DIGRAPHS. (ESPECIALLY DESIGNED TO SOLVE JAPANESE TRANSPOSITION "JAE.") SLIDING MESSAGE AGAINST ANOTHER TO RECORD LOCATIONS OF COINCIDENCES.	PUNCHING TELETYPEWRITER TAPES. (DIGRAPHIC WEIGHTS ALREADY PLUGGED ON PLUGBOARD.)	75 LETTERS PER SECOND USING TAPES OF ANY LENGTH.	1943?	ELECTROMECHANAGRAMMER (ATTACHMENT TO I.B.M. TABULATOR.)	SLIDING PART OF MESSAGE AGAINST WHOLE, LISTING TOTALS OF WEIGHTS OF RESULTANT DIGRAPHS. (ESPECIALLY DESIGNED TO SOLVE JAE.)	PULLING I.B.M. CARDS BY HAND; WIRING PLUGBOARD FOR EACH TEST. (DIGRAPHIC WEIGHTS ALREADY PUNCHED IN CARDS.)	2 POSITIONS TESTED PER SECOND, USING CARD DECK OF ANY LENGTH.	1941
POLYGRAPHIC COINCIDENCE COUNTER ("SAEGEBOCK")	SEPARATE COUNTING OF MONOGRAPHS, TRIGRAPHS, ETC., UP TO DECAGRAPHS, COINCIDENT BETWEEN MESSAGES, OR REPEATING WITHIN A MESSAGE; AND A RECORDING OF THE SEPARATE TOTALS THEREOF.	PUNCHING TELETYPEWRITER TAPES.	75 LETTERS PER SECOND USING TAPES OF ANY LENGTH.	1942	HAWKINS' RESISTOP BOARD AND COUNTER.	RECORDING TOTAL OF COINCIDENCES BETWEEN MESSAGES OR OF REPEATS WITHIN A MESSAGE. (NO SEPARATE POLYGRAPHIC COUNT.)	PUNCHING TELETYPEWRITER TAPES.	7 LETTERS TESTED PER SECOND, USING TAPE OF ANY LENGTH.	1940 (NOW OBSOLETE)
					JOOS' TYPEWRITER	RECORDING TOTAL OF COINCIDENCES BETWEEN MESSAGES OR OF REPEATS WITHIN A MESSAGE. (NO SEPARATE POLYGRAPHIC COUNT.)	PUNCHING TELETYPEWRITER TAPES.	7 LETTERS TESTED PER SECOND, USING TAPE OF ANY LENGTH.	1943
					INDEX OF COINCIDENCE MACHINE	INDICATING (BUT NOT EVALUATING OR RECORDING) TOTAL OF COINCIDENCES BETWEEN MESSAGES, OR OF REPEATS WITHIN A MESSAGE. (ACTUAL COUNT MUST BE DONE BY EYE AFTER HIGH VALUED POINTS ARE FOUND.)	PUNCHING TELETYPEWRITER TAPES; PHOTOGRAPHING AND DEVELOPING PLATES.	INSTANTANEOUS OVER SPAN OF 600 LETTERS ONLY.	1943
					70-MM. COMPARATOR	RECORDING SEPARATE TOTALS FOR ANY 5 PATTERNS UP TO TEN LETTERS IN LENGTH, COINCIDING BETWEEN MESSAGES OR REPEATING WITHIN A MESSAGE. (A "PATTERN" MAY BE, FOR EXAMPLE, A DIGRAPH-SPACE-TRIGRAPH.)	PUNCHING 70-MM. TAPES.	300 LETTERS EXAMINED PER SECOND USING TAPES OF ANY LENGTH.	1944
STATISTICAL DEPTH-INCREASER ("TURMUHR")	RAPID TESTING OF MESSAGES TO SEE IF ANY OF THEIR PARTS BELONG TO A GIVEN DEPTH OF STRIP-SYSTEM GENERATRICES. (ESPECIALLY DESIGNED TO SOLVE AMERICAN STRIP SYSTEM.)	PUNCHING TELETYPEWRITER TAPE. (SINGLE LETTER WEIGHTS ALREADY PLUGGED ON PLUGBOARD.)	1 LETTER PER SECOND USING TAPE OF ANY LENGTH.	1943?	(NONE COMPARABLE; WOULD PROBABLY ADAPT REGULAR I.B.M. PROCEDURES.)				
SIMPLE COUNTING APPARATUS	COUNTING OCCURRENCES OF FIGURE DIGRAPHS WITHIN A MESSAGE OR SET OF MESSAGES. (10X10 CLASSES OF DIGRAPHS.)	PUNCHING TELETYPEWRITER TAPE. (NECESSARY TO COPY OFF OR PHOTOGRAPH ANSWER.)	7 DIGRAPHS PER SECOND USING TAPE OF ANY LENGTH.	1943?	DIGRAPHIC FREQUENCY COUNTER OR "FREAK" (BEING BUILT.)	COUNTING OCCURRENCES OF LETTER OR FIGURE DIGRAPHS WITHIN A MESSAGE OR SET OF MESSAGES. (~~900 CLASSES OF DIGRAPHS.~~)	PUNCHING TAPES.	(ESTIMATED: 7 DIGRAPHS PER SECOND)	DUE IN 1946
DIFFERENCING CALCULATOR, NON RECORDING	COMPUTING UNENCIPHERED CODE GROUPS RESULTING FROM APPLYING TRIAL ADDITIVES TO A DEPTH OF ENCIPHERED CODE GROUPS; DIFFERENCING A DEPTH OF ENCIPHERED CODE GROUPS. DEPTH LIMITED TO 30 GROUPS.	SETTING UP OF DEPTH MANUALLY. (PROBABLY 5 MINUTES.)	RAPID MANUAL.	1943?	NATIONAL CASH REGISTER DIFFERENCING CALCULATOR	COMPUTING UNENCIPHERED CODE GROUPS RESULTING FROM APPLYING TRIAL ADDITIVES TO A DEPTH OF ENCIPHERED CODE GROUPS; DIFFERENCING A DEPTH OF ENCIPHERED CODE GROUPS. DEPTH LIMITED TO 20 GROUPS.	SETTING UP OF DEPTHS ELECTRICALLY. (ABOUT 1 MINUTE.)	RAPID MANUAL.	1944
DIFFERENCING CALCULATOR, RECORDING	FLAGGING DIFFERENCES IN A DEPTH OF ENCIPHERED CODE GROUPS. NO LIMIT TO DEPTH.	PUNCHING TELETYPEWRITER TAPES.	7 NUMBERS PER SECOND USING TAPE OF ANY LENGTH.	1943?	(NONE COMPARABLE; WOULD USE REGULAR I.B.M. PROCEDURES, PROBABLY WITH PRE-SENSING GANG PUNCH.)				
LIKELY ADDITIVE SELECTOR ("WITZKISTE")	RECORDING SCORES SHOWING STATISTICAL LIKELIHOOD OF EACH POSSIBLE ADDITIVE, IF APPLIED TO A GIVEN DEPTH OF ENCIPHERED CODE GROUPS. PRACTICAL LIMITS OF DEPTH, 5 TO 20. (ADAPTABLE TO NON-NORMAL ARITHMETIC IF SUFFICIENTLY LARGE DECK OF SPECIAL PLATES HAS BEEN PREPARED.)	(NO MAKEREADY AS USED PREMADE PHOTOGRAPHIC PLATE.) (PHOTOGRAPHING OF ANSWER REQUIRED.)	ABOUT 1 TO 5 MINUTES PER AVERAGE DEPTH.	1943?	LIKELY ADDITIVE SELECTOR. (PROPOSED AND TESTED BUT NEVER USED.)	RECORDING TALLIES SHOWING STATISTICAL LIKELIHOOD OF EACH POSSIBLE ADDITIVE, IF APPLIED TO A GIVEN DEPTH OF ENCIPHERED CODE GROUPS. PRACTICAL LIMITS OF DEPTH, 5 TO 20. (ADAPTABLE TO NON-NORMAL ARITHMETIC IF SUFFICIENTLY LARGE DECK OF SPECIAL CARDS OR PHOTOGRAPHIC PLATES HAS BEEN PREPARED.)	(NO MAKEREADY AS USED PREMADE PUNCHED CARDS OR PHOTOGRAPHIC PLATE.) (PHOTOGRAPHING OF ANSWER REQUIRED.)	ABOUT 1 TO 5 MINUTES PER AVERAGE DEPTH.	TESTED IN 1943
					KEY FINDER. (ATTACHMENT TO I.B.M. TABULATOR.)	RECORDING MOST LIKELY ADDITIVES AND RESULTANT UNENCIPHERED CODE GROUPS, WHEN TESTING DEPTHS OF UP TO 20 ENCIPHERED CODE GROUPS. (ADAPTABLE EQUALLY WELL TO NORMAL OR NON-NORMAL ARITHMETIC.)	PUNCHING OF I.B.M. CARDS FOR GROUPS IN DEPTH. (PLUGBOARDS ALREADY WIRED FOR SCORES INVOLVED.)	3 MINUTES PER DEPTH OF 20.	1943?
(NONE COMPARABLE; GERMAN NAVY ADAPTED REGULAR I.B.M. PROCEDURES TO ACCOMPLISH (I-146).)					SLIDE RUN MACHINE. (ATTACHMENT TO I.B.M. MACHINE.)	DETERMINING AN ENCIPHERED CODE MESSAGE'S ENCIPHERMENT-STARTING-POINT IN A BOOK OF KNOWN ADDITIVES. THIS IS DONE BY TESTING 8 CONSECUTIVE ENCIPHERED CODE GROUPS AGAINST A DECK OF ADDITIVE "CARDS", AND SCORING TRIAL DECIPHERMENTS. (ADAPTABLE EQUALLY WELL TO NORMAL OR NON-NORMAL ARITHMETIC.)	PUNCHING OF CIPHER CARDS. (PLUGBOARD ALREADY WIRED; CARD DECK OF ADDITIVES ALREADY PUNCHED.)	25 COMPLETE TESTS PER SECOND.	1943
(NONE COMPARABLE; PROBLEM DID NOT ARISE.)					"CAMEL" (ATTACHMENT TO I.B.M. MACHINE)	PERMITS DISCOVERY OF MESSAGES (IN CERTAIN JAPANESE ARMY CODE SYSTEMS) LIKELY TO CONTAIN CERTAIN SPECIFIED CLASSES OF PLAIN TEXT.	PUNCHING I.B.M. CARDS FOR MESSAGES.	3 OR 4 MESSAGES TESTED PER MINUTE	1945
(NONE EXACTLY COMPARABLE; ACTUALLY USED REGULAR I.B.M. PROCEDURES OR COULD ADOPT "POLYGRAPHIC COINCIDENCE COUNTER", "DIGRAPHIC WEIGHT RECORDER", OR PROPOSED "REPEAT FINDER.")					BRUTE FORCE (ATTACHMENT TO I.B.M. MACHINE)	INDEXING IN-PHASE BUT NOT NECESSARILY CONSECUTIVE REPEATS BETWEEN MESSAGES. (REPEATS NO MORE THAN 18 GROUPS APART.)	PUNCHING I.B.M. CARDS FOR MESSAGES AND EXPANDING DECK TO ONE CARD PER CIPHER GROUP.	?	1942
REPEAT FINDER (WAS BEING BUILT)	SEARCHING MASS OF MESSAGES FOR REPEATS OF 5 LETTERS OR MORE BETWEEN THEM.	PUNCHING TELETYPEWRITER TAPES; PHOTOGRAPHING AND DEVELOPING FILMS.	10,000 PER SECOND USING ANY LENGTH FILM.	WAS STILL TO BE DELIVERED.	TETRA-TESTER	FINDING REPEATS OF ANY GIVEN TYPE PATTERN, BETWEEN MESSAGES.	PUNCHING TELETYPEWRITER TAPES; PHOTOGRAPHING AND DEVELOPING FILMS. (PHOTOGRAPHING OF ANSWERS REQUIRED.)	5,000 POSITIONS PER SECOND USING FILM OF ANY LENGTH.	1944
(NONE COMPARABLE.)					5202	ESPECIALLY ADAPTED TO BREAKING 5 PERIODIC WHEELS OF GERMAN TELETYPE ENCIPHERING DEVICES, FROM A GIVEN MESSAGE.	PUNCHING TELETYPEWRITER TAPES; PHOTOGRAPHING AND DEVELOPING FILMS.	5,000 POSITIONS PER SECOND USING FILM OF ANY LENGTH.	1945
					DRAGON	ESPECIALLY ADAPTED TO SETTING A CRIB AGAINST PARTIALLY SOLVED GERMAN TELETYPE ENCIPHERED MESSAGE, SO AS TO AID FINAL SOLUTION.	PUNCHING TELETYPEWRITER TAPES.	5 MINUTES PER MESSAGE PER CRIB, USING TAPE OF ANY LENGTH.	1945
(NONE COMPARABLE.)					"003" OR "MADAME X" ("BOMBE")	ESPECIALLY DESIGNED TO SOLVE END PLATE STECKER, WHEEL ORDER AND WHEEL SETTINGS, OF A GERMAN ARMY ENIGMA, FROM A GIVEN CIPHER MESSAGE AND CRIB.	PLUGGING UP PLUGBOARD.	40 PER SECOND	1943
					SINGLE FRAME DUD-BUSTER ATTACHMENT	ESPECIALLY DESIGNED TO SOLVE WHEEL SETTINGS WHEN STECKER AND WHEEL ORDER ARE KNOWN.			
					SCRITCHER	ESPECIALLY DESIGNED TO SOLVE END PLATE STECKER, WHEEL ORDER, WHEEL SETTINGS, AND REVERSING WHEEL WIRING, OF A GERMAN ARMY ENIGMA, FROM A GIVEN CIPHER MESSAGE AND CRIB.	PLUGGING UP PLUGBOARD.	25 PER SECOND ("SUPER" STILL TO COME WILL HAVE SPEED OF 1,000 TO 10,000 PER SECOND.)	1945