German Cipher Machines of World War II

This publication is a product of the National Security Agency history program. It presents a historical perspective for informational and educational purposes, is the result of independent research, and does not necessarily reflect a position of NSA/CSS or any other U.S. government entity.

This publication is distributed *free* by the National Security Agency. If you would like additional copies, please email your request to history@nsa.gov or write to:

Center for Cryptologic History
National Security Agency
9800 Savage Road, Suite 6886
Fort George G. Meade, MD 20755-6886

David Mowry served as a historian, researching and writing histories in the Cryptologic History Series. He began his Agency career as a linguist in 1957 and later (1964-1969) held positions as a linguist and cryptanalyst. From 1969 through 1981 he served in various technical and managerial positions. In the latter part of his career, he was a historian in the Center for Cryptologic History. Mr. Mowry held a BA with regional group major in Germany and Central Europe from the University of California at Berkeley. He passed away in 2005.

Acknowledgment. The Center for Cryptologic History is grateful to mathematician David Perry for his thoughtful and thorough review of all technical material in this edition.

Cover: German soldiers using an ENIGMA cipher machine in the field

German Cipher Machines of World War II

David P. Mowry

Center for Cryptologic History
National Security Agency

Revised edition 2014

Introduction

Along with breaking the Japanese diplomatic cryptosystem usually referred to as "PURPLE," probably the greatest example of Allied cryptanalytic success in World War II was the breaking of the German ENIGMA machine. This cryptodevice was used by all of the German armed forces as the primary cryptosystem for all units below Army level or the equivalent. As D-Day approached, other German cryptodevices, the SZ-42 and the various T-52 machines, assumed great importance since they were used by the higher commands of the German armed forces. Many references to these German machines in the histories fail to provide information on what they looked like or how they worked. Another group of cryptodevices, those invented by Fritz Menzer for the Abwehr (Counterintelligence), have received little or no notice in the literature and are unknown to the public. This brochure is an attempt to remedy both lacks.

The author is deeply indebted to Mr. Ralph Erskine of Belfast, UK, for information concerning Fritz Menzer's Schlüsselgerät 39 (SG-39).

ENIGMA

In 1925 the German Army purchased several examples of a commercially produced cipher machine called the ENIGMA, manufactured first by Chiffriermaschinen Aktiengesellschaft, a company owned by Arthur Scherbius, and later by Chiffriermaschinen Gesellschaft Heimsoeth und Rinke. After some modification, the Army adopted the machine for extensive use.[1]

The standard military ENIGMA used three 26-point wired metal and black plastic rotors selected from a set of five to eight. Each rotor was a cylinder with a large, moveable notched wheel on one end with an alphabet (or numbers) around its circumference. One face of the cylinder had twenty-six spring-loaded copper pins protruding from it, and the other face had twenty-six flush copper contacts. (See Figures 1 and 2.) Inside each cylinder was a wired "maze" connecting the contacts to the pins.

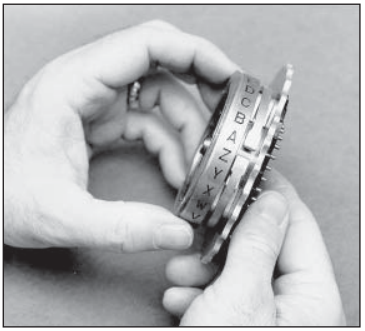


Fig. 1. Setting the notch ring on ENIGMA

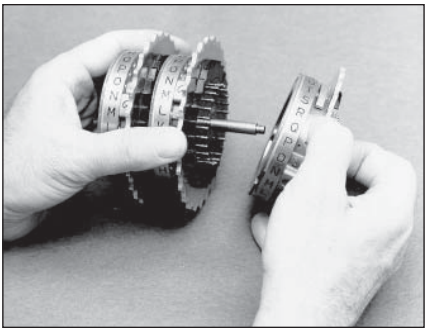


Fig. 2. Assembling the rotor set

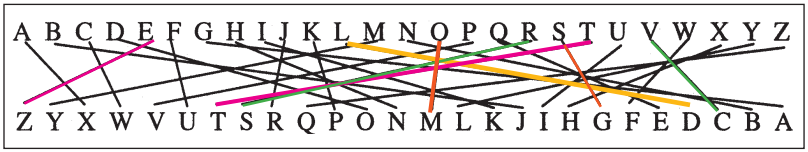


Fig. 3. Example of a wiring maze

With this rotor (Figure 3), the letters "ROOSEVELT" would come out as "SMMGZCZDT." Not too difficult to read … just monoalphabetic substitution. But ENIGMA used three rotors, each one wired differently, and a reflector. When a letter was input, the rightmost wheel would turn one space forward and an electrical pulse would route through each wheel in turn, then through the reflector, then back through the three wheels by a different route, and a glow-lamp would light to show the encrypted character. When the notch on that wheel progressed around to the reading point, the middle wheel would advance one space; and when the notch on the middle wheel progressed to its reading point, the leftmost wheel would advance one space. It would take 16,900 characters to return the three wheels to their initial position. By limiting allowable message length, this "cycling" would not happen.

Figure 4 shows a standard military ENIGMA in its wooden carrying case. All of its essential elements except the rotors are visible. From top to bottom: on the open lid are spare bulbs, a dark green

Fig. 4. Standard military ENIGMA

screen for covering the lights at night, instructions on operating and caring for the machine, and spare plugs for the plugboard; on the body of the machine are the three rotors (covered), the power source dial, the output letter panel, the input keyboard, and the plugboard or *stecker*.

The following description of the ENIGMA setup procedure is taken from the National Cryptologic Museum brochure *Solving the ENIGMA: History of the Cryptanalytic Bombe,* by Jennifer Wilcox. It took two and sometimes three people to operate the machine, but first it had to be set up. This involved selecting three rotors from the provided set according to the instructions in the monthly key list. Each rotor had a moveable placement notch on an outer ring. The notch forced the rotor to its left to step one place forward and could be moved to a different point on the rotor by rotating the outer ring (Figure 1). The

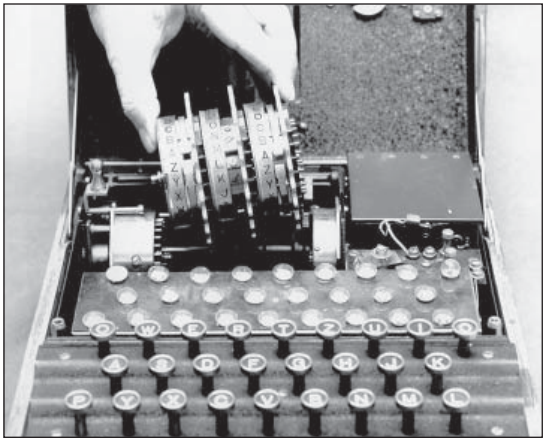


Fig. 5. Putting ENIGMA rotors in the basket

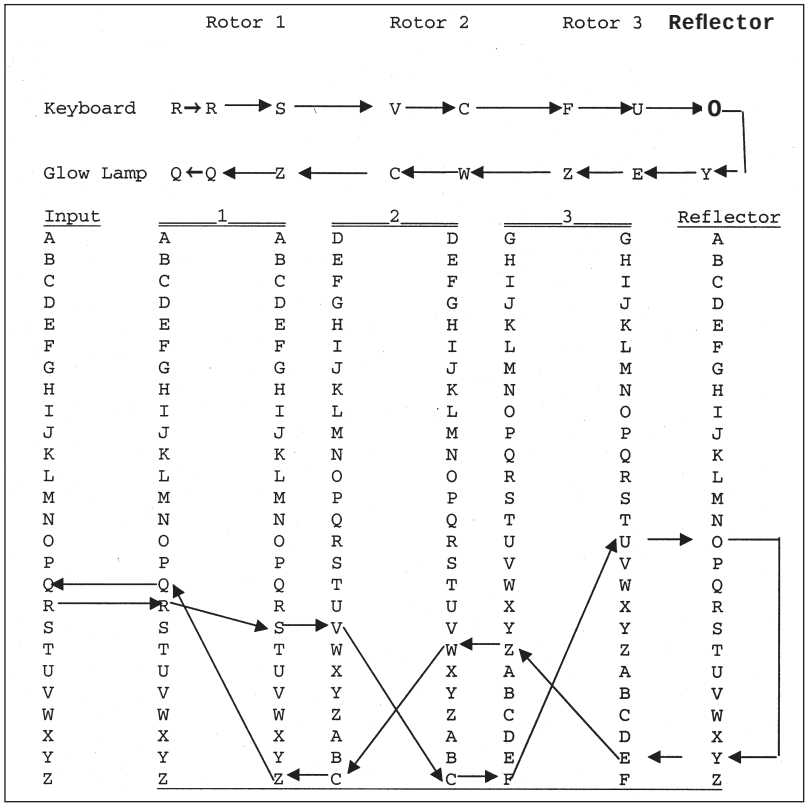


Fig. 6. Sample ENIGMA-type encryption (without stecker). A plaintext *R* would, in this case, produce the cipher value *Q*.

Fig. 7. Stecker (plugboard)

three rotors were then assembled on an axle in the proper order (Figure 2) and placed in the machine (Figure 5).

In addition, the stecker had to be applied. This was a military addition to the original ENIGMA and consisted of a plugboard with contacts for the letters of the alphabet. In accordance with the key list, plugs were inserted into this board in pairs to further encipher the characters. In Figure 7, for example, entering the letter *Q* on the keyboard would result in the letter *Y* being introduced into the maze, and, conversely, an encryption that would have lit the letter *Y* on the display would now, after passing through the stecker, light up the letter *Q*.

After the machine was set up, it was ready for use. The wheels were set with three letters (or numbers) appearing in the window as determined by the code clerk (Figure 8). These were changed with

Fig. 8. Setting the wheels on ENIGMA

each message sent, and the setting was included at a prearranged point in the message indicator. Encryption could then start. One operator used the keyboard while either reading the message or having it read to him. Another operator wrote down the cipher values as they lit up on the display (see cover photo). The recipient would set the rotors according to the transmitted window setting and decipher the message. Encryption and decryption followed the same procedure.

The "FISH" Machines

Under the general name of *Geheimschreiber* (secret writer), the Germans used two devices for enciphering high-level (Army level and above) radioprinter communications. (ENIGMA was used for Army level and below.) These were the T type 52-B/C/D/E, built by Siemens & Halske, and the SZ-40/SZ-42, built by Standard Elektrik Lorenz. The "SZ" meant *Schlüsselzusatz* (key attachment), so called because the essential encryption mechanism was in a box that could be detached from the radioprinter machine. The British referred to these machines by the generic name of FISH and specifically as STURGEON and TUNNY, respectively. The British titles will be used in this paper, inasmuch as these are the more familiar names.

General Comments on Enciphered Radioprinter

Baudot Code

Radioprinter communications are based on the Baudot code, which replaces each letter with five electrical impulses (or bauds), represented here by + (or "mark") and o (or "space"). There are thirty-two such combinations possible ($2^5 = 32$), accounting for twenty-six letters plus six extra characters. These six extra characters will be represented here by 3, 4, 8, 9, +, and /. The complete Baudot code is shown below.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	3	4	8	9	+	/
+	+	o	+	+	+	o	o	o	+	+	o	o	o	o	o	+	o	+	o	+	+	+	+	o	o	+	o	+	o		
+	o	+	o	o	o	+	o	+	+	+	+	o	o	o	+	+	+	+	o	o	+	+	+	o	o	o	o	+	+	o	+	o
o	o	+	o	o	+	o	+	o	+	+	o	+	+	o	+	+	o	+	+	o	+	+	o	+	+	o	o	o	+	+	o	o
o	+	+	+	o	+	+	o	o	+	+	o	+	+	+	o	o	+	o	o	o	+	o	+	o	o	+	o	+	o	o	o	o
o	+	o	o	o	o	+	+	o	o	o	+	+	o	+	+	+	o	o	+	o	+	+	+	+	+	o	o	+	o	+	o	

Radioprinter Operation

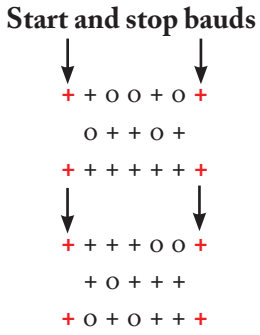
When a radioprinter key is struck, a sequence of seven impulses is generated and transmitted to the receiving radioprinter one at a time, in order. The first of these is the "start" pulse, which alerts the receiving radioprinter to receive the next six impulses. Five of these are the Baudot coding of the letter typed, causing the receiver to print that letter. The last impulse is the "stop" pulse.

The radioprinter signal is enciphered through "baud addition" in that the plaintext bauds are combined with key bauds according to the rule:

	+	o
+	o	+
o	+	o

Thus, + and + combine to give o
+ and o combine to give +
o and + combine to give +
o and o combine to give o

These rules can be condensed by saying that like signs combine to give o and unlike signs combine to give +.



When a cipher unit is added to a radioprinter, there are two types of operation that may be used. In "on-line" operation, the plain text is typed and is immediately enciphered by the machine, which transmits the cipher letter instead of the plain letter. In "off-line" operation, the cipher text is printed or, more likely, punched onto a paper tape for later transmission.

When on-line operation is used, the cipher is not in general broken up into message-length chunks so that several messages might be sent in succession without resetting the cipher unit for each one and thus possibly causing the two terminals to go out of synchronization.

Description of the TUNNY System

The name "TUNNY" referred specifically to a device attached to a Lorenz teletypewriter to encrypt its output (Figures 9-11). Operation was as follows: The *Schlüsselkasten* or cipher box consisted of twelve wheels, each with a prime number of settable lugs (*Sprossen*) around the circumference (wheel lengths were not prime). Each wheel was driven from a common shaft through a pair of gears.

For purposes of description, the wheels are numbered 1 to 12 reading from left to right from the front of the box (Figure 10). Baud-by-baud encipherment was accomplished by adding the plain baud to the mark or space appearing on the enciphering wheels. The

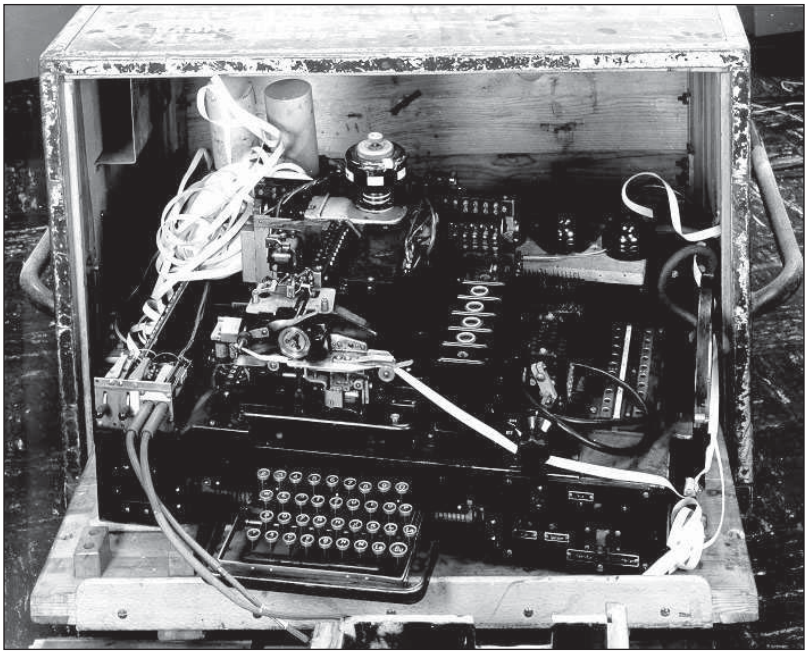


Fig. 9. TUNNY teletype base, in safe

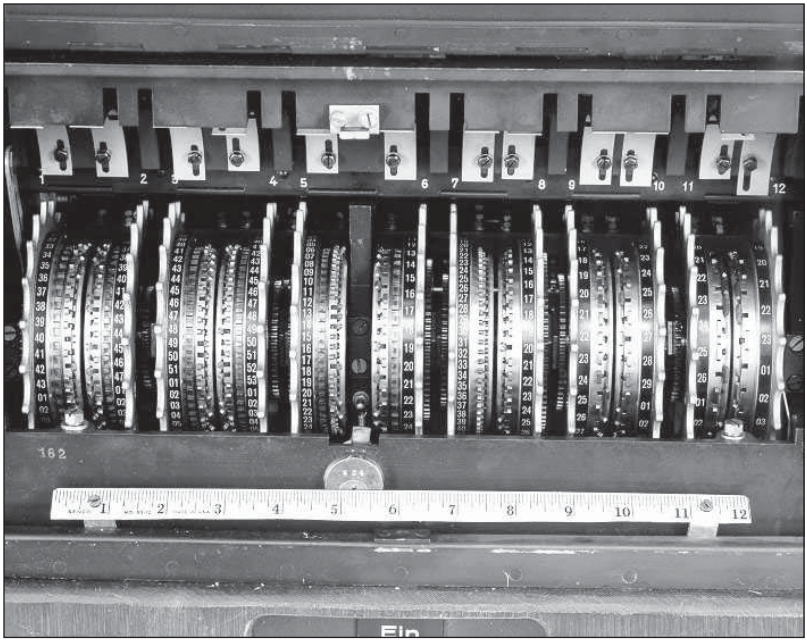


Fig. 10. TUNNY rotor basket

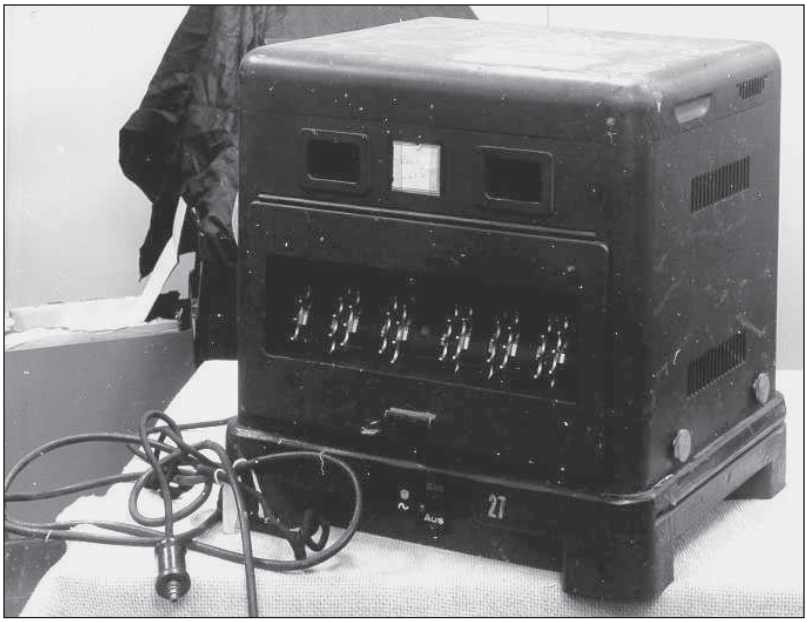


Fig. 11. TUNNY rotors

periodic, or so-called chi wheels (numbers 1 to 5), are of lengths 41, 31, 29, 26, and 23 and step once with each character enciphered. The aperiodic, or psi wheels (numbers 8-12), are of lengths 43, 47, 51, 53, and 59. The first chi wheel (number 1) interacts with the first psi wheel (number 8), forming a combined impulse which acts on the first impulse of the plaintext letter being enciphered. Likewise, the 2 and 9, 3 and 10, 4 and 11, and 5 and 12 wheels interact with the respective plaintext impulses. Wheels 6 and 7 were control wheels that caused irregular motion in the encipherment wheels.

The primary motor wheel or mu1 (number 6), of length 61, controls the motion of the secondary motor, or 37 wheel, mu2 (number 7), which in turn controls the motion of the aperiodic wheels. A mark in the number 6 wheel compels motion of the number 7 wheel; after this motion, if a mark is at the reading position of the number 7 wheel, it compels motion of all the psi wheels. Conversely, a space in the number 6 wheel denies motion to the number 7 wheel, and a space in the number 7 wheel denies motion to the five psi wheels. As used by the Germans, the number 6 wheel had between eleven and nineteen spaces. The number 7 wheel consistently had eleven spaces. Two consecutive spaces were very rare in either wheel.

In addition, there is a secondary chi effect on the psi wheels. That is, a space in the second chi wheel (number 2) two positions in back of its active position compels motion of the psi wheels. When the second chi was used in conjunction with the motor, the number 7 wheel had sixteen spaces, resulting in the same proportion of spaces to marks as when no secondary chi wheel effect was used. The patterns of the chi and psi wheels were changed monthly, the mu wheel patterns daily.

Figure 12 gives a sample run of fifty characters showing the effect of the above with the exception of the secondary chi effect. Arrows and bauds in red show where each wheel completes its cycle and starts over.

Fig. 12. TUNNY encryption: Sample run of fifty characters

	Chi	Psi				
	12345	12345	Mu1	Mu2	P	C
1	+oo+o	+o+oo	o	+	T	M
2	+oooo	+oooo	+	+	H	H
3	o++o+	o+o+o	o	o	E	X
4	+++oo	o+o++	+	+	9	X
5	oooo+	+oooo	o	o	Q	I
6	+o+o+	++ooo	+	o	U	W
7	oo+oo	oo++o	+	+	I	A
8	+o+oo	oooo+	o	+	C	G
9	oo+o+	oo+oo	+	o	K	Q
10	+oooo	++o+o	+	+	9	Y
11	o+o+o	o++oo	+	+	B	A
12	o++oo	oo+++	+	o	R	3
13	+o++o	oo+oo	o	+	O	V
14	+o++o	o+++o	+	+	W	Y
15	oo+oo	oo+o+	+	o	N	A
16	oooo+	+oooo	+	+	9	L
17	+oooo	+oooo	+	+	F	T
18	+oo+o	oo+oo	+	o	O	F
19	+oo+o	ooo++	+	+	X	T
20	+o+o+	+o++o	+	+	9	8
21	oo+oo	oo+oo	o	o	J	E
22	+oo++	oooo+	+	+	U	R
▶ 23	++ooo	oo+o+	+	+	M	V
24	o++oo	+oooo	+	o	P	Z
25	oo+oo	oo+oo	+	+	E	9
▶ 26	oo+o+	oo++o	+	+	D	B
27	++o+o	++ooo	o	+	9	Q
28	+ooo+	o++++	+	o	O	Z
▶ 29	oo+o+	++ooo	+	+	V	L
30	+oooo	++o+o	+	+	E	F
▶ 31	+ooo	ooo++	+	+	R	K
32	+o+o+	oo+oo	+	o	9	Y
33	oo+oo	oooo+	+	+	T	9
34	o+ooo	o+o+o	o	+	H	A
35	o++oo	o++oo	+	+	E	P
36	+o+oo	+oo++	+	o	9	S
▶ 37	+o++o	++ooo	+	+	L	5
38	oo+o+	o+oo+	+	+	A	J
39	ooo+o	oo+oo	+	+	Z	R
40	ooo+o	o++o+	o	o	Y	A
▶ 41	o+oo	ooo++	+	+	9	Y
42	+++oo	o+oo+	+	o	D	T
▶ 43	+++o+	o++oo	+	o	O	N
44	oo+++	++++o	+	+	G	X
45	+oo+o	+oooo	+	+	S	9
▶ 46	oooo+	oo+oo	+	o	9	M
▶ 47	+oooo	o+oo+	+	+	B	M
48	ooo+o	+oooo	o	+	A	5
49	+o+oo	+++oo	+	o	C	Z
50	oo+++	oo+oo	+	+	K	F

Description of the STURGEON System

There is a superficial resemblance between the TUNNY and STURGEON machines in that each has a basket containing large rotors (see Figures 10 and 13). However, the TUNNY basket is attached to a Lorenz radioprinter machine while the STURGEON basket is an integral part of the Siemens-Halske T-52 equipment. Also, the philosophy and operation of the two machines are completely different. Where TUNNY performs a substitution for each plaintext letter through baud addition using wheels 1-5 and 8-12, STURGEON performs a substitution for each plaintext letter through baud addition using wheels 1-5 and then transposes the bauds in the resulting cipher letter using wheels 6-10. (There are no motion wheels.) In other words, there is a ten-level key stream.

Production of this ten-level key stream can be accomplished by four slightly different methods, giving rise to four STURGEON models: T-52-B, T-52-C, T-52-D, and T-52-E. (T-52-A was an experimental model that was never used.) There are ten wheels in each model, and each wheel has a fixed notch pattern cut into its perimeter. The notches are referred to as "o" and the raised portions

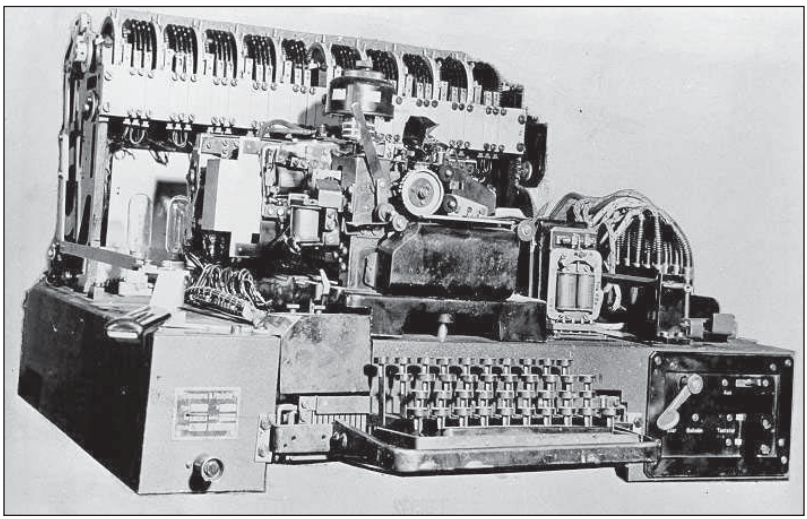


Fig. 13. STURGEON cipher machine

as "+". The wheels have lengths (+'s + o's) of 73, 71, 69, 67, 65, 64, 61, 59, 53, and 47, reading from 1 to 10.

The different key productions are obtained from different uses of the notch patterns and from different ways of controlling the stepping of the wheels. For each wheel there is an "encipherment reading station," which reads the baud (+ or o) from the wheel at a given enciphering position. These ten reading stations may be arbitrarily "steckered" (plugged) to ten points labeled 1, 3, 5, 7, 9, 2, 4, 6, 8, and 0. The notch patterns may be used with either a "1 to 1" stecker or a "4 to 1" stecker, and the stepping may be either regular or irregular. The models may be described on the basis of stecker and stepping as follows:

Stecker		Stepping
1-1	4-1	
T-52-B	T-52-C	Regular
T-52-D	T-52-E	Irregular

On a 1-1 stecker, the substitution keys come from the points 2, 4, 6, 8, and 0, while the transposition keys come from the points 1, 3, 5, 7, and 9. In this case, each baud of the key stream comes from a single wheel and is called a single-wheel stream.

On a 4-1 stecker, each key element is formed by the sum of four points, as:

Substitution	**Transposition**
Baud 1 = 5 + 7 + 4 + 8	Baud 1 = 1 + 3 + 6 + 0
Baud 2 = 3 + 5 + 9 + 0	Baud 2 = 2 + 4 + 6 + 8
Baud 3 = 1 + 3 + 2 + 8	Baud 3 = 5 + 7 + 6 + 0
Baud 4 = 9 + 2 + 6 + 0	Baud 4 = 1 + 3 + 5 + 4
Baud 5 = 7 + 9 + 2 + 8	Baud 5 = 1 + 7 + 9 + 4

For example, the first baud of the substitution stream is obtained by adding (using the usual rules) the bauds that are read from whichever four wheels happen to be steckered to points 5, 7, 4, and 8. In this case each level of the key-stream is a four-wheel stream.

After the plain letter has thus been enciphered, its bauds are transposed. If the first baud on wheel 6 is an o, bauds 1 and 5 of the cipher character are swapped; an o on wheel 7 swaps bauds 4 and 5; an o on wheel 8 swaps bauds 3 and 4; an o on wheel 9 swaps bauds 2 and 3; and an o on wheel 10 swaps bauds 1 and 2. A + in any of these positions would result in that specific transposition not being performed.

The term "regular stepping" (or "regular motion") means that each wheel moves one position after each encipherment. "Irregular stepping" means that the wheels do not all advance after each encipherment. In fact, the stepping of each wheel is controlled by some of the other wheels. This is effected by placing a motion-reading station on each wheel and arranging definite rules by which the signs read on one wheel help determine whether another wheel steps or stands still after a particular encipherment.

There are two categories of irregular motion: *Ohne Klartextfunktion* and *Mit Klartextfunktion* (without plaintext function and with plaintext function). The rules are shown below.

STURGEON irregular motion

Ohne	Mit
1, 2, 3, & 4 step 1 if 5 = o or 6 = o	1 steps 1 if 2 = + or 3 = + or P_3 = +
5 steps 1 if 6 = + or 7 = o	2 steps 1 if 3 = o or 4 = + or P_3 = +
6 steps 1 if 7 = + or 8 = +	3 steps 1 if 4 = o or 5 = +
7 steps 1 if 8 = o or 9 = o	4 steps 1 if 5 = o or 6 = o
8 steps 1 if 9 = + or 10 = o	5 steps 1 if 6 = + or 7 = o or P_3 = o
9 steps 1 if 10 = + or 1 = o	6 steps 1 if 7 = + or 8 = + or P_3 = o
10 steps 1 if 4 = o or 5 = +	7 steps 1 if 8 = o or 9 = o
	8 steps 1 if 9 = + or 10 = o
	9 steps 1 if 10 = + or 1 = o
	10 steps 1 if 1 = + or 2 = o

A wheel stands still (sticks) if neither of its motor wheels forces it to move. All signs are read from the motion-reading station.

P_3 refers to the third baud of the plaintext in the previous wheel position, not the present one. Note that in OHNE motion, the wheels 1, 2, 3, and 4 either all move or all stick. The reason for this is that it guarantees a cycle of at least 73 × 71 × 69 × 67, or 23,961,009. With MIT, no cycle guarantee is necessary. Note also that MIT motion is a form of autokey, with the plaintext contributing to the key.

The Menzer Devices

Ostwin Fritz Menzer was born 6 April 1908 in the village of Herrndorf in Saxony. At the age of eighteen he enlisted in the Army as a mechanic and was assigned to a motor battalion in Leipzig. Having shown an aptitude for cryptanalysis, in May 1935 he was transferred to OKW/Chi (the Army's cryptologic bureau), where he received his first formal training in the field. His enlistment expired on 31 May 1938, and he continued to work as a civilian. Two years later, he was promoted to the rank of superior government inspector. In 1942 Admiral Canaris, the chief of the Abwehr, charged Menzer with testing the security of Abwehr cryptosystems. From then to the end of the war, Menzer worked for the Abwehr as technical consultant in cryptography.[2]

During Menzer's service with OKW/Chi and the Abwehr (1935-1945), he was responsible for a number of advances in the science of machine cryptography. In general, his procedure was to adapt the use of Hagelin pin wheels to provide for irregular wheel motion in cryptoequipment.

The two major types of cryptoequipment used by the Germans before World War II were the ENIGMA and machines made under the Hagelin patents. As we have seen, in the ENIGMA motion was odometer-type, with the only variation being the starting point of the cycle on each rotor. In the Hagelin machines, as you will see, the key wheels also stepped once with each encipherment. Menzer's inventions were designed to make such motions unpredictable.

The Hagelin Patents

Boris Caesar Wilhelm Hagelin was a Swede born in 1892 in the Caucasus, probably in present-day Georgia. He received his degree in mechanical engineering from the Royal Institute of Technology in Stockholm in 1914. After gaining engineering experience in both Sweden and the United States, he returned to Sweden in 1922. At that time his father, a stockholder in Aktiebolaget Cryptograph (Cryptograph, Inc.), placed Boris in that firm to represent the family investment. In 1927 the firm was reorganized as Aktiebolaget Cryptoteknik with Boris in charge. The first cryptomachine using what would be known as "Hagelin action" was the C-36, which, with modifications, was adopted by the U.S. Army as the Converter M-209. The M-209 was used in military units division level and below during World War II and into the Korean War. The description of the workings of the M-209 given here was typical of the action now known as "Hagelin action."

The following description of Hagelin action in the M-209 is keyed to the photograph in Figure 14. The M-209 was essentially a Hagelin C-36 device made under license in the United States for use by the American armed forces in World War II.

There are six key wheels (labeled 1 in Figure 14) whose lengths are mutually prime. These lengths are indicated by different lengths of letter sequences (26, 25, 23, 21, 19, and 17) on the wheels. Each key wheel steps once with each encipherment, returning to its starting position after its period. These wheel lengths give a cycle length of $26 \times 25 \times 23 \times 21 \times 19 \times 17 = 101{,}405{,}850$.

On each key wheel there are pins corresponding to the letters (#5 in Figure 14). Each pin can be set as "active" (i.e., pushed to the left so it can engage a lug on the cage) or "inactive."

The "cage" (#3 in the figure) is a cylinder composed of twenty-seven bars bearing projections known as "lugs" (#4), which are positioned to correspond to the key wheels. The cage rotates once with every encipherment. If a lug encounters an active pin, the bar is slid to the left so that its end projects past the end plate (#2). In each case,

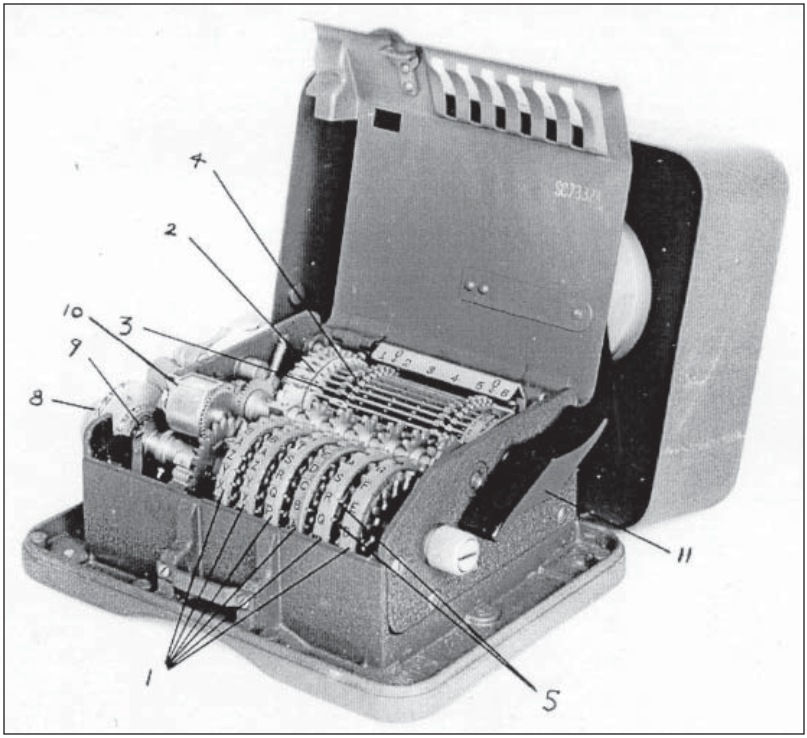


Fig. 14. The M-209 cipher machine

1, key wheels; 2, end plate; 3, "cage" or cylinder composed of bars; 4, projections or lugs; 5, pins corresponding to letters; 6,7 omitted; 8, knurled knob; 9, plaintext wheel; 10, character counter; 11, operating lever

this effectively creates a gear "tooth." These teeth engage another gear and turn it in accordance with the total number of teeth projecting from the cage. The number of lugs for each key wheel governs the number of teeth and thus the "kick" for that wheel.

To set the device up for encryption, the pins and lugs must be set according to a keylist giving the settings for the day. The key wheels are then turned by hand to position six letters in the starting window. These letters constitute the message indicator, which must be included in the message in some way to inform the decipherer where to set the wheels for decryption.

In operation, the encipherer sets the machine to "encipher" and turns a knurled knob (#8 in Figure 14) on the left side of the machine to align the desired letter on the plaintext wheel (#9) with an index mark. A low-frequency letter such as *X* is used as the word separator. The operating lever on the right side of the machine (#11) is then rotated. The cage rotates, the gear is turned and turns the print wheel, which is fixed to the plaintext wheel, the number of places determined by the projecting teeth on the cage. A counter (#10) keeps track of the number of characters enciphered.

With the completion of the movement of the operating lever and its return to its normal position, the paper tape advances one position, the print wheel prints the cipher character on paper tape, the bars in the cage return to their normal position, the key wheels step one position, and the machine is ready for its next input. Cipher characters are printed on gummed paper tape in five-letter groups.

The decipherer, in turn, sets his machine up in accordance with the key list. When the message is received, he sets the key wheels to the message indicator, sets the machine to "decipher," and follows the same procedure as was used in enciphering. The plaintext is then printed on paper tape in a continuous stream.

Schlüsselgerät 39 (SG-39)

In June 1945 Major Howard C. Barlow, USA, reported to Colonel George A. Bicher concerning Menzer's Schlüsselgerät 39 (SG-39).[3] Barlow had flown to Frankfurt-am-Main on 24 June to investigate the SG-39. In the course of his investigation, he found that although the machine was invented in 1939, only three had been constructed, and only one of these was complete. According to one of the technicians who worked on the machine, the long delay in production was caused by the Army's inability to decide whether it wished this model to be capable of operating on radioprinter lines or only for the production of printed tape. The eventual plan was to make this machine for use by lower-echelon units and later to make a similar machine which was to replace the T-52-D and T-52-E (STURGEON).[4]

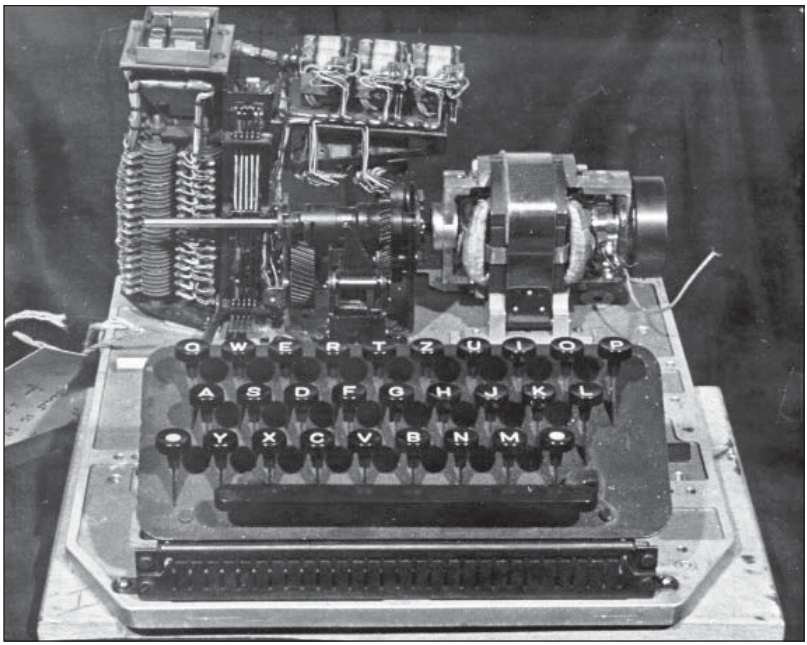


Fig.15. Incomplete Schlüsselgerät 39

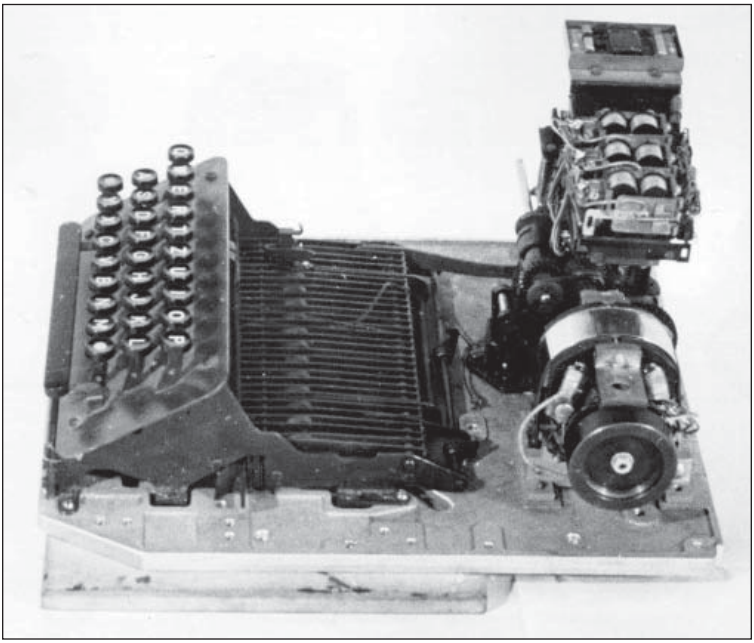


Fig. 16. Incomplete SG-39

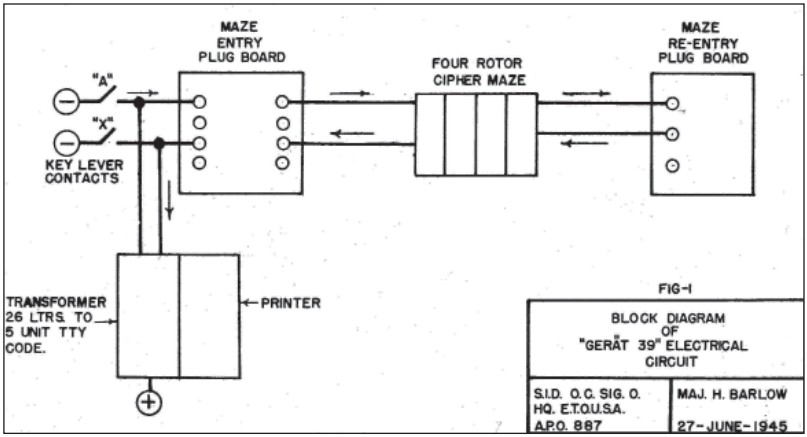


Fig. 17. SG-39 electrical circuits

Of the three machines identified by Barlow, one was complete, the second was missing the printing mechanism, and the third lacked both the printing mechanism and the rotor mechanism. The first two had been packed into boxes and shipped to a military depot at Tauberbischofsheim on 22 March 1945. Barlow took the third, and most incomplete, machine, but decided not to pick up the boxes containing the completed machines at the Tauberbischofsheim Depot as it was felt to be "too long a chance to be worthy of the 150-mile trip." As a result, the photographs in Figures 15 and 16 are of a very incomplete machine.

The SG-39, which Menzer invented in 1939, was an electrical motor-driven cipher machine intended eventually to replace the standard ENIGMA. The SG-39 had a standard typewriter keyboard; a three-position switch for "Off," "Encipher," and "Decipher"; a counter; a dual-printing unit; a motor-driven cipher maze; and changeable plugboards for rotor input and re-entry points. A block diagram of the electrical operation of the machine is given in Figure 17, and the general mechanical layout is shown in Figure 18. One of the dual printers printed the clear text and the other simultaneously printed cipher text spaced into four- or five-letter groups. The cipher maze consisted of four electrical rotors, one of which was stationary,

and three mechanical wheels with the stepping of the electrical rotors being effected both by Hagelin-type settable pins in the mechanical wheels and by further Hagelin-type settable pins contained as an integral part of the electrical rotors' setup on the equivalent of the ENIGMA notch ring. Encipherment of a character through the electrical maze was as is found in a normal ENIGMA.[5]

The stepping motions were as follows:

1. With each letter, the three mechanical wheels, which had lengths of 21, 23, and 25, moved forward one position each. If the pin setting of any mechanical wheel happened to be in an active position, the corresponding rotor would move one step forward. If, for example, the pins on wheels 1 and 3 were in active positions and the pin on wheel 2 was not, then rotor 2 would remain stationary and rotors 1 and 3 would

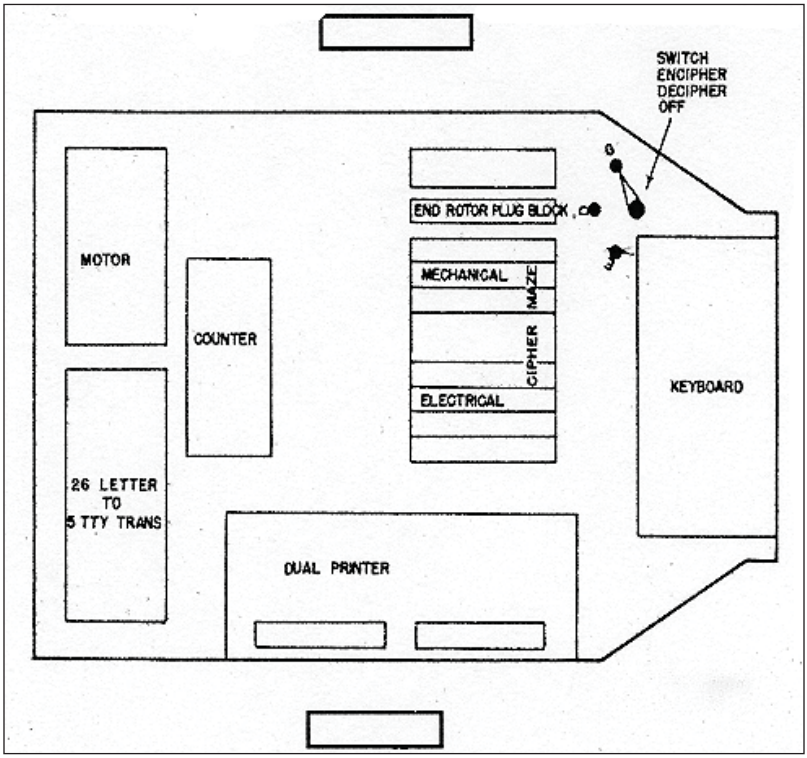


Fig. 18. SG-39 layout

step. Rotor 4 was used as a stator, that is, its position was set at the beginning of the message and it remained stationary throughout the message.

2. In addition to the stepping caused by the mechanical wheels, there was an additional independent stepping motion caused by the Hagelin-type pins on the periphery of each rotor. If the Hagelin-type pin on rotor 1 was in an active position, it caused rotor 2 to automatically move one step forward. If the pin on rotor 2 was in an active position, it caused both rotors 2 and 3 to move one step forward. If the pin on rotor 3 was in an active position, it caused rotor 1 to move one step forward. Rotor 4 had no stepping motion. If a specific rotor had been given one step forward by the mechanical wheels and in addition was independently kicked one step by the pins on the electrical rotors, only one of these kicks would take effect.

The SG-39 was fully automatic, in that when a letter key was pressed, the plain and cipher letters were printed on separate paper tapes, divided into four- or five-letter groups. The outputted character was converted into five-level radioprinter code before being fed to the print wheel. This would have allowed the output to be used to punch five-level paper tape for radioprinter transmission if so desired.

The cycle for an unmodified ENIGMA is 16,900. When set up in accordance with Menzer's instructions, the SG-39 had a cycle length of 2.7×10^8 characters—more than 15,000 times as long as the cycle length of the unmodified ENIGMA.

Schlüsselgerät 41

The Schlüsselgerät 41 (SG-41), invented in 1941, was based on Hagelin encryption but included a mechanism for variably stepping the Hagelin wheels (Figures 19-21).

This mechanical cipher machine had six pin wheels which were mutually prime. The first five of these wheels had kicks of 1, 2, 4, 8,

Fig. 19. Schlüsselgerät 41 ready for use

and 10 active pins, respectively. The sixth wheel made these kicks positive or negative. In addition to the pins operating on the lugs, there was for each wheel a "motion index reader" and, on the sixth wheel, a "kick index reader."

Fig. 20. Schlüsselgerät 41

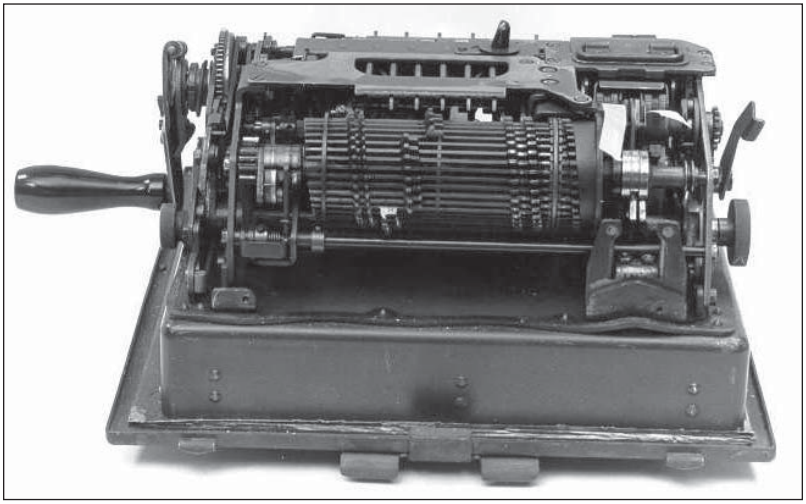


Fig. 21. Schlüsselgerät 41, rear view

The enciphering cycle (encryption of one letter) consisted of three elements:

> 1. Step 1 took place if and only if the sixth wheel had an active pin in the "motion index position." If this were the case, then all of the following 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 the motion index position, in which case it would move two steps.
>
> 2. A key kick was generated as in normal Hagelin action. If, however, the sixth wheel had an active pin in the kick index position, the key kick would be 25 minus the sum of all the other kicks. In other words, under such a circumstance, the key would complement itself.
>
> 3. This step was identical to step 1, except that it occurred whether or not wheel 6 had an active pin in the motion index position. In this step, wheel 6 also stepped one or two positions, depending on the state of wheel 5. [6]

The original specifications called for a lightweight, durable machine to be used by units forward of division. Menzer designed it to provide a cipher tape and to be keyboard operated in order to improve the speed of encryption. According to Menzer's description, he was able to redesign the arrangement of letters on the print wheels to flatten the cipher frequency count as a result of the keyboard operation.

Because of wartime shortages of aluminum and magnesium, the machine ended up weighing between twenty-six and thirty-three pounds, too heavy for field use. Removal of the keyboard would have lightened the machine, but the redesign of the print wheels prevented their being used directly for encipherment. Production stopped because no one knew what to do. About 1,000 machines had been constructed, and these were distributed to the Abwehr, which began using them in 1944.[7]

Ease of maintenance was not a strong point of the SG-41. Removal of the cover involved removing all external knobs and cranks and then undoing six screws. [8]

Schlüsselkasten

Although the Schlüsselkasten (cipher box) was not a machine, it was intended to be a substitute or backup for ENIGMA, and is therefore included in this booklet. The Schlüsselkasten was a mechanical cipher device that used the principle of sliding two printed strips against one another according to a prescribed plan to generate the cipher equivalents. The Germans intended to have 1,000 available by October 1945 and to mass-produce 10,000 per month by January 1946. It would have replaced the ENIGMA below the level of division. Nineteen forty-five was too late; if it had been introduced in 1942, it could have changed the course of the war. Basically, the Schlüsselkasten was a twelve-ounce aluminum box containing four Hagelin pin wheels and a coil spring which determined the stepping of a sliding strip on the top of the box.

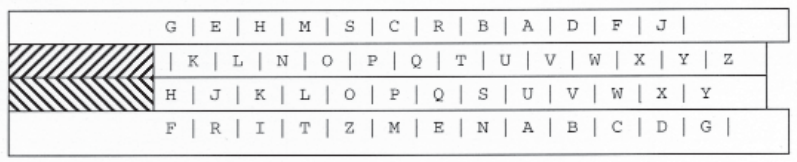


Fig. 22. Printed sliding strips of a Schlüsselkasten

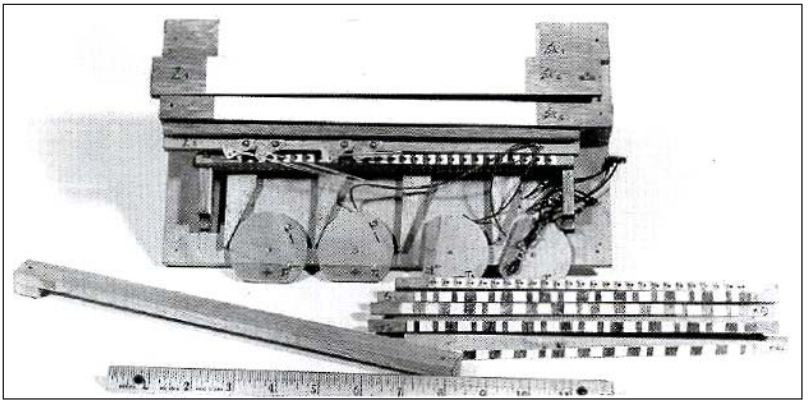


Fig. 23. These models (above and next page) were made by Fritz Menzer to illustrate aspects of the working of the Schlüsselkasten. No actual working devices are available.

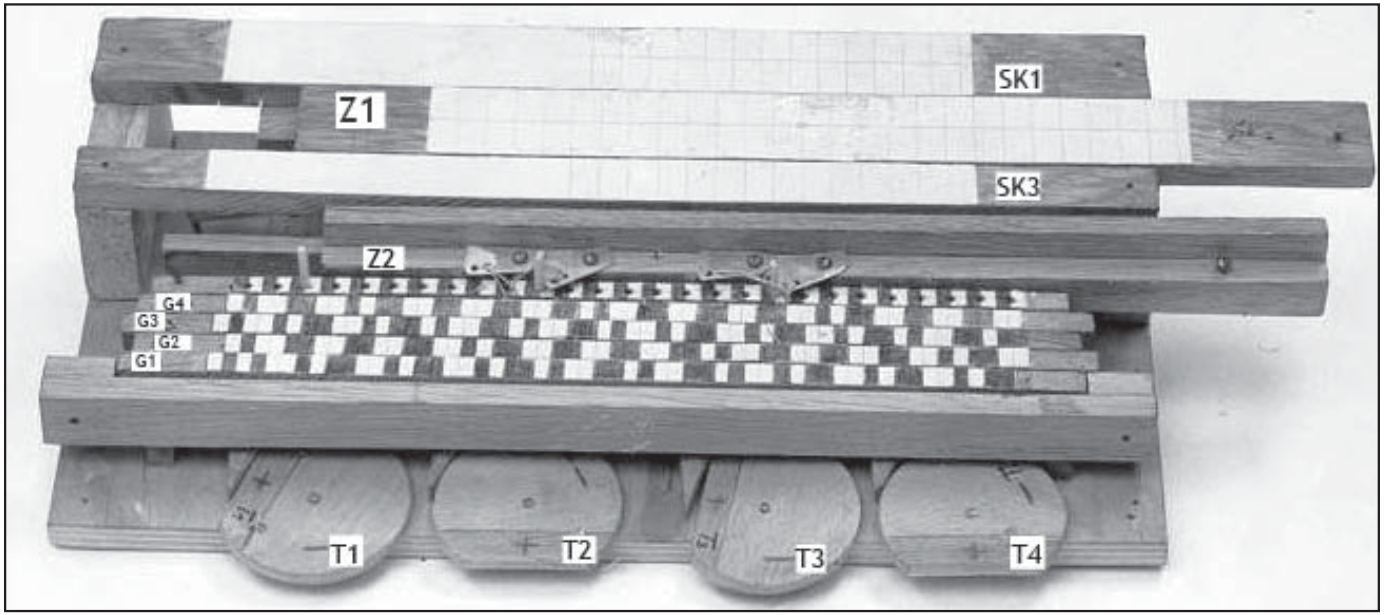


Fig. 24. A Schlüsselkasten model powered with elastic bands demonstrated the rules of motion in this device. The disks, T1-T4, represent slip-wheels which affect the relative positioning of pin wheels G1-G4. The black and white squares represent active and inactive pin wheels. Dowels would be inserted into the holes corresponding to positions where all holes were active or all inactive. Z1 and Z2 would be pulled to the right and released. Each time one of the four metal slips on Z2 encountered a dowel, the mechanism would stop and a cipher value would be read off of SK1 or SK3.

Thirteen characters from each of two key-word mixed alphabets were written on the fixed base, and the other thirteen of each on the top and bottom of the sliding strip. (The key-word mixed sequence in Figure 22 is based on *Geheimschreiber*—top row—and *Fritzmenzer*—bottom row.) The latter were written so that only one alphabet at a time was in phase. Alphabets could be changed as often as desired.

In use, the slide was pulled to the right until it stopped, winding the spring that drove the mechanism. Pressing a button released the slide to move left. When at either or both of the reading positions A1 or A2, the pins on all four pin wheels were all inactive, the slide stopped, and encipherment took place. If the step came from A1 alone or A1 and A2 together, the slide took an additional step. When the slide stopped, either the top or the bottom alphabet would be in phase, and the cipher value could be read off. Pressing the button again would allow the slide to slide left to its next stop.

Conclusion

The Germans had a good head start in the construction of mechanical cryptodevices before the beginning of World War II with ENIGMA, and developed excellent enciphered teleprinter devices with the T-52s and SZ-40/SZ-42s. If Menzer's devices had been introduced in a timely manner from 1940 on, they would certainly have complicated the Allied cryptanalytic effort, which was strongly oriented toward solution of ENIGMA traffic from 1939 on. This is not to say that the Allies would not have been able to read German traffic. The Germans did not intend to replace the ENIGMA on higher echelon communications, and in the face of necessity, methods would have been found to solve Menzer's devices. But the Allies would have lost much of the edge that the Poles presented to the British in 1939, when they turned over the results of their analysis of the ENIGMA to the Government Code and Cipher School.

Notes

1. David Kahn, *The Codebreakers* (New York: Macmillan, 1967), 421-22.

2. David P. Mowry, "Regierunges-Oberinspektor Fritz Menzer: Cryptographic Inventor Extraordinaire," *Cryptologic Quarterly,* Vol. 2, Nos. 3-4, Fall/Winter 1983-84, 21-36.

3. 79/49/TOPSEC/AS-14, TICOM DF-174, "Description of Contacts of Fritz Menzer with American and Soviet Authorities and Summary of Career"; WDGAS-14, 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, Vol. 2.

4. TICOM I-53, Memorandum to Colonel George A. Bicher, "Investigation of Firm 'Telefonbau-Und-Normalzeit' for Geraet 39," 27 June 1945.

5. Ibid.

6. Ibid.

7. WDGAS-14.

8. "Report on SG-41 by Wilhelm Buggisch," 30 August 1945.


NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA