Regierungs-Oberinspektor Fritz Menzer: Cryptographic Inventor Extraordinaire

DAVID P. MOWRY

This article is classified TOP SECRET CODEWORD in its entirety because the sources from which it was derived are all so classified.

It weighed one and three-quarter pounds and was spring-driven. According to German authorities, it was at least as secure as the Enigma. The Germans intended to have 1,000 available by October 1945 and to mass-produce 10,000 per month by January 1946. The Schlüsselkasten, or Cipher Box, would have replaced the Enigma below the level of division. If it had been introduced in 1942, while the German star was in the ascendant, it could have changed the course of the war. Nineteen forty-five was, of course, too late. In 1942, the resulting loss of intelligence to the Allies would have affected the outcome of the North African campaign and the Battle of the Atlantic, as well as subsequent campaigns. The inventor of the Schlüsselkasten, and other cipher devices, was Regierungs-Oberinspektor Fritz Menzer, of OKW/Chi, the Cryptologic Section of the German Army High Command.[1]

THE CAREER OF OBERINSPEKTOR MENZER

Ostwin Fritz Menzer was born 6 April 1908 in the village of Herrndorf in Saxony, the youngest of four children of a small businessman. After completing elementary school and an apprenticeship as a toolmaker, he enlisted in the Reichswehr in 1926 as a mechanic and was assigned to a motor battalion in Leipzig.[2]

Menzer had already developed an interest in cryptography and was granted his first patent in 1934, for a "combined measuring apparatus for angles and lengths, the data [from which was] expressed in an enciphered form in a four-place combination of letters." Based on his work on this device, he was permitted to attend a course for radio technicians at the Army Signal School. In May 1935 he was transferred to OKW/Chi to further develop his invention. Here he received his first formal training in cryptanalysis under the instruction of Ministerial Director Wilhelm Fenner.[3]

A year later, he had developed two methods for solving Hagelin C-36 encipherment and had developed an analytical method for the solution of the German Army Enigma. As a result, Menzer was ordered to establish a section in OKW/Chi to test foreign cryptosystems, to develop and test the security of German cryptosystems, and to construct cryptanalytic aids. Thus, at the age of 28, Menzer became the chief of communications security for the German Army. In his curriculum vitae, Menzer notes, "Since the troops and their command, because of their ignorance of the scientific status of cryptanalytic methods, regarded encipherment as a drag on modern communications technique, I often had to overcome great difficulties to put through my ideas." During this period, 1935 to 1938, Menzer also attended a special school for administration and economics.[4]

Menzer's enlistment expired on 31 May 1938, and he was discharged from active duty with the rank of Senior Radio Technician. He "converted" to civilian status, retaining his position. On 1 April 1940, he was promoted to the rank of Superior Government Inspector. Early in 1942, because of the increased requirements for long-range communications and because of increased emphasis on cryptosecurity, Menzer's section was broken up into three functional subsections. The Armed Forces, in general, had always been able

to submit their cryptosystems to OKW/Chi for evaluation, but had not been required to do so. Until October 1943, when Keitel, Chief of the OKW, issued an order specifying that no new ciphers could be introduced by any branch of the Armed Forces or government agency without prior approval by OKW/Chi, only the Abwehr (Military Intelligence) had done so. In 1942, after the breakup of Menzer's section, Admiral Canaris, the Chief of the Abwehr, charged Menzer with testing the security of Abwehr cryptosystems.[5]

Menzer found the Abwehr's systems to be depressingly inadequate, and in the summer of 1943, revamped all of the Abwehr hand systems then in use. He introduced the "ABC Schlüssel," "Procedure 62," and "Procedure 40," all of which were double transposition-substitution systems; and the Schlüsselrad, or Cipher Wheel, a hand operated autoclave, i.e., self-generating key cipher device.[6]

From April 1942 on, Menzer worked for the Abwehr as Technical Consultant in Cryptography. In this position, he traveled extensively on inspection trips and lectured officers and men on the principles of communications security. Late in the war his section was moved from Berlin to Werfen, Austria, where, on 8 May 1945, he was taken prisoner by the American forces and interned at Camp Heufeld near Munich. He was released on 17 June and went to Leipzig. On 22 September he transferred his residence from Berlin to Zschopau in Saxony, the Russian Zone. He was hired as a technical teacher for metal classes at the City Industrial School of Zschopau in January 1946. In November he was dismissed, because as a former member of the Wehrmacht, he was not eligible for a teaching position. He then established his own business in Zschopau, a workshop that employed seriously disabled veterans in the making of ladies' brooches.[7]

AFTER THE WAR

In early July 1947, the headquarters of the U.S. 7707 European Command Intelligence Center (ECIC) began trying to arrange to interrogate Menzer regarding his cryptographic work during the war. It was known that he sometimes visited Berlin, and an attempt was made to persuade him to come there for a two-week stay. At this point, Menzer's life began to resemble an Eric Ambler spy story.

Menzer's father-in-law and several neighbors were arrested by the Russians on 20 August, while Menzer and his family were on holiday. A man named Uhlig, who had worked with Menzer in OKW/Chi, contacted Menzer and told him that he (Uhlig) was supposed to induce Menzer to come to the American Zone. In the meantime, the 7707 ECIC had been informed, without Menzer's knowledge, that Menzer was living in difficult conditions in the Russian Zone and that he would insist on the transfer of himself, his family, and a "personal friend" (apparently Uhlig) to the American Zone.

According to a later statement by Menzer, Uhlig was a Soviet agent and was probably the person who had started the rumor that Menzer was in difficulty. In any case, Menzer considered the entire affair to be "preposterous" but finally agreed to meet with the Americans in Berlin on 8 September. Menzer went to Berlin and was flown to Oberursel with an American intelligence officer, Uhlig, and two other Germans.[8]

In Oberursel, Menzer became very suspicious of Uhlig, particularly after he found out that Uhlig had told the Americans that he could go back to Zschopau and remove Menzer's furniture to the West. Feeling very dissatisfied with the whole situation, Menzer left Oberursel on his own on 12 September and returned to Zschopau. On 20 September, a message was brought to Menzer's home informing him that the President of the Chamber of Industry and Commerce wanted to speak to him at the Town Hall. When he arrived for the meeting, Menzer was arrested by the Russians and taken to the prison in Dresden.

F

In Dresden, Menzer was interrogate
wanted to know the details of his mee
Uhlig, who had requested this of him a

Menzer was held in solitary confiner
but, apparently, not mistreated. It was
Uhlig was a Soviet agent and that the
(Menzer) to escape to the West thro
establish Uhlig's bona fides and secure

Finally, on 13 March 1948, Menzer
a spy for the Russians. He was orderec
of Uhlig's willingness to work for the
truthfully on his contacts with Uhlig.
had no interest in moving to the Wes
that he was being watched closely and
Another factor causing him to delay
before fleeing. In April 1949 he had m
his family fled to West Berlin, where
removed to West Germany in June
documents until 1951.[11]

MENZER'S INVENTIONS

During Menzer's service with OKW,
for a number of advances in the science
was to adapt the use of Hagelin pin
cryptoequipment.

The two major types of cryptoequi
were the Enigma and machines made
stepped once with each encipherment
"length" wheels. In the Enigma, moti
the starting point of the cycle on each
such motions unpredictable.

The Luckenfüllerwalze. Normal Er
respect to the rotor) ring with a sing
blocking wheel which regulated the dri
reading position, the next subordinate
Luckenfüllerwalze, the notch ring was
which could be filled in to make them
subordinate rotor.[12]

The Schlüsselgerät 39. Invented b
coupled three Hagelin pin wheels with
the rotors. All three wheels stepped
according to normal Enigma rules, exce
wheel prevented the coupled rotor fro
$26^3 = 17{,}576$ characters. When set u
Schlüsselgerät 39 had a cycle length of
as the cycle length of the unmodified E

The Schlüsselgerät 39 was fully aut
plain and cipher letters were printed
groups.

ation, but had not been required to do
OKW, issued an order specifying that
of the Armed Forces or government
he Abwehr (Military Intelligence) had
ion, Admiral Canaris, the Chief of the
Abwehr cryptosystems.[5]
singly inadequate, and in the summer
then in use. He introduced the "ABC
ll of which were double transposition-
r Wheel, a hand operated autoclave,

Abwehr as Technical Consultant in
vely on inspection trips and lectured
s security. Late in the war his section
n 8 May 1945, he was taken prisoner
ld near Munich. He was released on
ansferred his residence from Berlin to
ired as a technical teacher for metal
January 1946. In November he was
hrmacht, he was not eligible for a
iness in Zschopau, a workshop that
ladies' brooches.[7]

707 European Command Intelligence
Menzer regarding his cryptographic
es visited Berlin, and an attempt was
k stay. At this point, Menzer's life

re arrested by the Russians on 20
lay. A man named Uhlig, who had
r and told him that he (Uhlig) was
n Zone. In the meantime, the 7707
ge, that Menzer was living in difficult
nsist on the transfer of himself, his
the American Zone.
was a Soviet agent and was probably
as in difficulty. In any case, Menzer
ut finally agreed to meet with the
o Berlin and was flown to Oberursel
other Germans.[8]
hlig, particularly after he found out
go back to Zschopau and remove
ed with the whole situation, Menzer
ned to Zschopau. On 20 September,
m that the President of the Chamber
the Town Hall. When he arrived for
taken to the prison in Dresden.

In Dresden, Menzer was interrogated initially by 20 Russian officers in uniform, who wanted to know the details of his meetings with the Americans. Omitting any mention of Uhlig, who had requested this of him at Oberursel, Menzer described what had happened.[9]

Menzer was held in solitary confinement for six months and was frequently interrogated but, apparently, not mistreated. It was while in prison that Menzer became convinced that Uhlig was a Soviet agent and that the entire situation was a set-up designed to get him (Menzer) to escape to the West through Uhlig's good offices and with Uhlig, thus to establish Uhlig's bona fides and secure a good job for him with American intelligence.[10]

Finally, on 13 March 1948, Menzer was released, after signing an agreement to work as a spy for the Russians. He was ordered to spy on Uhlig, apparently to continue the fiction of Uhlig's willingness to work for the Americans. Menzer did so, reporting dutifully and truthfully on his contacts with Uhlig. When the charade had started, in 1947, Menzer had had no interest in moving to the West. His attitude had now changed. However, he felt that he was being watched closely and decided to wait for a more favorable opportunity. Another factor causing him to delay was the fact that he wanted to clear up his debts before fleeing. In April 1949 he had met all of his financial obligations and in May he and his family fled to West Berlin, where he surrendered to American authorities. He was removed to West Germany in June 1948. He continued to be mentioned in documents until 1951.[11]

MENZER'S INVENTIONS

During Menzer's service with OKW/Chi and the Abwehr (1935–45), 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. In the latter, all wheels stepped once with each encipherment; the cycle was extended by the use of different "length" wheels. In the Enigma, motion was odometer-type, with the only variation being the starting point of the cycle on each rotor. Menzer's inventions were designed to make such motions unpredictable.

The Luckenfüllerwalze. Normal Enigma rotors had on the left side a movable (with respect to the rotor) ring with a single drive notch, and on the right a fixed 26-notch blocking wheel which regulated the drive. When the drive notch on one rotor reached the reading position, the next subordinate rotor would advance one position. In Menzer's Luckenfüllerwalze, the notch ring was fixed on the rotor and had 26 drive notches, any of which could be filled in to make them inactive, thus providing for irregular stepping of the subordinate rotor.[12]

The Schlüsselgerät 39. Invented by Menzer in 1939, this development of Enigma coupled three Hagelin pin wheels with the Enigma rotors to provide variable stepping of the rotors. All three wheels stepped once with each encipherment. Rotors stepped according to normal Enigma rules, except that an active pin at the reading station for a pin wheel prevented the coupled rotor from stepping. The cycle for an unmodified Enigma is $26^3 = 17{,}576$ characters. When set up in accordance with Menzer's instructions, the Schlüsselgerät 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.

The Schlüsselgerät 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 five-letter groups.

Because of constant technical improvements on the part of the Ordnance Department, development of the Schlüsselgerät 39 was not completed until 1944.[13]

The Schlüsselgerät 41. This mechanical cipher machine, invented in 1941, was based on Hagelin encipherment but included a mechanism for variably stepping the Hagelin wheels.

The Schlüsselgerät 41 had six pin wheels which were mutually prime. The first five of these wheels had kicks of 1, 2, 4, 8, and 10 respectively. The sixth wheel made these kicks positive or negative.

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

1. This 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 which was the sum of all the kicks of wheels which had active pins in the "kick index position." 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 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.[14]

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 encipherment. As a result of the keyboard operation, he was able to redesign the arrangement of letters on the print wheels to flatten the cipher frequency count.

Because of the wartime shortages of aluminum and magnesium, the machine ended up weighing between 12 and 15 kilograms, 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.[15]

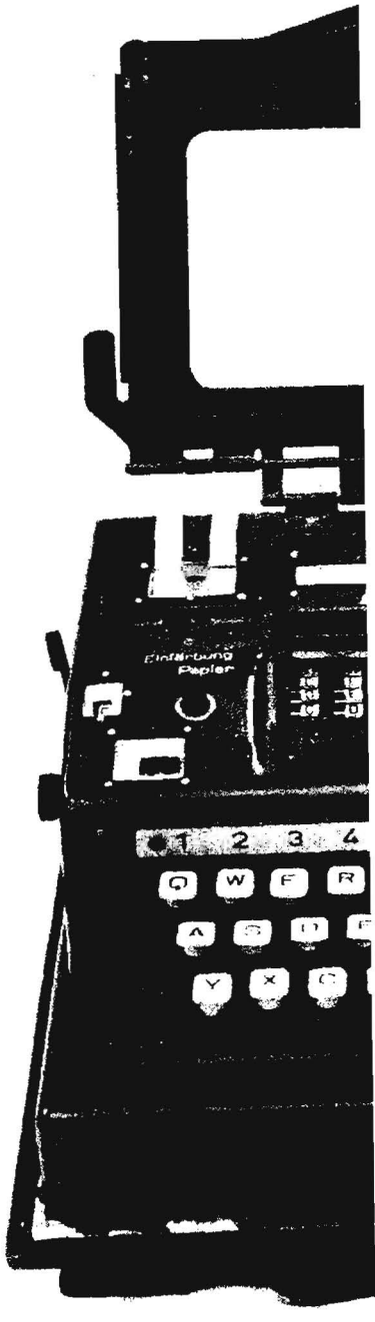
attack. In 1947, Frank Lewis, in WDGAS-71, stated that if a mechanically reliable machine could be built embodying the same principles as the Schlüsselgerät 41, it would undoubtedly be a valuable asset. He noted that, because of the key complementing characteristic of the machine, statistical tests did not seem to offer any particular promise for solution.[16]

The Schlüsselkasten. The Cipher Box was a mechanical cipher device making use of the principles of sliding strips. Basically, it was a three-quarter pound aluminum box containing three Hagelin pin wheels and a coil spring which determined the stepping of a sliding strip or "slide rule" on the top of the box.

Two alphabets were written on the slide rule, 13 characters of each on the fixed base, and 13 characters of each on the top and bottom of the sliding strip. The latter were so written 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 A_1A_2 the pins were all inactive, the slide stopped and encipherment

(Text continued on page 30)



EO 1.4.(b) EO 1.4.(c)

Fig. 1. S

ıe part of the Ordnance Department,
:ted until 1944.[13]
:hine, invented in 1941, was based on
variably stepping the Hagelin wheels.
vere mutually prime. The first five of
/ely. The sixth wheel made these kicks

consisted of three elements:

ıad an active pin in the "motion index
lowing occurred: Wheel 1 moved one
tep unless the wheel to its left had an
case it would move two steps.

of all the kicks of wheels which had
, the sixth wheel had an active pin in
minus the sum of all the other kicks.
vould complement itself.
urred whether or not Wheel 6 had an
ep, Wheel 6 also stepped one or two

durable machine to be used by units
a cipher tape and to be keyboard
rment. As a result of the keyboard
letters on the print wheels to flatten

l magnesium, the machine ended up
field use. Removal of the keyboard
of the print wheels prevented their
ıed because no one knew what to do.
:se were distributed to the Abwehr,

ıat if a mechanically reliable machine
ılüsselgerät 41, it would undoubtedly
complementing characteristic of the
icular promise for solution.[16]
nical cipher device making use of the
rter pound aluminum box containing
mined the stepping of a sliding strip

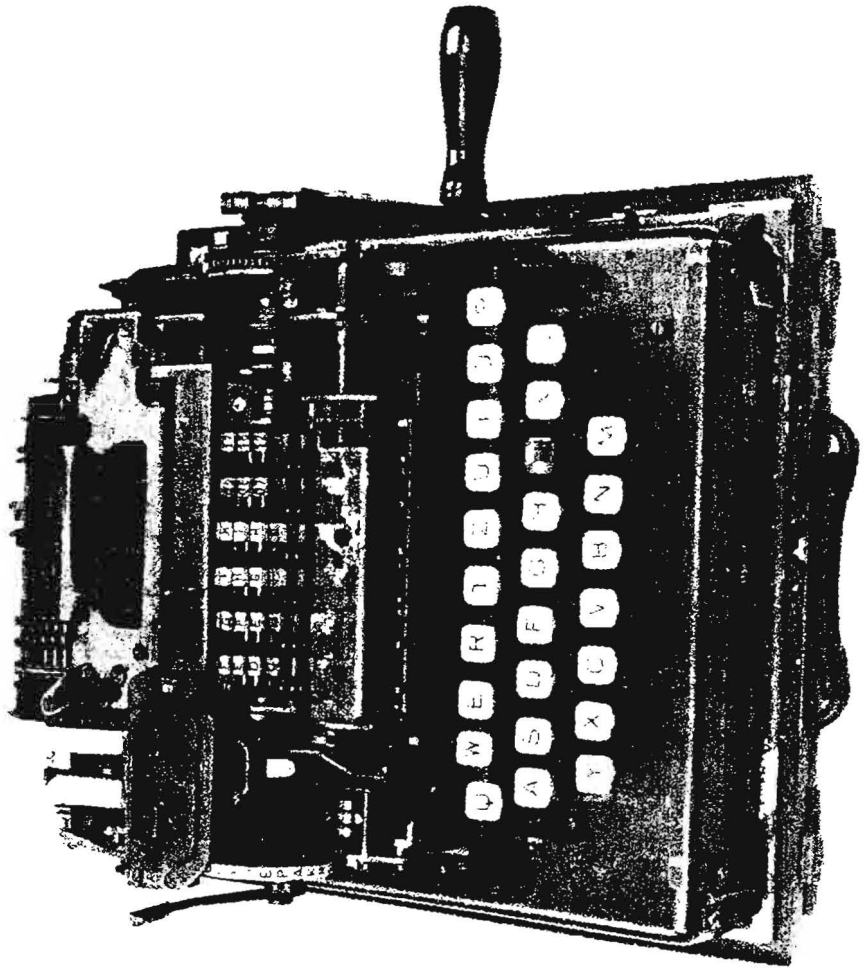
haracters of each on the fixed base,
the sliding strip. The latter were so
Alphabets could be changed as often

pped, winding the spring that drove
move left. When at either or both of
the slide stopped and encipherment

(Text continued on page 30)

Fig. 1. Schlüsselgerät 41. Ready for use.

EO 1.4.(c) EO 1.4.(b)



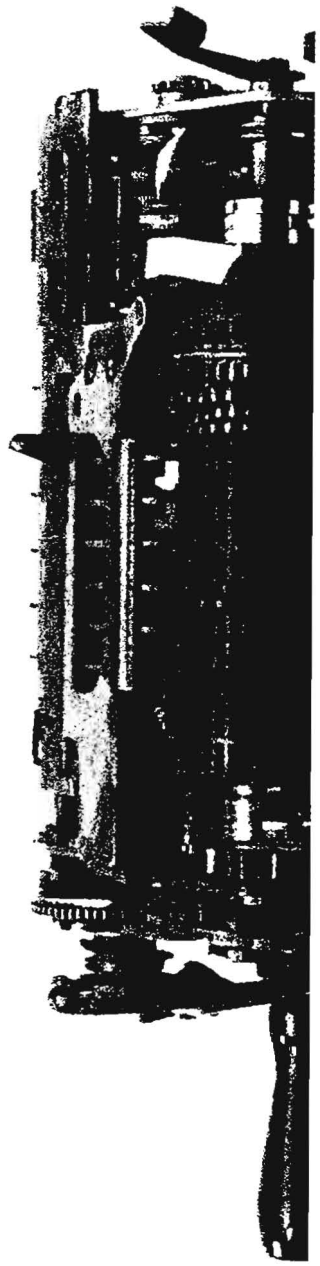


Fig. 2. Schlüsselgerat 41. Ease of maintenance was not a strong point of the SG-41. Removal of the cover involved removing all external knobs and cranks and then undoing six screws.

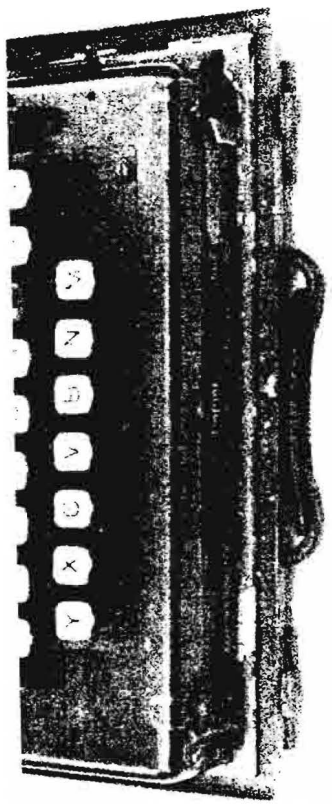


Fig. 2. Schlüsselgerät 41. Ease of maintenance was not a strong point of the SG-41. Removal of the cover involved removing all external knobs and cranks and then undoing six screws.

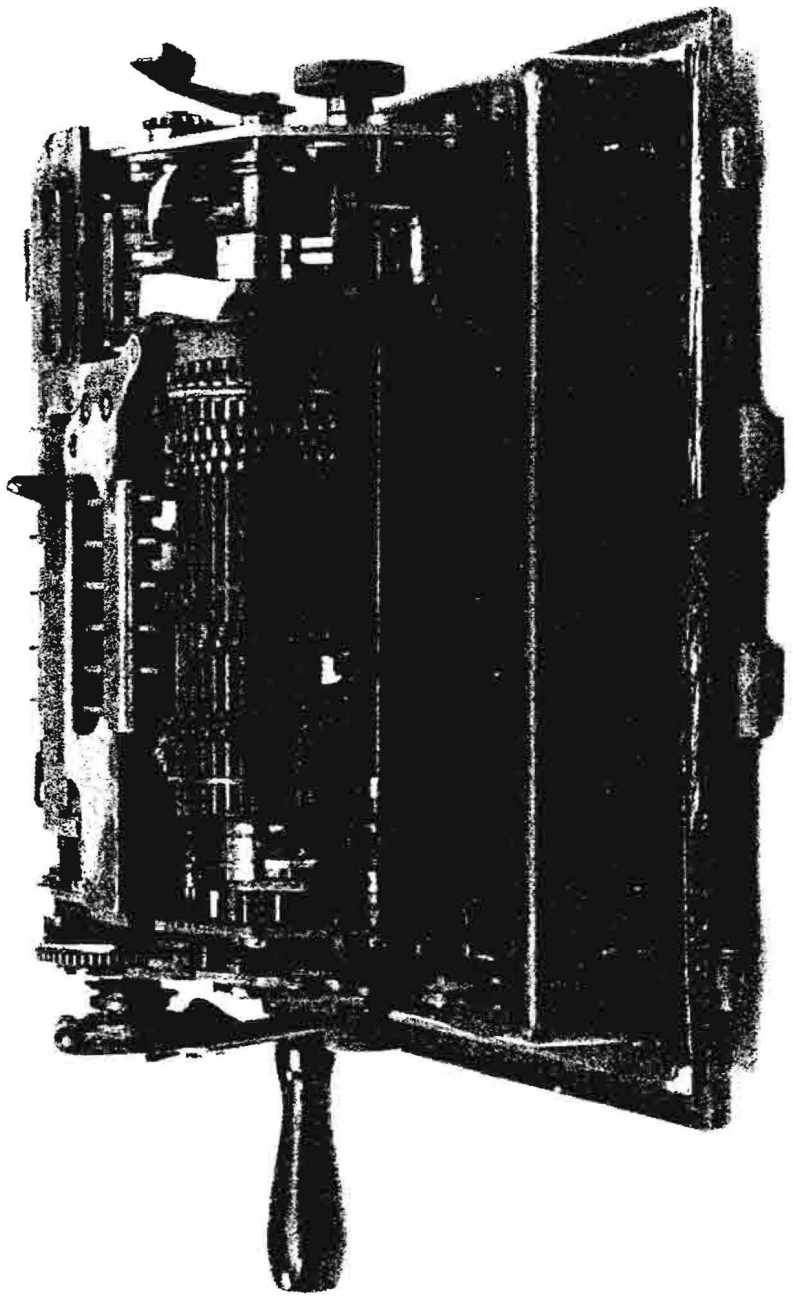


Fig. 3. Schlüsselgerät 41. Rear view.

Schlüsselkasten (figs. 4 and 5). These models, made by Fritz Menzer, were devised to illustrate certain aspects of the working of the Schlüsselkasten. No actual working models of this device are available.

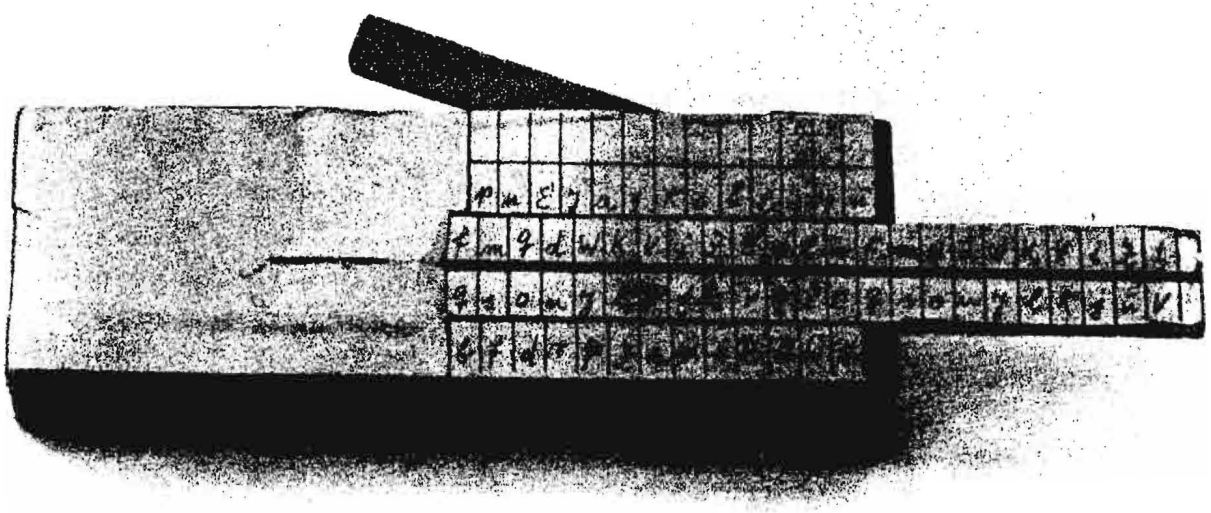


Fig. 4. Wooden model, presumably the same size as the actual device, demonstrating the movement of the "slide rule."

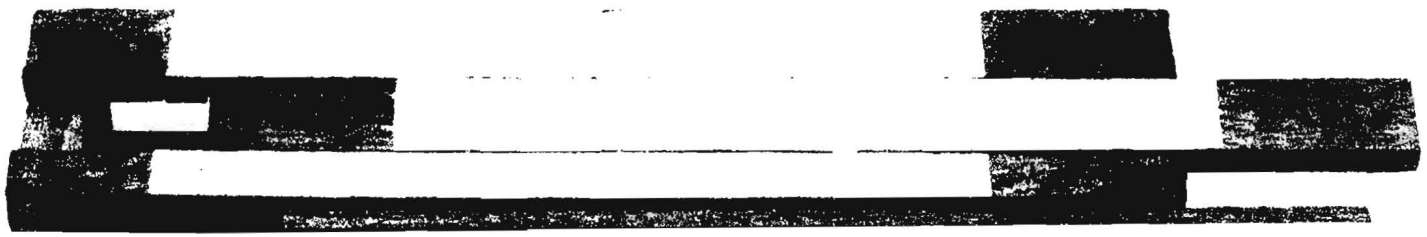


Fig. 4. Wooden model, presumably the same size as the actual device, demonstrating the movement of the "slide rule."

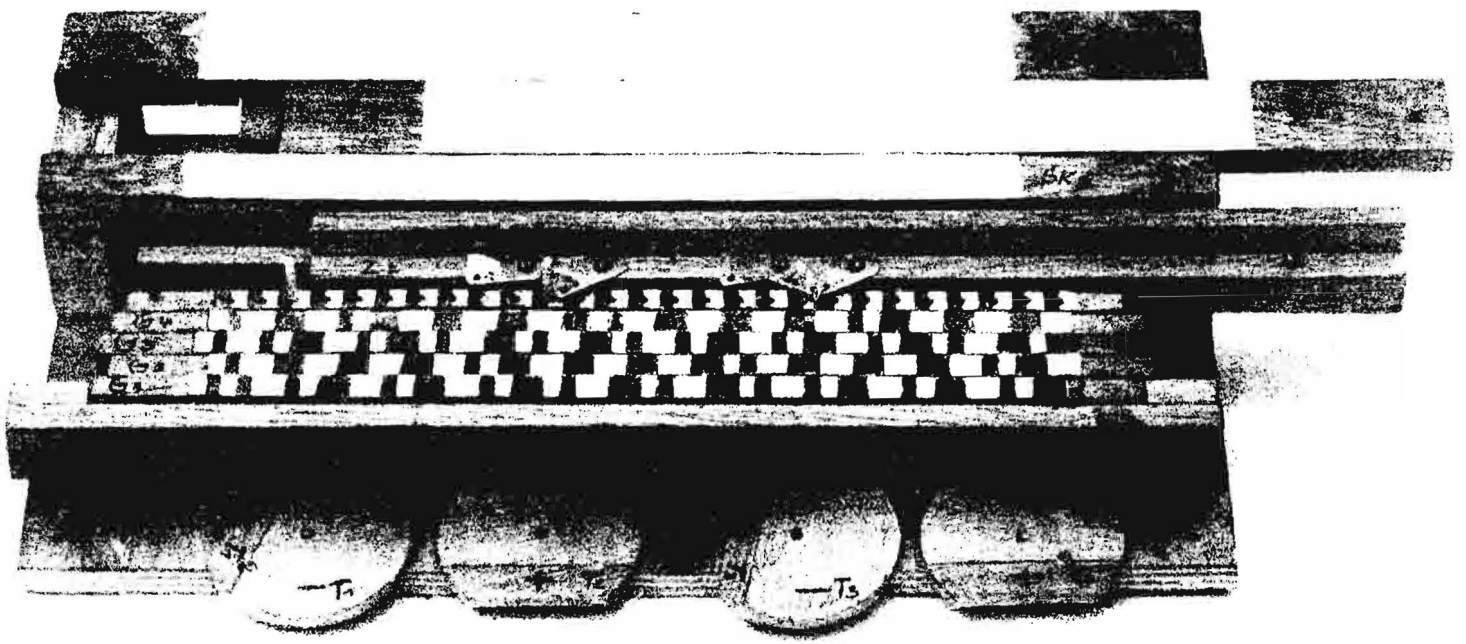


Fig. 5. Wooden model powered with elastic bands demonstrating the rules of motion in the device. The disks, T1–T4, represent slip wheels which affect the relative positioning of the four pin wheels, G1–G4. The black and white squares represent active and inactive pins. Dowels are inserted in the holes corresponding to positions where all holes are active or all inactive, and Z1 and Z2 are pulled to the right and released. Each time one of the four metal slips on Z2 encounters a dowel, the mechanism will stop and a cipher value may be read off of SK1 or SK3.

took place. If the step came from A_2 alone or A_1 and A_2 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 strip to slide left to its next stop. As mentioned at the beginning of this article, the Germans intended to replace many Enigmas with the Schlüsselkasten. The device had a fairly high degree of security, as might be expected from a sliding strip system with irregular movement. Given the alphabets on the slide rule, it was possible to recover the pin patterns with a crib of about 30 letters. Without the crib, however, computer assistance would have been necessary; and large quantities of cipher would have been required to recover the alphabets. A modification was considered in which two 26-character alphabets were slid against one another, rather than the 13-character segments. This would have increased the device's security, since more text would have been required to recover the alphabets. It would, however, have simplified recovery of the pin pattern after alphabet recovery. In any case, solution of a single message was most unlikely.[17]

The Schlüsselscheibe. The Schlüsselscheibe was designed by Menzer for use by clandestine agents. The operating principle was similar to that of the Schlüsselkasten. In the case of the Schlüsselscheibe, three resettable but permanently notched wheels were used. For encipherment, the inner disk was rotated to wind the spring. Pressing the key would then release the inner disk and allow it to rotate until stopped by the notch rings. If the inner disk stopped in a position where its letters were in phase with those of the outer disk, the cipher value would be read directly. If the stop was in an intermediate position, the number of the line opposite the plain value would be read, and the cipher value taken from the cell with that number.[18]

The Schlüsselrad. The Schlüsselrad was a hand-operated cipher device designed for agent use. It was made up of two disks. The lower disk had 52 notches or holes around its edge, into which a pencil or stylus could be inserted to turn the disk. On the face of the disk were 52 cells into which a keyword-mixed alphabet could be inscribed twice, clockwise. The upper disk had a direct standard alphabet inscribed clockwise on one-half of its periphery, next to a semicircular window that, when the two disks were assembled concentrically, revealed 26 characters of the mixed sequence on the lower disk. The upper disk also had a notch cut into its edge which exposed ten of the holes on the lower disk. This notch had the digits 0 to 9 inscribed next to it, in a counterclockwise direction so that when the exposed holes were lined up with the numbers, the letters on the lower disk were lined up with the letters on the upper disk.

Various methods of key generation were used. On Chilean links, an 11-letter key word was numbered as for a transposition key, with the first digit of two-digit numbers dropped. This key was extended by appending a two-digit group count and a four-digit time group:

A N T O F O G A S T A
1 6 0 7 4 8 5 2 9 1 3 12 1440

On other links, a Fibonacci sequence of 100–125 digits would be generated through various manipulations of the date, time, and a secret number. If a message were longer than the key, it would be reversed as many times as necessary. Key generation tables were also used.

In use, the key constituted the input to an autoclave. After aligning the alphabets according to a prearranged system or according to an indicator in the message, a stylus was inserted in the hole corresponding to the first key digit, and the lower disk was rotated clockwise until the stylus was stopped by the end of the notch. The plain text letter was then found on the upper disk and its cipher value read off of the lower disk. The stylus

(Text continued on page 35)

Schlüsselscheibe (figs. 6, 7, 8, and 9). T
captured by the Russians to illustrate t

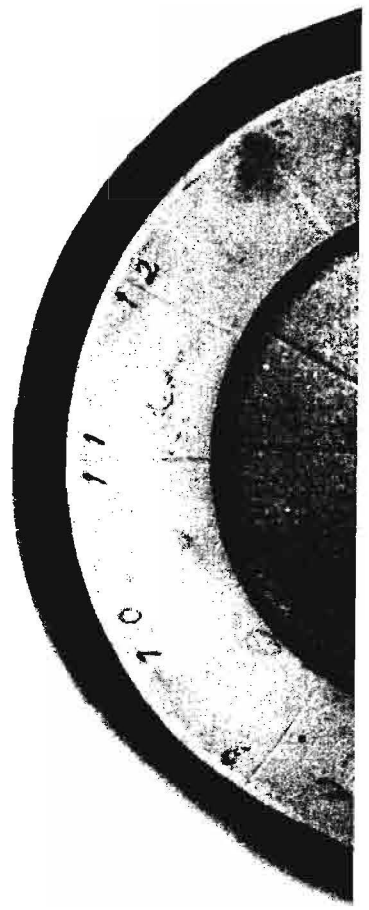


Fig. 6. Bakelite and aluminum model
cipher disk when the control lever (alig

Schlüsselscheibe (figs. 6, 7, 8, and 9). These models were also made by Fritz Menzer. All working models were captured by the Russians to illustrate the operation of the device to Allied authorities.

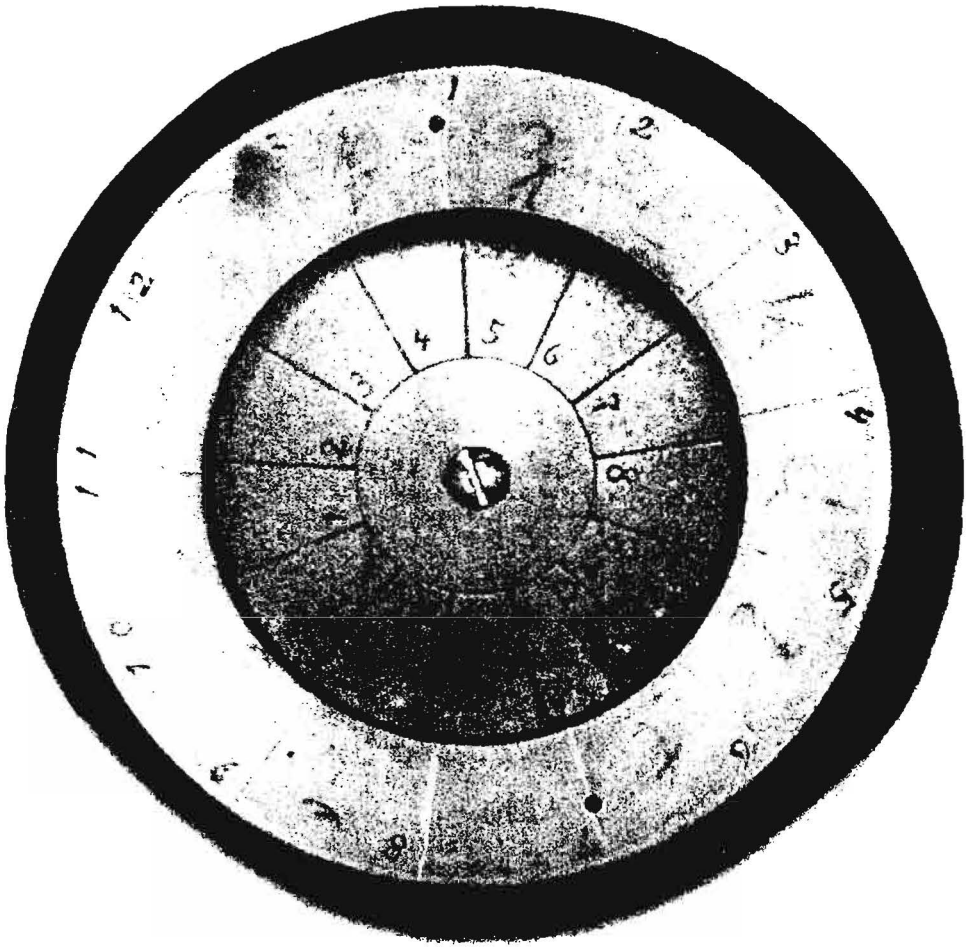


Fig. 6. Bakelite and aluminum model powered with a rubber band. Demonstrates the movement of the central cipher disk when the control lever (aligned with line 10 in the photograph) is pressed.

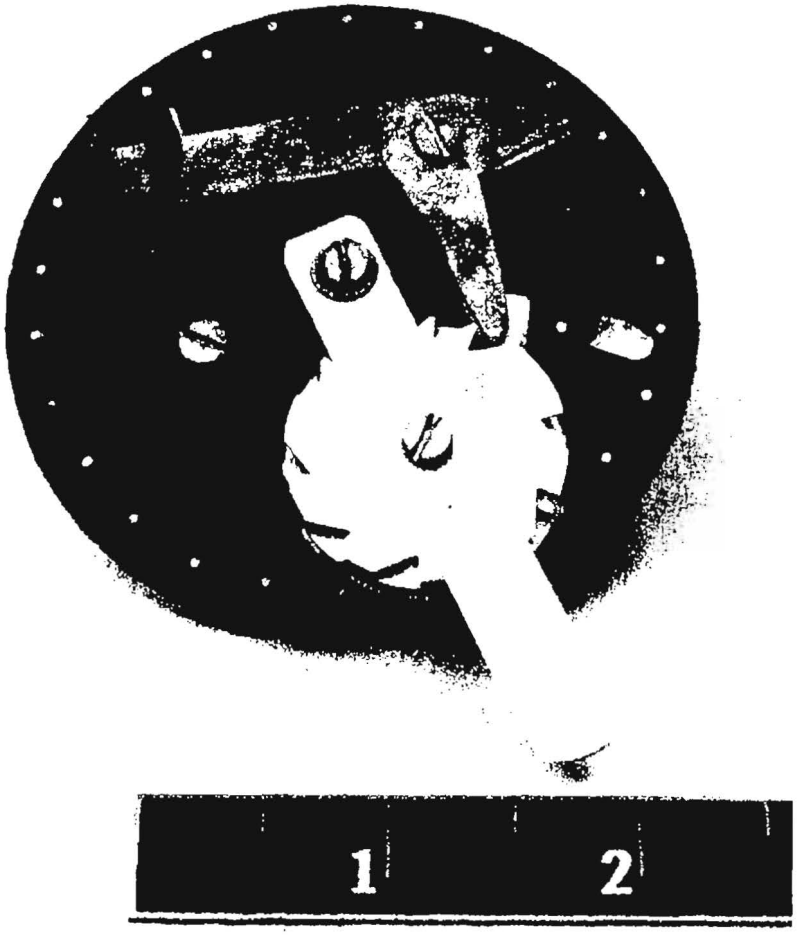


Fig. 7. Bakelite and aluminum model illustrating internal cam and notch wheel operation.

Fig. 8. Bras

ıternal cam and notch wheel operation.

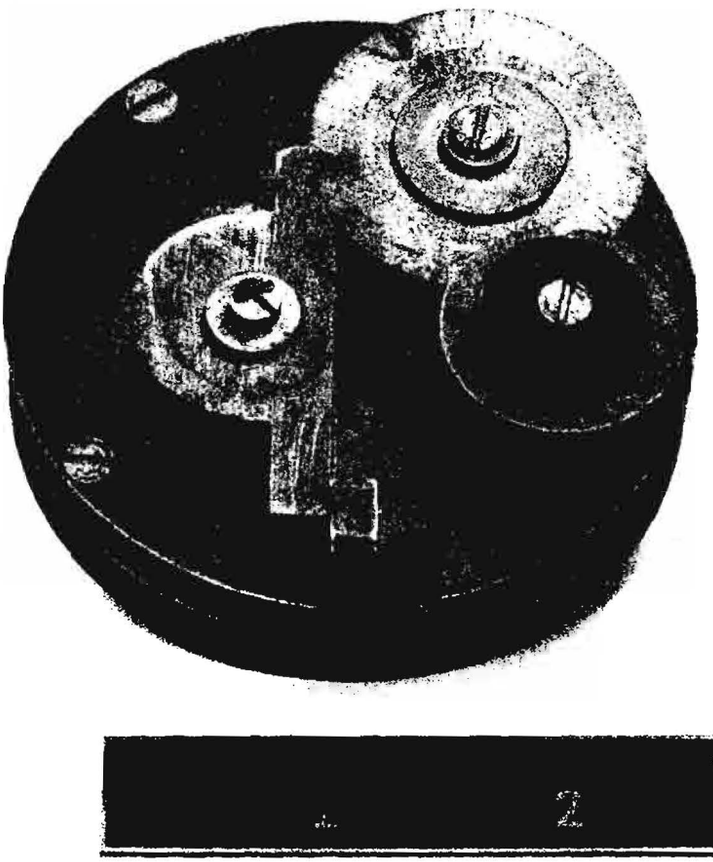


Fig. 8. Brass model showing cam and lever operation.

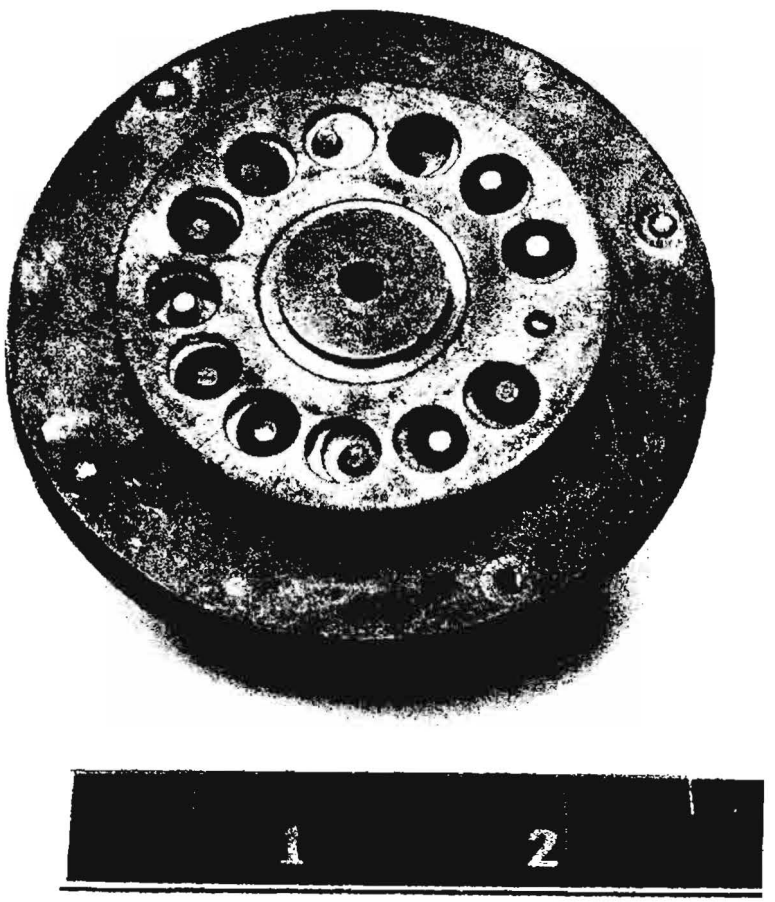


Fig. 9. Reverse of figure 8, showing slip wheels.

was then placed in the hole cor
procedure was repeated for the sec
cipher was equal to the sum of all

IF

If Menzer's devices had been in
certainly have complicated the A
toward solution of Enigma traffic f
been able to read German traffic.
higher echelon communications, a
found to solve Menzer's devices. E
to the British in 1939, when they
GC&CS.

Who knows? If the introductio
unwieldy bureaucracy, maybe Fritz

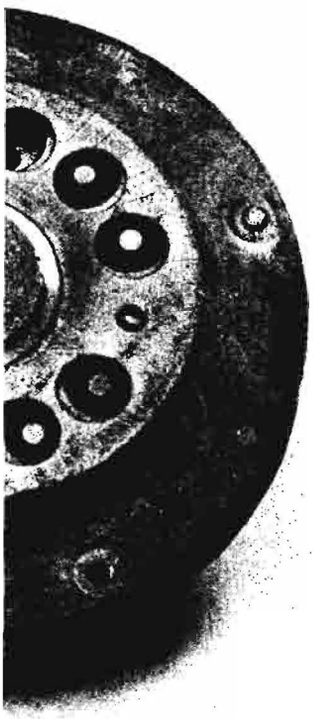
was then placed in the hole corresponding to the second digit of key, and the same procedure was repeated for the second letter of text. Thus, the true key at any point in the cipher was equal to the sum of all the previous key inputs (mod 26).[19]

IF

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 we 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 we would have lost the edge that the Poles presented to the British in 1939, when they turned over the results of their analysis of the Enigma to GC&CS.

Who knows? If the introduction of his inventions had not been slowed down by an unwieldy bureaucracy, maybe Fritz could have won the war!

EO 1.4.(c)



owing slip wheels.

~~(S-CCO)~~ Since September 1981, Mr. Mowry has served as a historian in T542, researching and writing a history of [redacted] recently published in the Cryptologic History Series. He began his Agency career as a Turkish linguist in 1957 and later (1964–69) held an [redacted] position as [redacted] From 1969 through 1981 he served in various technical and managerial positions in the [redacted] Division. Mr. Mowry holds a BA with regional group major in Germany and Central Europe from the University of California at Berkeley and is certified as a Cryptanalyst, Linguist, and Cryptologist.

EO 1.4.(c)

EO 1.4.(c)

NOTES

[1] 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, p. 30.

[2] 79/49/TOPSEC/AS-14 [redacted] "Description of Contacts of Fritz Menzer with American and Soviet Authorities and Summary of Career," p. 16.

[3] Ibid., pp. 16–17.

[4] Ibid., p. 17.

[5] Ibid., pp. 17, 18, and 21; and WDGAS-14, op. cit., Vol. 3, pp. 18–20.

[6] Ibid., p. 21, and *The History of Coast Guard Unit 387*, pp. 156–211.

[7] 79/49/TOPSEC/AS-14, op. cit., pp. 21–22.

[8] Ibid., pp. a, b, and 6–7.

[9] Ibid., p. 9.

[10] Ibid., p. 10.

[11] Ibid., pp. 2, 4–15, and 22–23.

[12] Ibid., p. 18; WDGAS-14, op. cit., pp. 22–23; and DF-174C, 11/50/TOPSEC/AFSA-14, "Remarks by Menzer on Various German Cryptographic Devices." January 1950, pp. 1–2.

[13] 79/49/TOPSEC/AS-14, op. cit., p. 19; and 115/49/TOPSEC/AS-14, [redacted] "Four Papers by Fritz Menzer," December 1949.

[14] WDGAS-14, Vol. 2, op. cit., p. 29.

[15] "Report on SG 41 by Wilhelm Buggisch," 30 August 1945.

[16] Memorandum from Frank W. Lewis, WDGAS-71, to Colonel Solomon Kullback, WDGAS-70, "Study of the C-41 Cipher Device," 4 March 1947; [redacted] and DF-19, "Cipher Device-41," 10 January 1944.

[17] 79/49/TOPSEC/AS-14, op. cit., pp. 31–32; 32/51/TOPSEC/AFSA-14, R-1, "Schlüsselkasten 50," May 1951; and an undated, unsigned paper, "Study of 'Schlüsselkasten'," in Folder S-14, 340 of the NSA Cryptologic Collection.

[18] 79/49/TOPSEC/AS-14, op. cit., p. 33; and 33/51/TOPSEC/AFSA-14, R-2, "Schlüsselscheibe 50," May 1951.

[19] [redacted]

EO 1.4.(c)

EO 1.4.(b)

[redacted]