THE COMMERCIAL ENIGMA: BEGINNINGS OF MACHINE CRYPTOGRAPHY

Louis Kruh[1] and Cipher Deavours[2]

ADDRESS: (1) 17 Alfred Road West, Merrick NY 11566 USA (2) Department of Mathematics, Kean University of New Jersey, Union NJ 07083 USA.

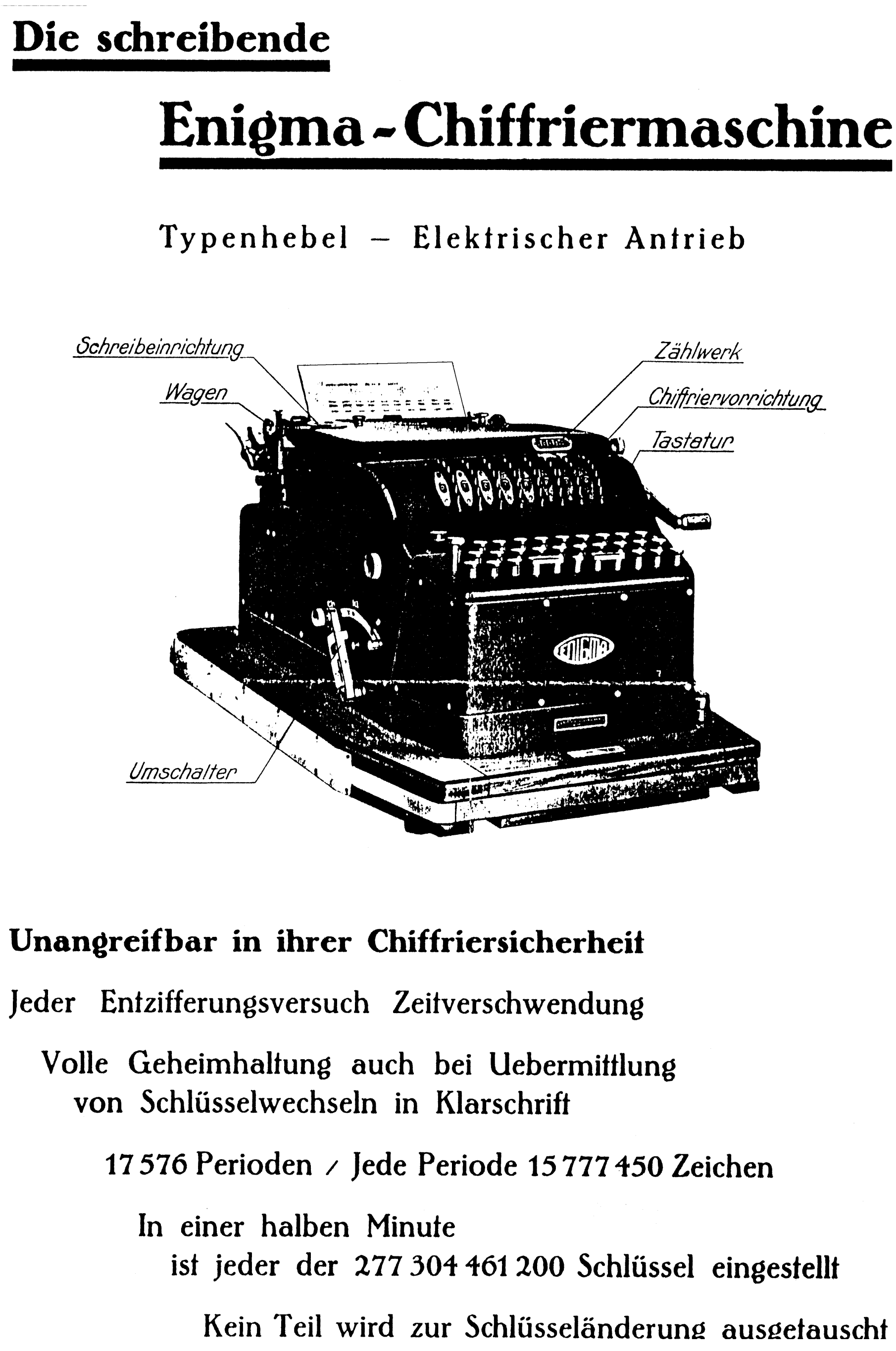
ABSTRACT: A brief history and description of the first four models of the Enigma cipher machine, designed for the commercial market, taken in part from the authors' book [1].

KEYWORDS: Arthur Scherbius, ciphering typewriter, wired codewheel, rotors, *Umkerwalze*, reflecting principle, Hugo Koch, Model A, Model B, Model C, Model D, ratchet wheel notch, wiring, *Chiffrienmaschinen AG*.

Within a three-year period, four inventors in four different countries came up with the idea of using a rotor or wired codewheel to scramble letters in a cipher machine. They were Edward H. Hebern, United States, 1917; Arthur Scherbius, Germany, 1918, Hugo Alexander Koch, Netherlands, 1919; Arvid Gerhard Damm, Sweden, 1919. None was financially successful but Scherbius, who called his machine Enigma, was responsible for introducing several models of what eventually became the best known cipher machine in the world.

In 1918, Scherbius, an electrical engineer, and E. Richard Ritter, a certified engineer, founded the firm of Scherbius and Ritter and tried to interest the Imperial German Navy in its cipher machine. The naval staff found the machine provided good security but felt that current traffic did not make it worthwhile. Following a suggestion from the naval staff, Scherbius approached the Foreign Office to consider it for diplomatic correspondence but there was no interest. Subsequently Scherbius and Ritter transferred the cipher patent rights to the Gewerkschaft Securitas. On July 9, 1923, Securitas founded the Chiffriermaschinen Aktien-Gesellschaft (Cipher Machines Stock Corporation). Scherbius and Ritter were on its board of directors.

The corporation promoted an early model of its cipher machine with a two-page flier. (Figure 1A and Figure 1B) It also exhibited the Enigma at the 1923 Congress of the International Postal Union in Bern, Switzerland. This was Model A of what was to be a long line of Enigma variations. The machine was heavy and



Die schreibende

Enigma - Chiffriermaschine

Typenhebel – Elektrischer Antrieb

Schreibeinrichtung
Wagen
Zählwerk
Chiffriervorrichtung
Tastatur
Umschalter

Unangreifbar in ihrer Chiffriersicherheit

Jeder Entzifferungsversuch Zeitverschwendung

Volle Geheimhaltung auch bei Uebermittlung
von Schlüsselwechseln in Klarschrift

17 576 Perioden / Jede Periode 15 777 450 Zeichen

In einer halben Minute
ist jeder der 277 304 461 200 Schlüssel eingestellt

Kein Teil wird zur Schlüsseländerung ausgetauscht

Figure 1A. First page of two page flier promoting Enigma.

bulky, bearing a standard typewriter keyboard for input. In fact, the machine could be used as a regular typewriter, even in the middle of ciphering text, if desired. Enigma A (Figure 3 and Figure 4) followed closely the original Scherbius patent in construction, and consisted of four rotors which were driven by four geared wheels. These four drive wheels each drove one rotor and were gapped in their number of teeth. They revolved in regular fashion with periods of 11, 15, 17, and 19. The 11th wheel had only five teeth with the other six positions being gaps. The 15th wheel had nine teeth and six gaps, while the 17th and 19th wheels each had 11 teeth with six and eight gaps, respectively.

English Translation of Figure 1A

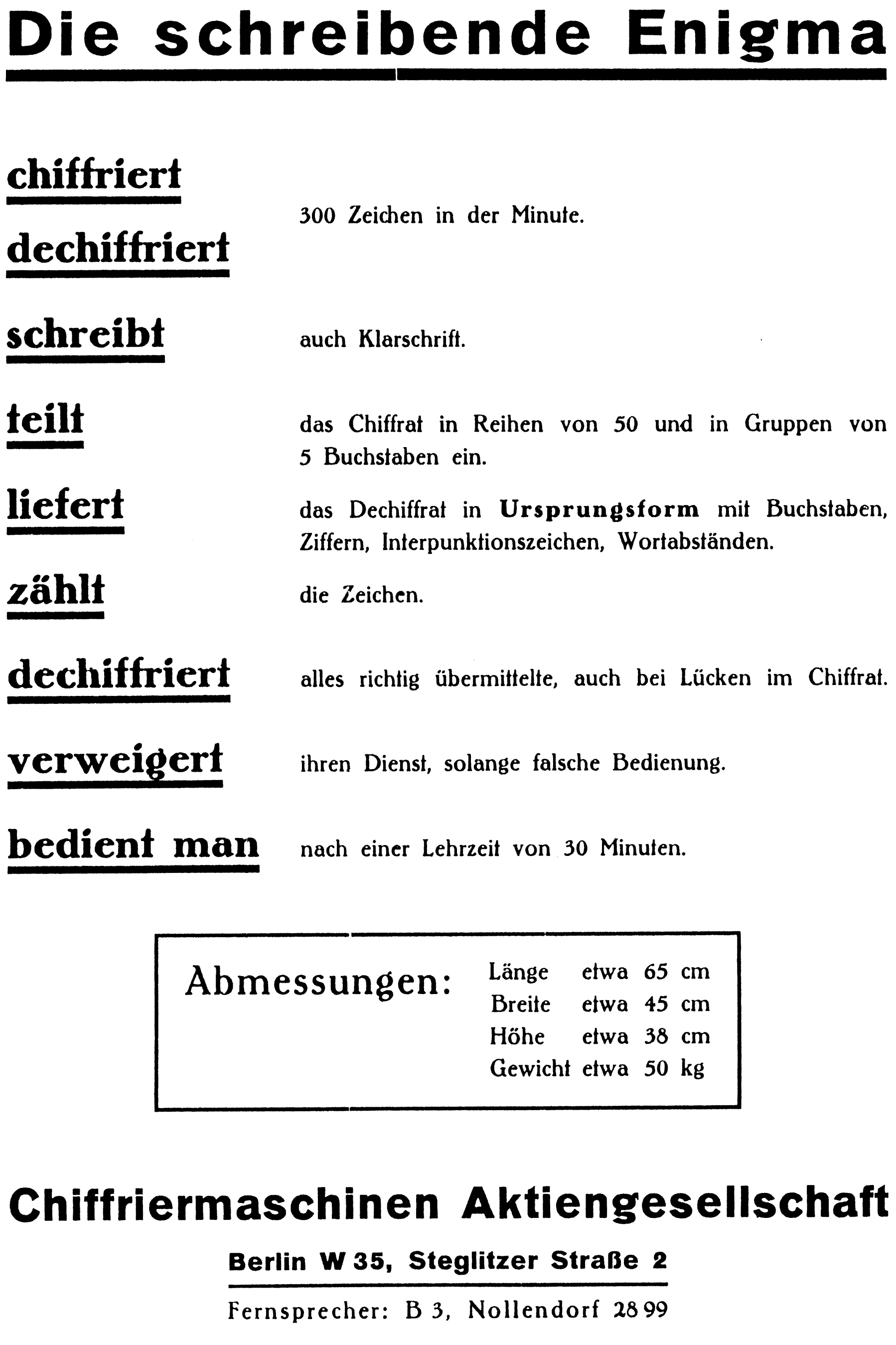
The printing
Enigma Cipher Machine
Type Bar — Electrical Drive

[Captions on picture, left side]
Printing mechanism
Carriage
Switch
[Right side]
Counting register
Cipher mechanism
Keyboard

Unassailable in its cipher security
Every attempt at solution wastes times
Full secrecy even during cleartext transmission of key changes
17,576 periods / Each period 15,777,450 symbols
Any one of the 227,304,461,200 can be input in half a minute
No part will be exchanged during a key shift [language unclear]

Figure 2A. Translation of two page flier promoting Enigma.
(Opposite) Figure 1A. Translator: David Kahn.

The rotor movement was quite irregular looking because rotors paused whenever they encountered a gapped sector of their wheels. For the sequence of rotor movements to repeat required $11 \cdot 15 \cdot 17 \cdot 19 = 53,295$ steps. However, the rotors will not have returned to their starting positions when the drive wheels have returned to their starting positions and so the period is generally much longer and depends on the exact placement of the gaps in the wheels. The number of initial settings for a given rotor was, clearly, $11 \cdot 15 \cdot 17 \cdot 19 \cdot 284$, because each rotor had 28 contacts. (The Enigma A had a 28-letter alphabet, which included three accented letters for the German language, but omitting one letter of the alphabet



Die schreibende Enigma

chiffriert
dechiffriert 300 Zeichen in der Minute.

schreibt auch Klarschrift.

teilt das Chiffrat in Reihen von 50 und in Gruppen von 5 Buchstaben ein.

liefert das Dechiffrat in **Ursprungsform** mit Buchstaben, Ziffern, Interpunktionszeichen, Wortabständen.

zählt die Zeichen.

dechiffriert alles richtig übermittelte, auch bei Lücken im Chiffrat.

verweigert ihren Dienst, solange falsche Bedienung.

bedient man nach einer Lehrzeit von 30 Minuten.

Abmessungen:			
Länge	etwa	65	cm
Breite	etwa	45	cm
Höhe	etwa	38	cm
Gewicht	etwa	50	kg

Chiffriermaschinen Aktiengesellschaft

Berlin W 35, Steglitzer Straße 2
Fernsprecher: B 3, Nollendorf 28 99

Figure 1B. Second page of two page flier promoting Enigma.

not often used in German.) The following year, Enigma A was exhibited at the 1924 International Postal Congress held in Stockholm, Sweden.

English Translation of Figure 1B

The Printing Enigma

Ciphers
Deciphers
300 symbols per minute

Prints cleartext as well
Divides the ciphertext into rows of 50 and groups of 5 letters
Delivers the plaintext in original form with letters, numbers, punctuation, word divisions
Counts all symbols
Deciphers everything if it is correctly transmitted, even if there are gaps in the ciphertext
Cannot be operated if improperly used
Can be used after 30 minutes instruction

Dimensions:
Length about 65 cm
Width about 45 cm
Height about 35 cm
Weight about 50 kg

Cipher Machine Inc.
Berlin W35, Steglitzer Strasse 2
Telephone: B 3, Nollendorf 2899

Figure 2B. Translation of two page flier promoting Enigma.
(Opposite) Figure 1B. Translator: David Kahn.

While Enigma A was not a great financial success despite the publicity it attracted, the company soon had three other models: B, C, and D. Model B (Figure 5) was of similar construction to Model A, but had the usual 26-contact rotors. Models C and D were portable and cryptographically unlike the A and B versions of the machine. Both machines had four 26-contact rotors but the fourth rotor, or Umkerwalze, was, in effect, a "half" rotor. This"reflecting" rotor caused current entering it to be turned back through the three previous rotors along a different path from that taken upon entry. As one faced the machine, the reflecting rotor was on the left with the entrance rotor on the right. If we denote the rotors R, I, II, III, then the enciphering current traversed the rotors in the order III, II, I, R, I, II, III. The reflecting principle was invented by Hugo Koch, and meant that, at any rotor setting, if a given letter, let us say A is enciphered into W, then W must also encipher into A. This means that each cipher alphabet generated by the machine is reciprocal. Additionally, no letter could represent itself because the reflected rotor path could never intersect the direct path. Because of the reflection process, no deciphering switch was necessary on the machine. One had only to arrange the rotors in the same order and starting position as used in encipherment and then type the ciphertext letters to recover the plaintext as glow-lamps indicated the results.

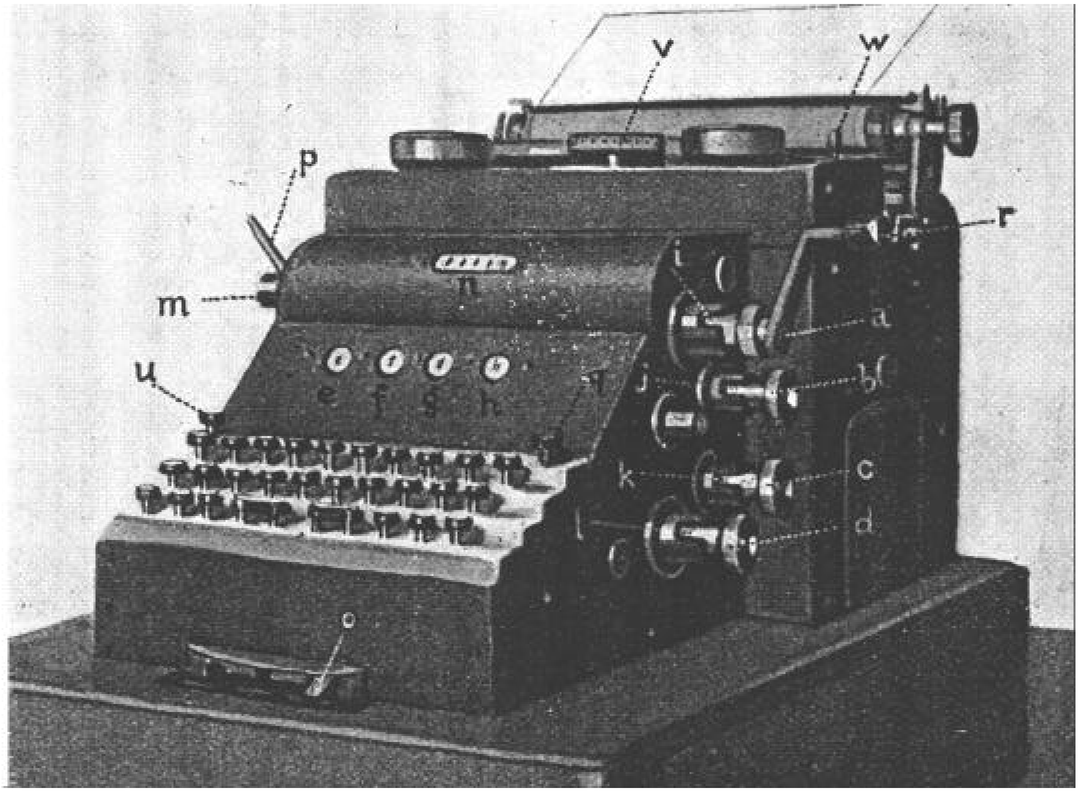


Figure 3. Model A.

The enciphering equation of this commercial Enigma is:

$$pKC(i)WC(-i)C(j)VC(-j)C(k)UC(-k)RC(k)U^{-1}C(-k)C(j)V^{-1}C(-j)C(i)W^{-1}C(-i)K^{-1} = c$$

where R denotes the reflecting rotor, and U, V, W are the other three rotors viewed facing the machine. K was the standard A-Z sequence, or identity transformation in Model C, while on Model D it was the keyboard permutation which was based on the standard German typewriter keyboard of that day, namely:

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

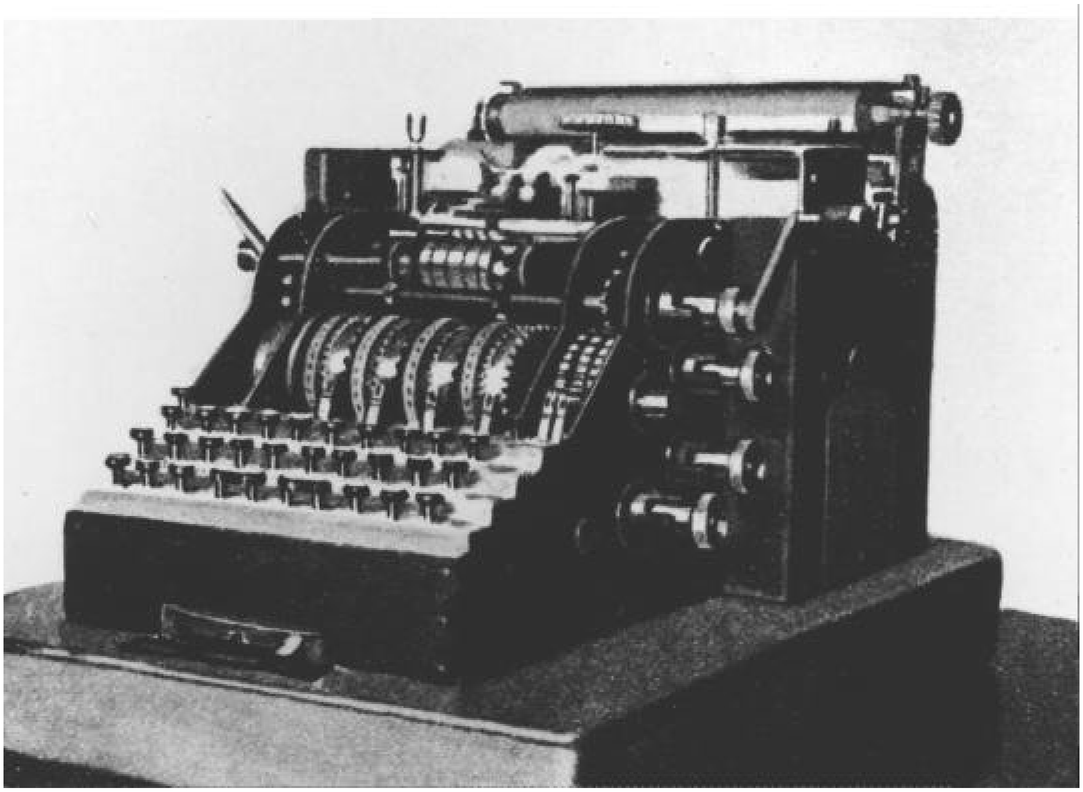


Figure 4. Model A with face plate removed.

Although Model C (Figure 6) and Model D (Figures 8 and 9) resembled one another, there were some minor differences. The reflecting rotor in Enigma C (Figure 7) could not be set and was confined to one of two possible positions in the machine. Additionally, the keyboard and glow-lamps were set up in the traditional A-Z sequence. The reflecting rotor of Model D (Figure 8) could be set, but did not move during encipherment. In both models, the fast rotor was the right-most one, the medium rotor to the left of the fast one, and the slow rotor to the left of the medium one. The ratchet wheels on the Enigma were built into the rotors instead of being separate, which gave rise to some anomalies in rotor movement.

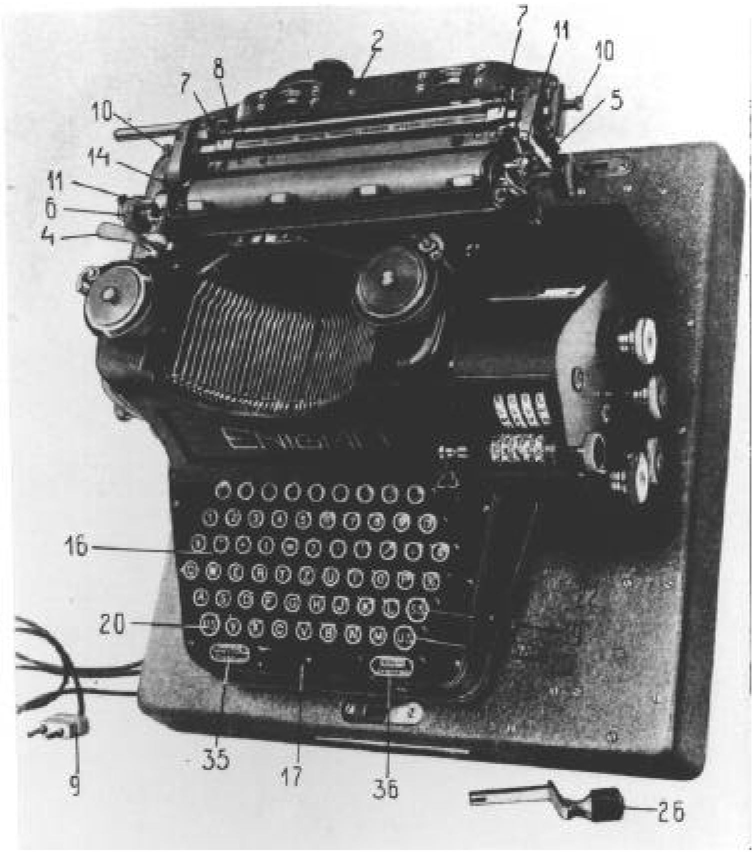


Figure 5. Model B (Top view).

When the ratchet wheel notch on the fast rotor reached a certain point in its revolution, a pawl drove the medium rotor one step forward. When the ratchet wheel notch on the medium rotor reached a certain point, the slow rotor was moved similarly. However, whenever the slow rotor stepped, the medium rotor also stepped because of the mechanical construction. Thus, at certain positions, the medium rotor could take two steps in succession. Therefore, the potentially maximum cycle length of $2^{63} = 17,576$ was not obtained. The basic cycle was of length $26 \cdot 25 \cdot 26 = 16,900$. Because one could obviously set the three right rotors in any one of 263 positions, then there must be some rotor starting positions that had no predecessors as well as some, which had more than one possible predecessor. It should be noted that the patent for this machine made provision for multi-notched rotors.

To facilitate the initial setting of the rotors, each had an “alphabet ring” bearing either the standard A-Z alphabet or the numbers 1-26. The alphabet rings could be rotated with respect to the body of the coding cylinder; thus, the ring setting was a part of the machine's key. The ratchet notch on each rotor was rigidly attached to the body of the coding cylinder in this version of the Enigma. The rotors were removable and interchangeable (except for the reversing rotor, which was always placed on the left).

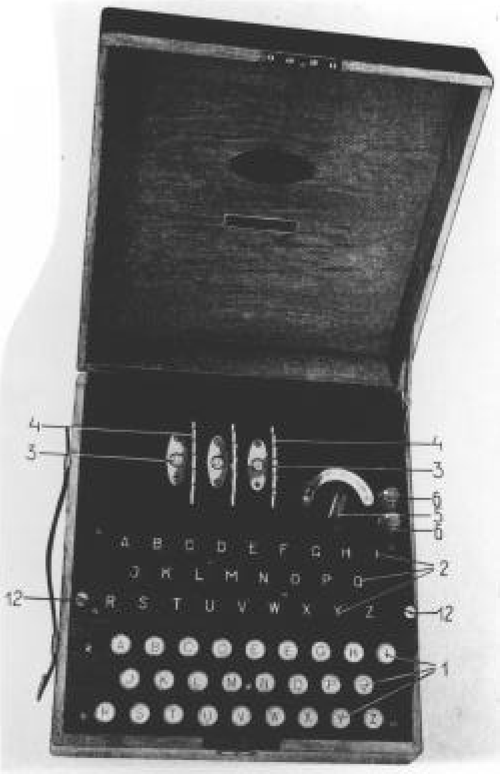


Figure 6. Model C.

After a short time, Enigma C became extinct with the D model becoming the widely sold commercial version of the device. Chiffrienmaschinen AG produced well-written documentation for their machines. The lengthy sales pamphlet, which accompanied the machine, described the need for cryptography, the extreme ease of use of the machine, and the amount of text, about 30 typewritten pages, which could be safely enciphered at one key setting. Additionally, methods of forming keys and secretly transmitting them in the ciphertext were illustrated. Strangely enough, the one short example of plain/cipher text given was bogus. The company had its "ciphering typewriter" examined by foreign experts in the field and salesmen were provided with favorable reviews to use in sales promotion. For example, after a two month test of the Enigma, a Captain Henri Koot, Dutch Army cryptologic expert, wrote,"I dare say that it satisfies all requirements, be they ever so high even the possession of an equal machine with the same electrical connections both in the ciphering cylinders and in the other parts of the machine will not enable an unauthorized person to find out its solution."

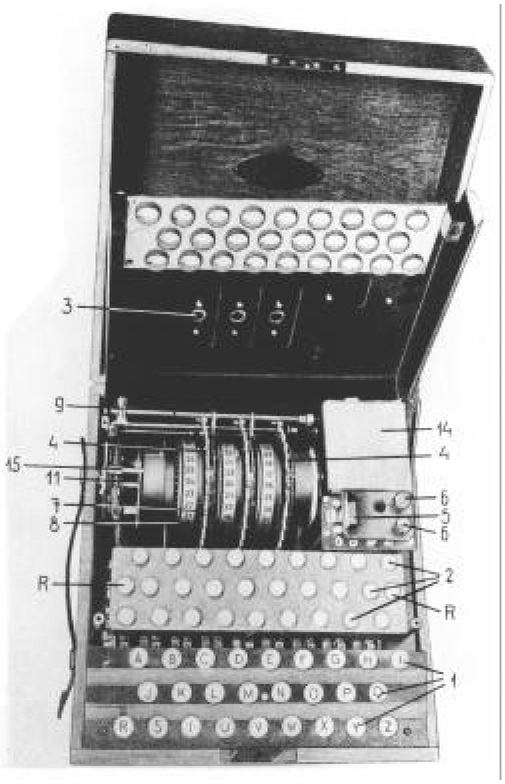


Figure 7. Model C with inner lid open.

The wiring used in the commercial Enigma D was as follows:

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

The contact numbers are printed on the coding cylinder bodies. The wiring given here is read when the alphabet ring on each rotor is placed so that the letter A corresponds to contact point 1. Each coding cylinder body had its ratchet notch at contact position 21 (G) and caused movement when contact 2 (Z) appeared in the setting window. Thus, with the alphabet rings set as above, successive rotor positions would be:

W	Z	Y	X
W	Z	Y	Z
W	Z	Z	A
W	A	A	B
W	A	A	C
W	A	A	D

A number of governments bought Enigmas for study. Among the interested parties was the German Navy, which in 1925 decided to put an Enigma machine into use the following year. The first Naval Enigmas had 29-contact rotors (included ä ö ü in German) and used three rotors chosen from a set of nine. Possibly, certain other modifications may have been made to the Navy machine.

The Italian Navy adopted the commercial Enigma as Naval Cipher D. Studies based on matching cipher and plain text indicate that the Naval machine was rewired as might be expected. The British solution of this Enigma variation largely led to the Italian defeat at the battle of Matapan.

The German army, which previously had been considering adoption of the Enigma, now undertook to redesign and strengthen the machine's ciphers. By 1928, early models of the redesigned Wehrmacht machine, denoted model G, were in use, and in June 1930, the final"revised standard" version of the device, Enigma I came into use by the Army.

Enigma I was distinguished from the commercial Enigma by the following changes:

1. The reflecting rotor was made static and greatly reduced in size to save money.
2. The rotatable alphabet rings were retained, but the stepping ratchet notch was rigidly affixed to this ring instead of the coding cylinder body.
3. A plug-board was inserted into the front of the machine whose 26 plugholes could be connected in pairs by plugs. The earliest such plugs, (*Stoppelstellung*) were later replaced by double-ended banana style ones (*Steckerverbindung*). The plugs functioned the same way, however, in both constructions. The plug-board introduced a variable reciprocal permutation between the keyboard and the fast rotor, and the inverse permutation between

the fast rotor exit point and the lamp-board. (The reciprocal encipherment was retained in this manner.)

4. The keyboard entrance permutation was changed from that of the standard typewriter to the identity permutation, A=A, B=B, et cetera. (The arrangement of letters in the keyboard was unaltered, however.)

This model of the Enigma became the most widespread of the ensuing Enigma variations, used by the German Navy beginning in October 1934 and the Air Force beginning in August 1935.

In 1974, when the British revealed *The Ultra Secret*, the world became aware of the German Enigma Cipher Machine and the vital role it played in World War II. It also learned how breaking Germany's most important cipher system helped in its defeat and shortened the War by at least one and possibly two years, according to some authorities. Since then, hundreds of books, newspaper and magazine articles, television programs, major motion pictures and even a Broadway play have made the Enigma the most widely known cipher machine in the world. On April 12, 2001, a Model D Enigma was sold at auction in London for $15,220. Few people, however, are aware that the machine was initially rejected by Germany and Arthur Scherbius, after developing four different Enigma models, was still a failure in his efforts to convince business people that: "One secret, well protected, may pay the entire cost of the machine."[1]

ACKNOWLEDGMENTS

A special note of thanks to David Kahn for his suggestions for improving the text.

Our deep appreciation to Jürgen Rohwer who graciously allowed us to use a new version of his chart, which illustrates the evolution of the German Enigma and some other rotor cipher machines.

REFERENCES

1. Deavours, Cipher A., and Louis Kruh. 1985. *Machine Cryptography and Modern Cryptanalysis*. Dedham MA: Artech House.

2. Garlinski, Józef. *The Enigma War*. New York: Charles Scribner's Sons, 1979.

[1] The Glow-Lamp Ciphering and Deciphering Machine: Enigma. *Cryptologia*, 25(3): 163–174. This article is a reprint of the original , mid-1920's, sales brochure for the Enigma.

3. Kahn, David . 1991. *Seizing the Enigma: The Race to Break the German U-Boat Codes, 1939-1943*. Boston: Houghton Mifflin.

4. Kahn, David. 1996. *The Codebreakers: The Story of Secret Writing. Revised ed.* New York: Scribner.

5. Kozaczuk, Wladyslaw. 1984. *Enigma: How the German Machine Cipher Was Broken and How it Was Read by the Allies in World War Two*. Frederick MD: University Publications of America.

6. Rohwer, Jürgen and Eberhard Jäckel. 1979. *Die Funkaufklarung und ihre Rolle im Zweiten Weltkrieg*. Stuttgart: Motorbuch Verlag.

7. Singh, Simon. 1999. *The Code Book: The Evolution of Secrecy from Mary Queen of Scots to Quantum Cryptography*. New York: Doubleday.

8. Türkel, Siegfried. 1927. *Chiffrieren Mit Geráten und Maschinen*. Graz: Ulr. Mosers Buchhandlung.

BIOGRAPHICAL SKETCHES

Louis Kruh, a founding co-editor of *Cryptologia* and co-author of *Machine Cryptography and modern Cryptanalysis*, has an enormous collection of cryptologic items amassed over 40 plus years. This collection supplied most of the illustrations for this article and, between writing reviews and articles for *Cryptologia*, he is trying to compile a computerized list of his holdings.

C. A. Deavours, a founding co-editor of *Cryptologia* and co-author of *Machine Cryptography and modern Cryptanalysis*, is a faculty member teaching mathematics and computer science at Kean University of New Jersy in Union NJ. Professor Deavours has a distinguished career of consulting, cipher busting, crypto teaching, and computer connecting. His most recent interest is web-based learning and keeping the university's web radio station, WKNJ Internet Radio, on air.

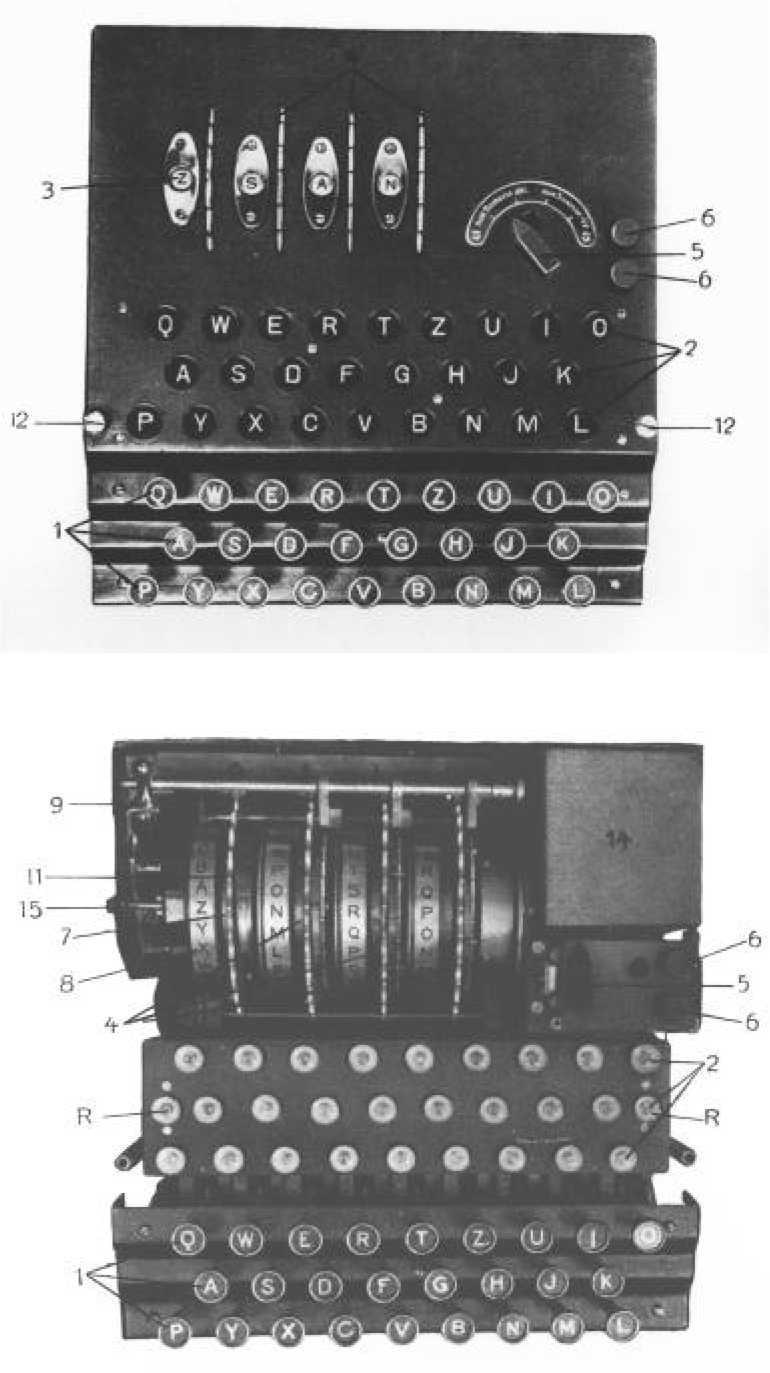


Figure 8. I (above) Model D and II (below) Model D with lid removed.

Illustration	I, 11:	1. Key-board.
”	I, II:	2. Glow lamp board.
”	I:	3. Windows.
”	I, II:	4. Ciphering cylinders (rollers).
”	I, II:	5. Switch-handle.
”	I, II:	6. Connecting terminals for accumulator working.
”	II:	7. Spring for adjusting the letter-ring.
”	II:	8. Letter-ring.
”	II:	9. Lever.
”	II:	11. Reversing cylinder.
”	II:	12. Lid screws.
”	II:	14. Dry battery.
”	II:	15. Guide pin.
”	II:	R. Spare-lamps.

(Opposite) Explanation of the Figures 8 I & II

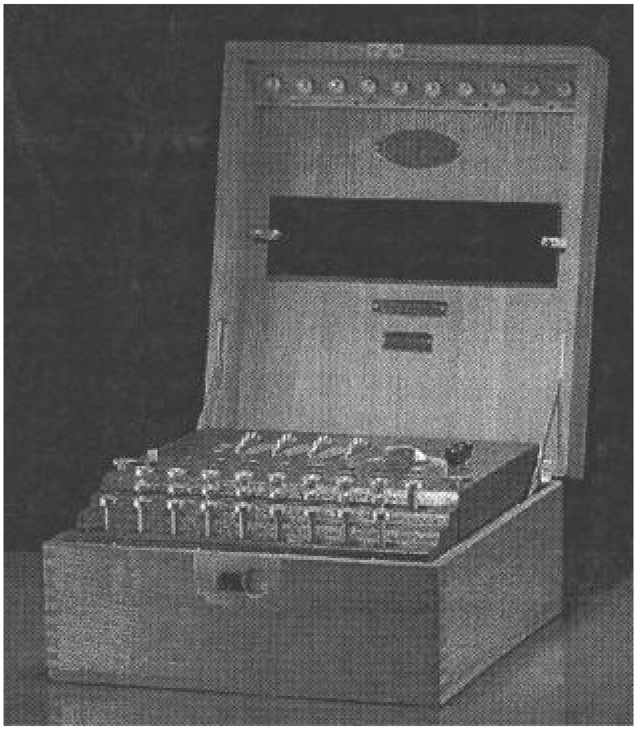


Figure 9. Model D “Enigma enciphering machine” was sold at auction in London, 12 April 2001, for $15,220. Illustration downloaded from Christies' (auctioneer) web site.

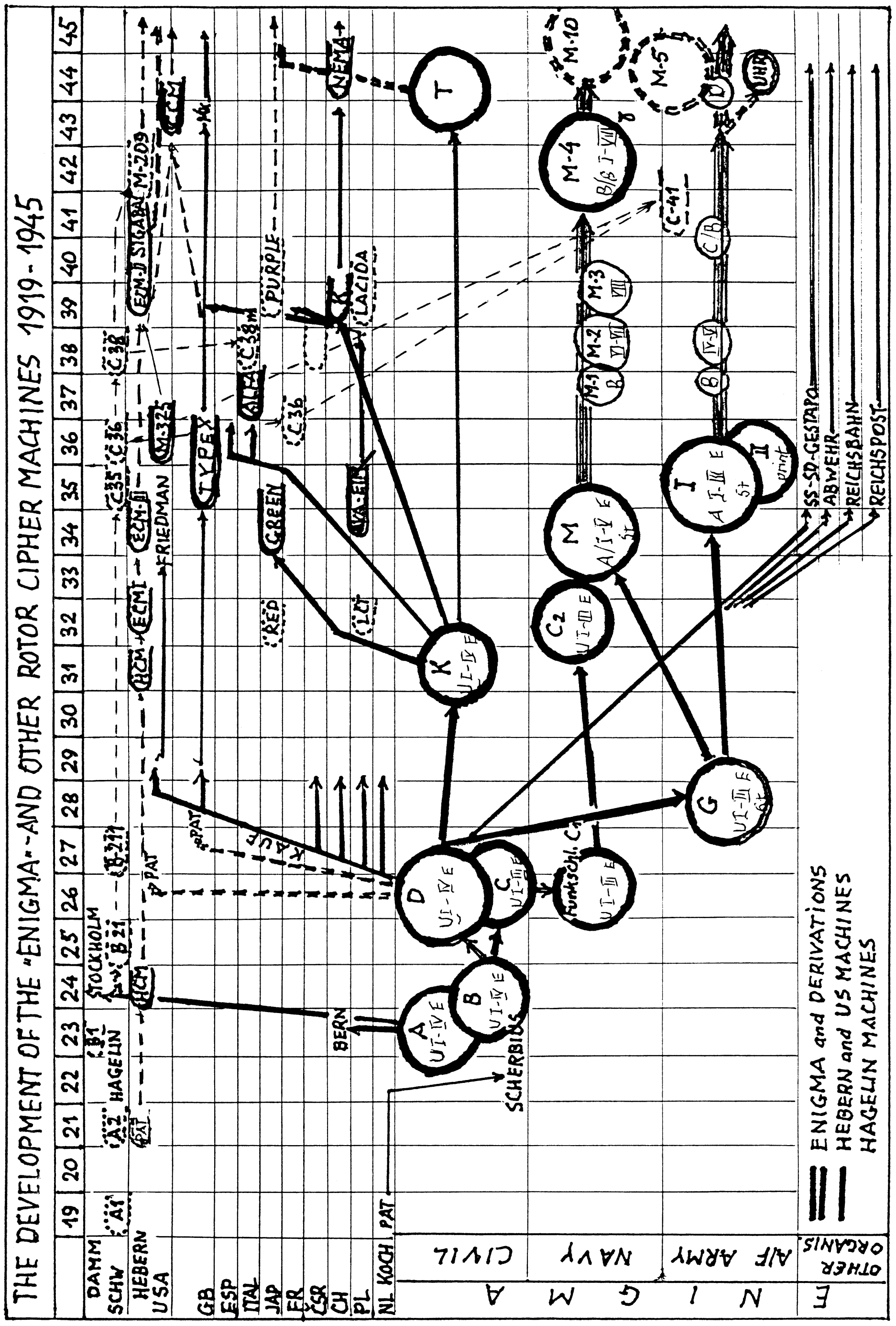


Figure 10. Evolution of the Enigma Cipher Machine.
Diagram created by Jürgen Rohwer.