View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Wilfrid Laurier University

Canadian Military History

Volume 6 | Issue 2 Article 9

1-24-2012

The Engima Cipher Machine

Tony Wilson

Recommended Citation

Wilson, Tony (1997) "The Engima Cipher Machine," *Canadian Military History*: Vol. 6: Iss. 2, Article 9.
Available at: http://scholars.wlu.ca/cmh/vol6/iss2/9

This Canadian War Museum is brought to you for free and open access by Scholars Commons @ Laurier. It has been accepted for inclusion in Canadian Military History by an authorized administrator of Scholars Commons @ Laurier. For more information, please contact scholarscommons@wlu.ca.

The Enigma Cipher Machine Type "A"
A general view with the main and keyboard patch panel covers open. The Rotary switch to the right of the cipher cylinders is the battery on/off switch.
(Canadian War Museum Photo)

Published by Scholars Commons @ Laurier, 1997

The Enigma Cipher Machine

Tony Wilson

Enigma: a Puzzle; a Riddle

Introduction

There can be little doubt that the German "Enigma" was the best and safest mechanical cipher machine available to any country at the outbreak of the Second World War. Its general use by all three services of the German armed forces presented the Allies with a very serious impediment to their efforts to read the German military message traffic and a great deal of time and effort was expended in attempts to devise a rapid and accurate method of deciphering it.

That these efforts were in the end successful, was due in the main to the work of a dedicated team of scientists and academics based at the Bletchley Park facility north of London, England, and the establishment of the "Ultra" intelligence gathering and distribution operation that worked so well for the Allies throughout the most crucial parts of the conflict.[1]

The author's interest in the Enigma began when working as a volunteer communications specialist at the Canadian War Museum. Two Enigma machines were discovered stored with the radio and other electronic equipment at the Vimy House storage facility. Further investigation of these machines found that one was the three-cipher-cylinder Type "A." It was even found to be in operating condition, being essentially complete with three of its five cipher cylinders in place.

The other machine was a four-cylinder Type "M." It was in generally good condition, but lacked most of its cipher cylinders. It currently forms part of a Naval display at the Canadian War Museum on Sussex Drive in Ottawa, Ontario.

Secret Writing – Some Historical Notes

From the earliest times, there has been a need to transmit information in a form that cannot be understood by anyone but the intended recipient. The information may be personal, industrial, professional, political or military, but whatever the source, the key requirement is that it remains secret to any unauthorized readers.

The act of converting information into a form which is useless to anyone except the proper recipient is known as encoding or encipherment. Although the terms are often used interchangeably, properly, a "code" is the substitution of a group of letters or figures, or a mixture of both, for a set phrase. Conversely, a "cipher" involves the substitution of other letters or figures or, again, a mixture of both, for the original individual letters and/or figures in the message.

For example, in a code, "send help" might be rendered as "27"; or "cease firing" as "63"; in a cipher, "send help" might be rendered as "jugr fjbn" and "cease firing" as "ightr joudim."

The methods devised to convert plain language, or "plaintext," to a ciphered message, or "ciphertext," are many and varied. Some are simple - e.g., scrambling the order of letters in a word, so that "secret" becomes "etserc"; one- or two-letter shifts, such a=b, b=c, c=d, etc. Others

© Canadian Military History, Volume 6, Number 2, Autumn 1997, pp.72-78.

are more complicated. For example, the Greek Polybius devised an arrangement of letters in a square with the rows and columns numbered, from which each letter is enciphered into a two-digit number. Using the English alphabet, and merging the "i" and "j" into one unit, the Polybius Square, as it is known, appears like this:

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	ij	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

From this, the letters of a message can be translated into ciphertext as a=11; h=23; r=42, etc.

A rather more complicated version of the Polybius Square was proposed by a German, Johannes Trithemius, who, in his work *Polygraphiae* (1518) set out a square comprised of all the letters of the alphabet, arranged both vertically and horizontally, with each row of letters shifted by one letter from the row above.

Known as a "tableau," such an arrangement can appear thus:

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

Such a tableau can be used in many ways to encipher a document, but the simplest is to encipher the first letter from the first alphabet, the second from the second, the third from the third, etc. Then the ciphertext of a message that started "fire left..." would appear as "fjth pjla...."

While the main requirement of rendering communications unintelligible to the unauthorized reader has been met, the increasing complication of enciphering methods led to many attempts to simplify and accelerate the conversion of the plaintext into a ciphertext and the ciphertext back into the original plaintext. Fast translation to and from ciphertext is of the essence, particularly under battle conditions, and much effort has been put into devising methods which will speed the process while ensuring the highest level of secrecy.

Two common early methods involved the use of masks which could be placed over the plaintext to encipher, or over the ciphertext to decipher, the message, code books and tables and in mechanical form, concentric discs, each engraved with the alphabet, one disc being free to rotate within the other, allowing the two alphabets to be displaced in relation to one another, depending on the cipher requirement.[2]

Development of the German "Enigma" Cipher Machine

The speed of operation offered by mechanical methods resulted in much effort being applied to the development of reliable portable machines. The basic rotating disc approach developed into quite complex mechanisms involving more than one rotating disc, or cylinder, and operation from lettered keyboards. When produced in a suitably rugged form, such equipment is capable of reliable operation under battlefield conditions.

In the late 1910s, Alexander Koch, a Dutch national, filed a patent for a form of a mechanical cipher machine which could use electrical impulses transmitted though a rotor mechanism to produce a ciphertext. However, it would seem that no practical machine was ever produced and the Dutch patent was assigned in 1927 to Arthur

Scherbius, a German. In the early 1920s, Scherbius had designed an electromechanical cipher machine consisting of a typewriter-like keyboard, which, when a key was depressed, caused an electric current to flow through contacts on a series of rotating cylinders to light a lamp under an alphabetic display panel. Depending on the setting of the cylinder contacts, the illuminated letter was different from the key letter pressed. With the same cylinder settings at the originating and receiving ends, messages could be rapidly and reliably enciphered and deciphered.

Scherbius named his machine the "Enigma," and after making several modifications to the original design, set up a company to produce it. In 1923, this company was acquired by a group of businessmen, put on a proper capitalized footing and named the *Chiffriermaschinen Aktiengesellschaft* (Cipher Machines Corporation), with manufacturing premises in Berlin. Patents were applied for and granted in a number of countries and serious attempts were made to promote the Enigma, which had been developed into a machine about the size of a portable typewriter, but with relatively little success.

In 1934 the company was wound up and its assets transferred to a new company, named *Chiffriermaschinen Aktiengesellschaft Heimsoeth und Rinke*, Heimsoeth and Rinke having been two of the directors of the original organisation. While examples of the Enigma were obtained by several countries, including the U.S.A., sales were not particularly outstanding until the German Military High Command recognised the utility and security offered by the Enigma and adopted it as the standard cipher machine for the *Kriegsmarine* (Navy), *Wehrmacht* (Army) and *Luftwaffe* (Air Force), after which all commercial sales were banned.

Initially, production for the German forces was from the *Chiffriermaschine* company, but with the Enigma's use down to unit level, wartime requirements were so large that this company was unable to meet the demand. Starting in mid-1943, production was also carried out by the *Olympia Buromaschinenwerke* (typewriter) company. By the end of 1943, the Olympia company was delivering over 70 machines per month for the German navy alone.

The "Enigma" Described

The Enigma machine is essentially a mechanical device using variable electrical connections to perform the enciphering and deciphering operations. Two basic types were produced, the Type "A" machine, which was used by both the army and the air force, and the later Type "M" machine, used by the navy. The machine consists of a wooden case containing a typewriter-like keyboard for the input of either the plain- or ciphertext, depending on which operation is to be done. Also included are associated electrical contacts and a fixed input/output cylinder to connect to the rotating encoding cylinders. Five encoding cylinders were supplied with each Type "A" machine, of which any three were installed at any one time. Six or seven encoding cylinders were supplied with each Type "M" machine, of which any four, and later five, were installed when in operation. The cylinders are marked with the serial number of the machine to which they belong and with the Roman numerals I to V, VI or VII. The output device is a letter display panel, each letter being illuminated by an incandescent lamp. A reversing cylinder and an electrical jumper panel complete the operating mechanism.

The machine is fitted with an integral box for a rechargeable 2.4-volt nickel-iron secondary battery, which provides the power to illuminate the lamps. Connectors are provided for an external battery, if required. To protect the lamps from a higher than normal operating voltage when using a newly-charged battery, a position on the on/off switch introduces a series resistance into the supply line, thereby limiting the current to the lamps to a safe value.

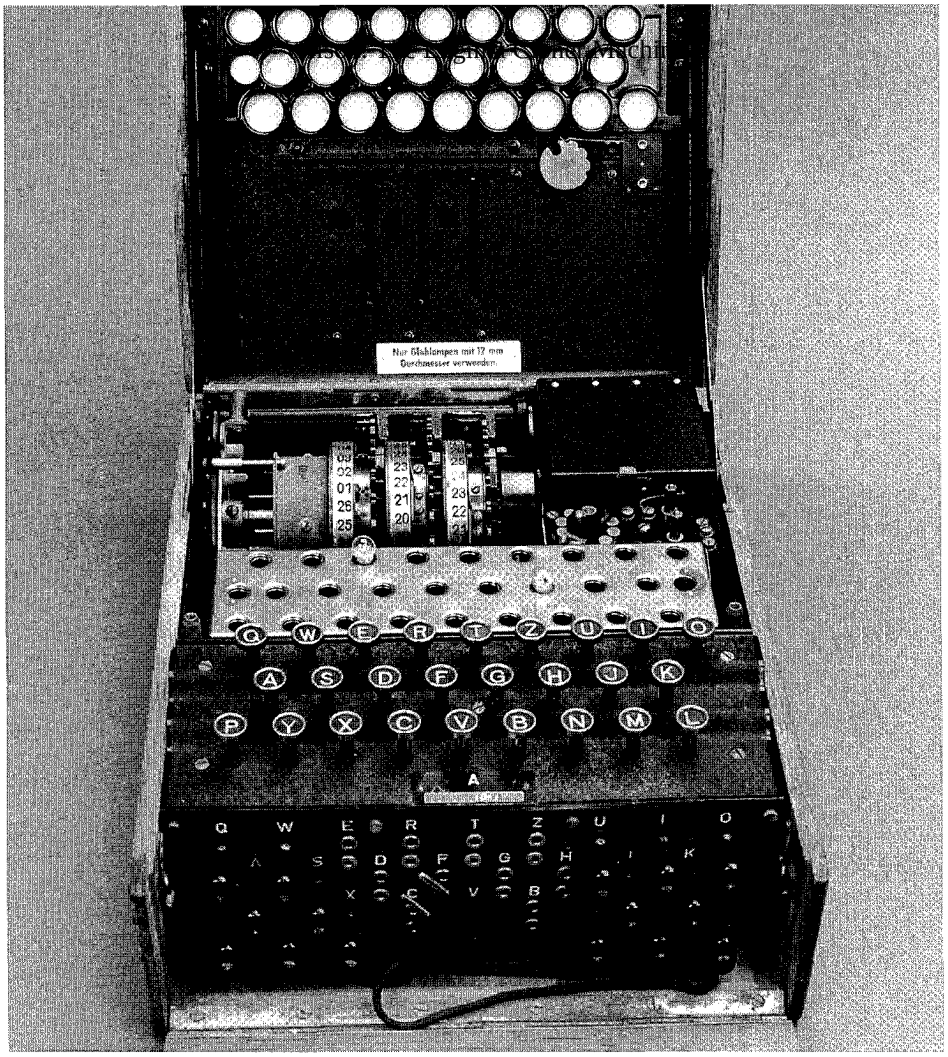
Mechanical Arrangement

Letter Keys

Operation of a letter key closes electrical contacts and operates a pawl mechanism to rotate one or more of the encoding cylinders.

Encoding cylinders

The encoding cylinders are equipped with twenty-six ratchet teeth, corresponding to the contacts on the sides of the cylinder, the positions



(CWM Photo)

The Enigma Cipher Machine Type "A" with the Lamp Panel cover open, showing lamp mounting plate and cipher cylinders in position. The operating battery is installed in the box to the right of the cipher rotors. The input/output cylinder is to the right of the cipher cylinders and the reflecting cylinder is to their left.

of which are shown by a numbered ring mounted on the side of the cylinder. A locking pin equipped with an index mark allows the position of the numbered ring to be changed relative to that of the contacts. Depending on the cipher requirements of the day, the three, (four or five) cylinders can be arranged in any order, on a single shaft which is installed between the input/output cylinder and the reversing cylinder. For example, cylinders I, II and IV may be required, but installed in the order IV, I, II, whereas at another time, the requirement might be II, III, V, ordered III, II, V.

When a letter key is operated, a pawl bears onto the tooth of the first code cylinder and advances it one step. The operating pawls for the remaining cylinders are normally held free of the teeth on their respective cylinders by a flat fibre disc mounted on the side of the adjacent cylinders. This disc is provided with a single cut out tooth which allows an adjacent pawl to engage with a tooth on the second code cylinder, thereby advancing it by one step.

Further operations of the letter keys only rotate the first cylinder until the pawl again engages the single tooth, when the second cylinder is advanced one more step.

In the same way, when the second cylinder has been rotated to the point of its single tooth, the third cylinder will be advanced one step (and similarly for the fourth and/or fifth cylinders on the Type "M" machine).

Electrical Arrangement

Keyboard and Input/Output Connector

The electrical contacts associated with each letter key are connected in sequence to the contact pins of the input/output cylinder, so that if we take

Published by Scholars Commons @ Laurier, 1997

the letter A to be connected to contact 1, B = 2, C = 3, etc., to Z = 26. A second set of contacts on each letter key disconnects the associated letter lamp, to ensure a letter cannot be enciphered as itself.

In addition, an arrangement of jumper cords and plugs and sockets enables the connections between the key contacts, the letter lamps and the input/output contacts to be altered. For example, the key contacts for the letter "A" could be jumpered to operate through the input/output cylinder contacts normally associated with the letter "J," which would at the same time transfer the connection to the "J" lamp to the lamp corresponding to the letter "A".

Code Cylinders

The code cylinders are equipped with 26 flat contacts on one side and 26 spring-loaded pin contacts on the other. These contacts are connected in a random pattern by internal jumpers and, as noted above, the contact position is indicated by a numbered wheel on the side of the cylinder. The jumpering pattern is different for each code cylinder in the set provided for a given machine.

Reversing Cylinder

The reversing cylinder has 26 contacts, thirteen of which are internally connected in a random pattern to the remaining thirteen.

Circuit Operation

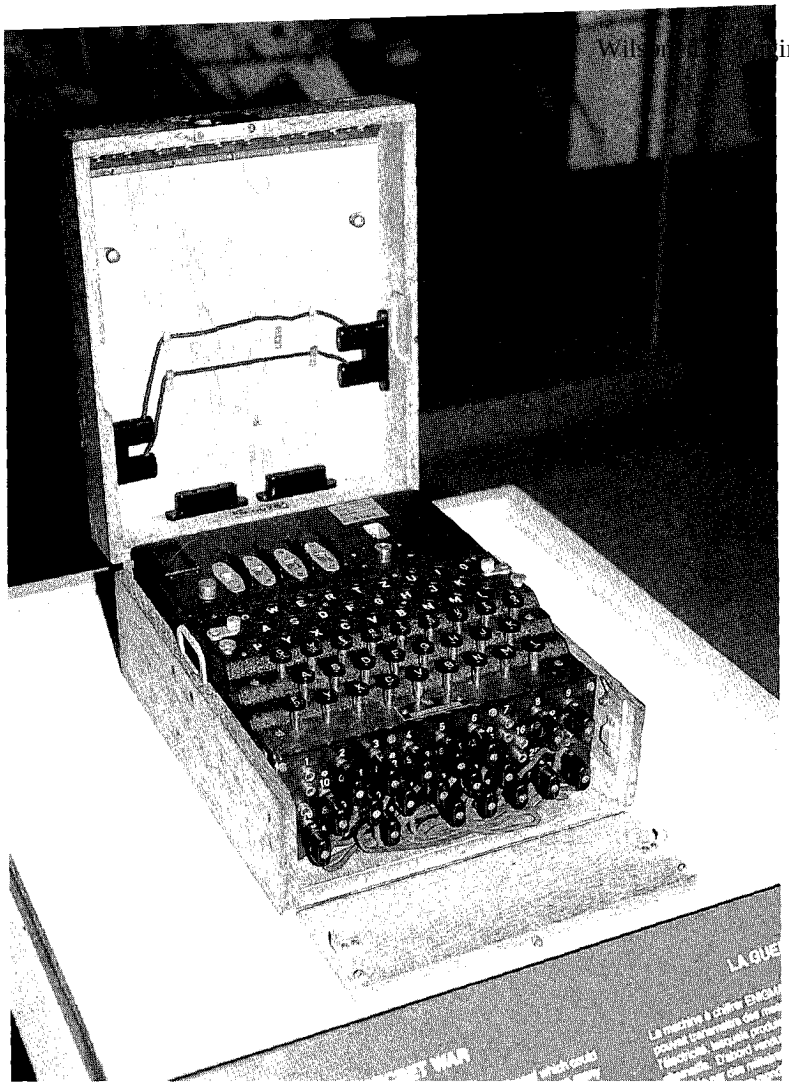
Pressing a letter key operates its associated electrical contacts and sends a current to the encoding circuit while a second set of contacts on the letter key opens the connection to the equivalent letter lamp, thereby preventing that letter being enciphered as itself. From the key contact, the current flows to the input/output connector, through the contacts on both sides of the three code cylinders to the reversing cylinder. At the reversing cylinder, the current is routed back via a different set of contacts on the three code cylinders to the input/output cylinder to light a letter lamp.

The number of combinations available through the various arrangements described above is quite phenomenal! For example, given that all the encoding cylinders are set such that there must be twenty-six movements of each before the position of the adjacent cylinder is affected, we have an initial twenty-six different connections before the second cylinder is moved on by one step. We now have a further twenty-six movements t the current passes twice through the three cylinders, once from key to reversing cylinder and then, by a different path, from the reversing cylinder to the letter lamp, and that the encoding cylinders can be arranged a number of different orders between the input/output and the reversing cylinders, providing even more possible connections. Add to this the jumper arrangement of the key and lamp circuits, where up to thirteen cross-connections can be made at any one time, and the additional encoding cylinders provided with each machine, and the total number of combinations available in any one machine becomes astronomical.

With this capability, it was believed that messages encoded by the Enigma system would be unbreakable. However, much effort was expended by the British, initially aided by the acquisition of a copy of the Enigma, which had been produced by a Polish group, some of whose members had worked at the factory in Germany prior to the Second World War. A special group dedicated to code-breaking was set up at Bletchley Park, a country house facility located 50 miles north of London, with some limited success. However, the breakthrough came in May 1941, when the corvette *Aubretia* and the destroyers *Bulldog* and *Broadway* attacked the German U-boat *U-110*. The U-boat was forced to the surface and abandoned by the crew, but did not sink. A party from *Bulldog* boarded the submarine and stripped it of its code books, radio dial settings and its Enigma machine, which was complete with its operating and code settings. The material was brought back to the UK and handed over to the experts at Bletchley Park, from which it was possible to develop methods of decoding Enigma traffic.

In-service Operation

While its enciphering capabilities are outstanding, the essence of the Enigma cipher machine is the simplicity of its operation. To encipher a message, the operator set the



(CWM Photo)

The Enigma Type "M" used by the German Navy.

appropriate settings of the numbered rings on the encoding cylinders, the positions of the keyboard jumper cords and the position on the shaft of the code cylinders and their starting points. He then pressed keys corresponding to the letters in the plaintext and the enciphered letters were illuminated on the display panel.

To decipher a message, the operation was the same, with the same machine settings as were used to encipher the message. In this case, however, the letters of the ciphertext were typed in by the operator and the illuminated letters that resulted were those of the plaintext.

Possibly the most serious complaint about its operation was that, for maximum speed, it required three operators, one to read the input text, one to operate the keyboard and one to read off the output text from the lamp panel.

Enigma Machines at the Canadian War Museum

The Canadian War Museum possesses two Enigma machines, a Type "A," serial number 16263 and a Type "M," serial number 6026. Both machines were obtained as war reparation items and unfortunately we have no record of their use by the German forces. It is thought likely that they were each used by a number of units, as the Enigma machine was not a field-repairable item and would have been returned to a depot pool on an over-the-counter exchange basis in the event of a repair being required. Lacking the records of such facilities, the history of our machines remains a mystery.

The Type "A" machine bears the label "16263/jla/43," the "jla/43" indicating it was manufactured by the *Schiffriermaschine Gesellschaft* in 1943. The machine is almost complete, lacking only encoding cylinders III and IV and lamps, and is in working order. It is presently stored at the Vimy facility.

The Type "M" machine bears the labels "M6026" and "6026/aye/43," the "aye/43" indicating that it was manufactured by the *Olympia Buromaschinenwerke A.G.* in 1943. This machine is incomplete, lacking five of the original seven encoding cylinders, although its general condition is good. It presently forms part of a naval display at the Museum site on Sussex Drive in Ottawa.

Notes

1. F.W. Winterbotham, *The Ultra Secret* (New York: Harper and Row, 1974, provides a first hand account of the Ultra operations.
2. David Kahn, *The Code-Breakers* (New York: MacMillan, 1967) contains an excellent and comprehensive history of secret communication.

Tony Wilson is a retired senior manager with Northern Telecom, and a former member of the Royal Corps of Signals. He currently volunteers twice a week at the Canadian War Museum.