Enigma machine

A three-rotor German military Enigma machine showing, from bottom to top, the plugboard, the keyboard, the lamps and the finger-wheels of the rotors emerging from the inner lid (version with labels).

In the history of cryptography, the **Enigma** was a portable cipher machine used to encrypt and decrypt secret messages. More precisely, Enigma was a family of related electro-mechanical rotor machines — comprising a variety of different models.

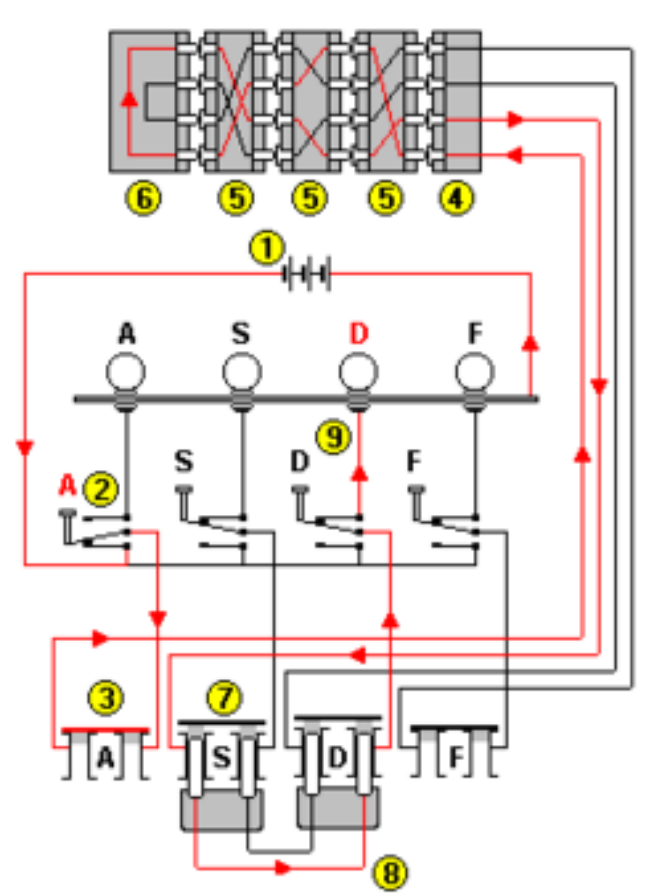
The Enigma was used commercially from the early 1920s on, and was also adopted by the military and governmental services of a number of nations — most famously by Nazi Germany before and during World War II.

The German military model, the **Wehrmacht Enigma**, is the version most commonly discussed. The machine has gained notoriety because Allied cryptologists were able to decrypt a large number of messages that had been enciphered on the machine. The intelligence gained through this source — codenamed ULTRA — was a significant aid to the Allied war effort. The exact influence of ULTRA is debated, but a typical assessment is that the end of the European war was hastened by two years because of the decryption of German ciphers.

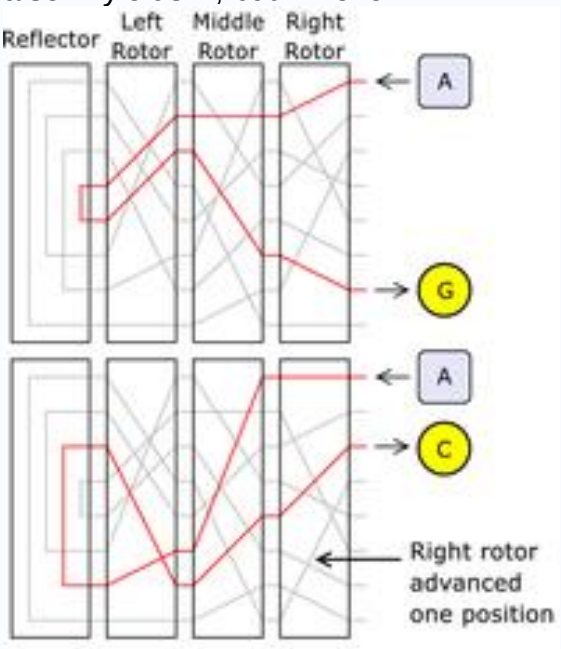
Although the Enigma cipher has cryptographic weaknesses, it was, in practice, only their combination with other significant factors which allowed codebreakers to read messages: mistakes by operators, procedural flaws, and the occasional captured machine or codebook.

This article discusses the Enigma machine itself: its components and its procedures. For the history and techniques of how Enigma was broken, see **Cryptanalysis of the Enigma**. For a discussion of how Enigma-derived intelligence was put to use, see **ULTRA**.

Description



Enigma wiring diagram showing the current flow when pressing the 'A' key is encoded to the 'D' lamp, also D yields A, but A never A



The scrambling action of the Enigma rotors shown for two consecutive letters — current is passed into set of rotors, around the reflector, and back out through the rotors again. Note: The greyed-out

lines represent other possible circuits within each rotor, which are hard-wired to contacts on each rotor. Letter A encrypts differently with consecutive key presses, first to G, and then to C. This is because the right hand rotor has stepped, sending the signal on a completely different route.

Like other rotor machines, the Enigma machine is a combination of mechanical and electrical systems. The mechanical mechanism consists of a keyboard; a set of rotating disks called *rotor*s arranged adjacently along a spindle; and a stepping mechanism to turn one or more of the rotors with each key press. The exact mechanism varies, but the most common form is for the right-hand rotor to step once with every key stroke, and occasionally the motion of neighbouring rotors is triggered. The continual movement of the rotors results in a different cryptographic transformation after each key press.

The mechanical parts act in such a way as to form a varying electrical circuit — the actual encipherment of a letter is performed electrically. When a key is pressed, the circuit is completed; current flows through the various components and ultimately lights one of many lamps, indicating the output letter. For example, when encrypting a message starting ANX..., the operator would first press the A key, and the Z lamp might light; Z would be the first letter of the ciphertext. The operator would then proceed to encipher N in the same fashion, and so on.

To explain the Enigma, we use the wiring diagram on the left. To simplify the example, only four components of each are shown. In reality, there are 26 lamps, keys, plugs and wirings inside the rotors. The current flows from the battery (1) through the depressed bi-directional letter-switch (2) to the plugboard (3). The plugboard allows rewiring the connections between keyboard (2) and fixed entry wheel (4). Next, the current proceeds through the - unused, so closed - plug (3) via the entry wheel (4) through the wirings of the three (Wehrmacht Enigma) or four (Kriegsmarine M4) rotors (5) and enters the reflector (6). The reflector returns the current, via a different path, back through the rotors (5) and entry wheel (4), and proceeds through plug 'S' connected with a cable (8) to plug 'D', and another bi-directional switch (9) to light-up the lamp.

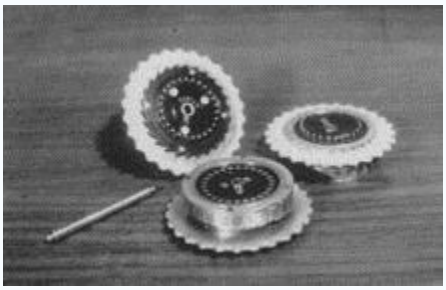
So the continual changing of electrical paths through the unit because of the rotation of the rotors (which cause the pin contacts to change with each letter typed) implements the polyalphabetic encryption which provided Enigma's high security (for the time).

Rotors

The left side of an Enigma rotor, showing the flat electrical contacts. A single turnover notch is visible on the left edge of the rotor.

The right side of a rotor, showing the pin electrical contacts. The Roman numeral V identifies the wiring of the rotor.

The rotors (alternatively *wheels* or *drums* — *Walzen* in German) form the heart of an Enigma machine. Approximately 10 cm in diameter, each rotor is a disk made of hard rubber or bakelite with a series of brass spring-loaded pins on one face arranged in a circle; on the other side are a corresponding number of circular electrical contacts. The pins and contacts represent the alphabet — typically the 26 letters A–Z (this will be assumed for the rest of the description). When placed side-by-side, the pins of one rotor rest against the contacts of the neighbouring rotor, forming an electrical connection. Inside the body of the rotor, a set of 26 wires connects each pin on one side to a contact on the other in a complex pattern. The wiring differs for every rotor.



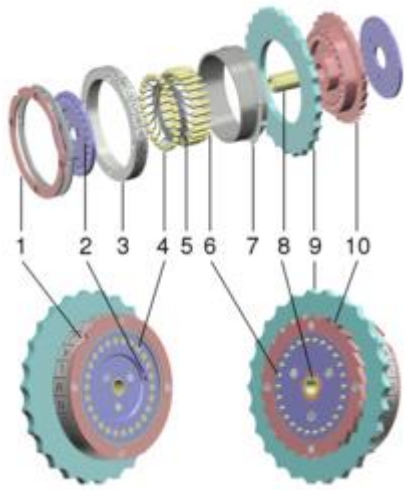
Three Enigma rotors and the shaft on which they are placed when in use.

By itself, a rotor performs only a very simple type of encryption — a simple substitution cipher. For example, the pin corresponding to the letter E might be wired to the contact for letter T on the opposite face. The complexity comes from the use of several rotors in series — usually three or four — and the regular movement of the rotors; this provides a much stronger type of encryption.

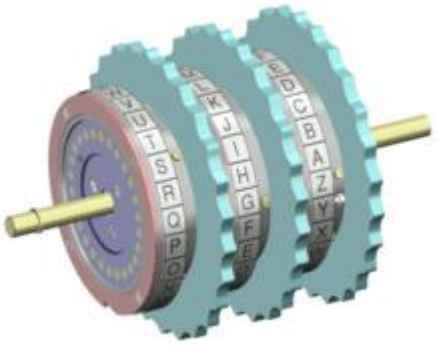
When placed in the machine, a rotor can be set to one of 26 positions. It can be turned by hand using a grooved finger-wheel which protrudes from the internal cover when closed, as shown in Figure 2. So that the operator knows the position, each rotor has an *alphabet tyre* (or letter ring) attached around the outside of the disk, with 26 letters or numbers; one of these can be seen through a window, indicating the position of the rotor to the operator. In early Enigma models, the alphabet ring is fixed; a complication introduced in later versions is the facility to adjust the alphabet ring relative to the core wiring. The position of the ring is known as the *Ringstellung* ("ring settings").

The rotors each contain a notch (sometimes multiple notches), used to control the stepping of the rotors. In the military versions, the notches are located on the alphabet ring.

Exploded view of an Enigma rotor	Three rotors in sequence



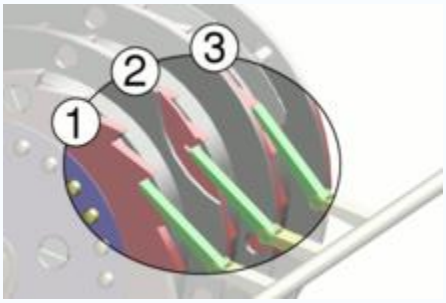
1. notched ring
2. marking dot for "A" contact
3. alphabet tyre
4. plate contacts
5. wire connections
6. pin contacts
7. spring-loaded ring adjusting lever
8. hub
9. finger wheel
10. ratchet wheel



The Army and Air Force Enigmas came equipped with several rotors; when first issued there were a total of three. On 15 December 1938, this changed to five, from which three were chosen for insertion in the machine. These were marked with Roman numerals to distinguish them: I, II, III, IV and V, all with single notches. The Naval version of the Wehrmacht Enigma had always been issued with more rotors than the other services: at first, five, then seven and finally eight. The additional rotors were named VI, VII and VIII, all with different wiring, and had two notches cut into them, resulting in a more frequent turnover.

The four-rotor Naval Enigma (M4) accommodated an extra rotor in the same space as the three-rotor version. This was accomplished by replacing the original reflector with a thinner reflector and adding a special fourth rotor. The fourth rotor can be one of two types: *Beta* or *Gamma*. This 4th rotor never steps, but can be manually placed in any of the 26 positions.

Stepping motion



Stepping motion of the Enigma. All three ratchet pawls (green) push in unison. In the first rotor (1), the ratchet (red) is always engaged, and steps with each keypress. Here, the second rotor (2) is engaged because the notch in the first rotor is aligned with the pawl; it will step with the next keypress. The third rotor (3) is not engaged, because the notch in the second rotor is not aligned; the pawl will simply slide over the curved ring.

To avoid merely implementing a simple substitution cipher, some rotors turn with consecutive presses of a key. This ensures that the cryptographic transformation is different at each position, producing a formidable polyalphabetic substitution cipher.

The most common arrangement utilises a ratchet and pawl mechanism. Each rotor is affixed with a ratchet with 26 teeth; a group of pawls engage the teeth of the ratchet. The pawls are pushed forward in unison with each keypress on the machine. If a pawl engages the teeth of a ratchet, that rotor advances by one step.

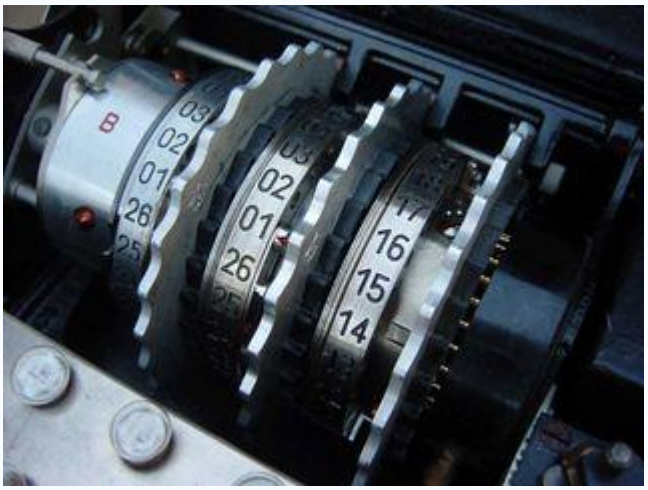
In the Wehrmacht Enigma, each rotor is affixed with an adjustable notched ring. The five basic rotors (I-V) have one notch each, while the additional naval rotors VI, VII and VIII have two notches. At a certain point, a rotor's notch will align with the pawl, allowing it to engage the ratchet of the next rotor with the subsequent key press. When a pawl is not aligned with the notch, it will simply slide over the surface of the ring without engaging the ratchet. In a single-notch rotor system, the second rotor is advanced one position every 26 advances of the first rotor. Similarly, the third rotor is advanced one position for every 26 advances of the second rotor. The second rotor also advances at the same time as the third rotor, meaning the second rotor can step twice on subsequent key presses — "double stepping" — resulting in a reduced period[1].

This double stepping causes the rotors to deviate from a normal odometer. A double step occurs as follows: the first rotor steps, and takes the second rotor one step further. If the second rotor has moved by this step into its own notch-position, the third pawl can drop down. On the next step this pawl pushes the ratchet of the third rotor and advances it, but will also push into the second rotor's notch, advancing the second rotor a second time in a row.

With three wheels and only single notches in the first and second wheels, the machine has a period of 26 × 25 × 26 = 16,900 (NOT 26 X 26 X 26 because of the double stepping of the second rotor. see bottom of page in the references section, for a link to a PDF file on this 'double stepping'). Historically, messages were limited to a couple of hundred letters, and so there was no risk of repeating any position within a single message.

To make the use of the naval fourth rotors "Beta" and "Gamma" possible, introduced in 1942, the reflector was changed to a thin model and the special thin fourth rotor was placed against it. No changes were made to the mechanism. Since there are only three pawls, the fourth rotor never steps, but can be manually set into one of its 26 positions.

When pressing a key, the rotors step before the electrical circuit is connected.



The Enigma rotor assembly. The three movable rotors are sandwiched between two fixed wheels: the entry wheel on the right and the reflector (here marked "B") on the left.

Entry wheel

The entry wheel (*Eintrittswalze* in German), or entry stator, connects the plugboard, if present, or otherwise the keyboard and lampboard to the rotor assembly. While the exact wiring used is of comparatively little importance to the security, it proved an obstacle in the progress of Polish cryptanalyst Marian Rejewski during his deduction of the rotor wirings. The commercial Enigma connects the keys in the order of their sequence on the keyboard: Q⟶A, W⟶B, E⟶C and so on. However, the military Enigma connects them in straight alphabetical order: A⟶A, B⟶B, C⟶C etc. It took an inspired piece of guesswork for Rejewski to realise the modification, and he was then able to solve the equations.

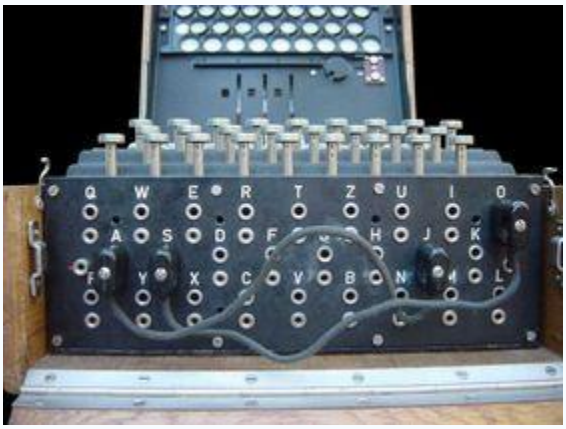
Reflector

With the exception of the early models A and B, the last rotor is followed by a *reflector* (German: *Umkehrwalze*), a patented feature distinctive of the Enigma family amongst the various rotor machines designed in the period. The reflector connects outputs of the last rotor up in pairs, redirecting current back through the rotors by a different route. The reflector ensures that Enigma is self-reciprocal: conveniently, encryption is the same as decryption. However, the reflector also gives Enigma the property that no letter can encrypt to itself. This was a severe conceptual flaw and a cryptological mistake subsequently exploited by codebreakers.

In the commercial Enigma model C, the reflector can be inserted in one of two different positions. In Model D the reflector can be set in 26 possible positions, although it does not move during encipherment. In the Abwehr Enigma, the reflector is stepped during encryption in a similar way to the other wheels.

In the German Army and Air Force Enigma, the reflector is fixed and does not rotate, and appeared in four versions. The original version was marked *A*, and was replaced by *Umkehrwalze B* on 1 November 1937. A third version, *Umkehrwalze C* was used briefly in 1940, possibly in error, and was solved by Hut 6[2]. The fourth version, first observed on 2 January 1944 is a rewireable reflector, called *Umkehrwalze D*, allowing the Enigma operator to alter the connections as part of the key settings.

Plugboard



The plugboard (*Steckerbrett*) is positioned at the front of the machine, below the keys. When in use, there can be up to 13 connections. In the above photograph, two pairs of letters are swapped (S-O and J-A).

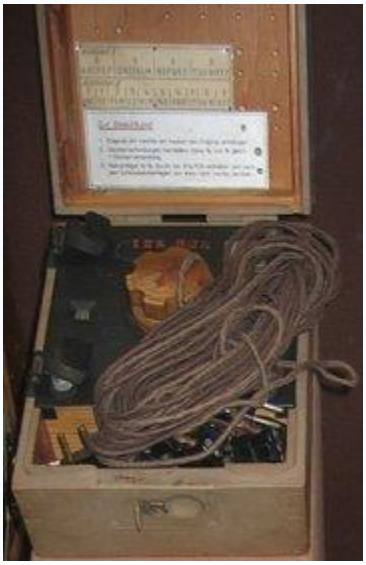
The plugboard (*Steckerbrett* in German) is a variable wiring that could be reconfigured by the operator (visible on the front panel of Figure 1; some of the patch cords can be seen in the lid). It was introduced on German Army versions in 1930 and was soon adopted by the Navy as well. The plugboard contributes a great deal to the strength of the machine's encryption, more than an extra rotor would. Enigma without a plugboard — "unsteckered" Enigma — can be solved relatively straightforwardly using hand methods; these techniques are generally defeated by the addition of a plugboard, and codebreakers resorted to special machines to solve it.

A cable placed onto the plugboard connects letters up in pairs, for example, E and Q might be a steckered pair. The effect is to swap those letters before and after the main rotor scrambling unit. For example, when an operator presses E, the signal is diverted to Q before entering the rotors. Several such steckered pairs, up to 13, might be used at one time.

Current flows from the keyboard through the plugboard, and proceeds to the entry-rotor or *Eintrittswalze*. Each letter on the plugboard has two jacks. Inserting a plug will disconnect the upper jack (from the keyboard) and the lower jack (to the entry-rotor) of that letter. The plug at the other end of the crosswired cable is inserted into another letter's jacks, switching the connections of the two letters.

The "Schreibmax" was a printing unit which could be attached to the Enigma, removing the need to laboriously read and write down the letters off the light panel.

Accessories



The Enigma Uhr attachment

A handy feature that was used on the M4 Enigma was the "Schreibmax", a little printer which could print the 26 letters on a small paper ribbon. This excluded the need for a second operator, reading the lamps and writing the letters down. The Schreibmax was placed on top of the Enigma machine and was connected to the lamp panel; to install the printer, the lamp cover and all lightbulbs had to be removed. Besides its handiness, it improved operational security: the signal officer no longer had to see the plaintext, as the printer might have been installed in the captain's cabin of a submarine, so that the signals officer did the typing and key handling but never gained knowledge of secret received plaintext information.

Another accessory was the remote lamp panel. If the machine was equipped with an extra panel, the wooden case of the Enigma was wider and could store the extra panel. There was a lamp panel version that could be connected afterwards, but that required, just as with the Schreibmax, the lamp panel and lightbulbs to be removed. The remote panel made it possible for a person to read the decrypted text, without giving the operator access to it.

In 1944, the Luftwaffe introduced an extra plugboard switch, called the Uhr (clock). There was a little box, containing a switch with 40 positions. It replaced the default plugs. After connecting the plugs, as determined in the daily key sheet, the operator could turn the switch in one of the 40 positions, each position resulting in a different combination of plug wiring. Most of these plug connection are, unlike the default plugs, not pair-wise.

Mathematical description

The Enigma transformation for each letter can be specified mathematically as a product of permutations. Assuming a three-rotor German Army/Air Force Enigma, let P denote the plugboard transformation, U denote the reflector, and L,M,R denote the actions of the left, middle and right rotors respectively. Then the encryption E can be expressed as

$$E = PRMLUL^{-1}M^{-1}R^{-1}P^{-1}$$

After each key press the rotors turn, changing the transformation. For example, if the right hand rotor R is rotated i positions, the transformation becomes $\rho^{i}R\rho^{-i}$, where ρ is the cyclic permutation mapping A to B, B to C, and so forth. Similarly, the middle and left-hand rotors can be represented as j and k rotations of M and L. The encryption function can then be described as:

$$E = P(\rho^{i}R\rho^{-i})(\rho^{j}M\rho^{-j})(\rho^{k}L\rho^{-k})U(\rho^{k}L^{-1}\rho^{-k})(\rho^{j}M^{-1}\rho^{-j})(\rho^{i}R^{-1}\rho^{-i})P^{-1}$$

Procedures for using the Enigma


In use, the Enigma required a list of daily key settings as well as a number of auxiliary documents. The procedures for German Naval Enigma were more elaborate, and secure, than the procedures used in other services. The Navy codebooks were also printed in red, water-soluble ink on pink paper so that they could easily be destroyed if they were at risk of being seized by the enemy. The above codebook was taken from captured U-boat *U-505*.

In German military usage, communications were divided up into a number of different networks, all using different settings for their Enigma machines. These communication nets were termed *keys* at Bletchley Park, and were assigned codenames, such as *Red*, *Chaffinch* and *Shark*. Each unit operating on a network was assigned a settings list specifying the Enigma for a period of time. For a message to be correctly encrypted and decrypted, both sender and receiver have to set up their Enigma in the same way; the rotor selection and order, the starting position and the plugboard connections need to be identical; these settings have to be agreed on beforehand, and were distributed in codebooks.

An Enigma machine's initial state, the cryptographic key, has several aspects:

- Wheel order (*Walzenlage*) — the choice of rotors and the order in which they are used.
- Initial position of the rotors: — chosen by the operator, different for each message.
- Ring settings (*Ringstellung*) — the position of the alphabet ring relative to the rotor wiring.
- Plug settings (*Steckerverbindungen*) — the connections of the plugs in the plugboard.

Enigma was designed to be secure even if the rotor wiring was known to an eavesdropper, although in practice the wiring was kept secret. With secret wiring, the total number of possible configurations has been calculated to be around 10^{114} (approximately 380 bits); with known wiring and other operational constraints, this is reduced to around 10^{23} (76 bits)[3]. Users of Enigma were assured of its security by the large number of possibilities; it was not feasible for an adversary to even begin to try every possible configuration in a brute force attack.

Indicators

Most of the key were kept constant for a set time period, typically a day. However, a different initial rotor position was chosen for each message, because if a number of messages are sent encrypted with identical or near-identical settings, a cryptanalyst has several messages "in depth", and might be able to attack the messages using frequency analysis. To counter this, a different starting position for the rotors was chosen for each message; a similar concept to an initialisation vector in modern cryptography. The starting position was transmitted along with the ciphertext. The exact method used is termed the "indicator procedure" — weak indicator procedures allowed the initial breaks into Enigma.

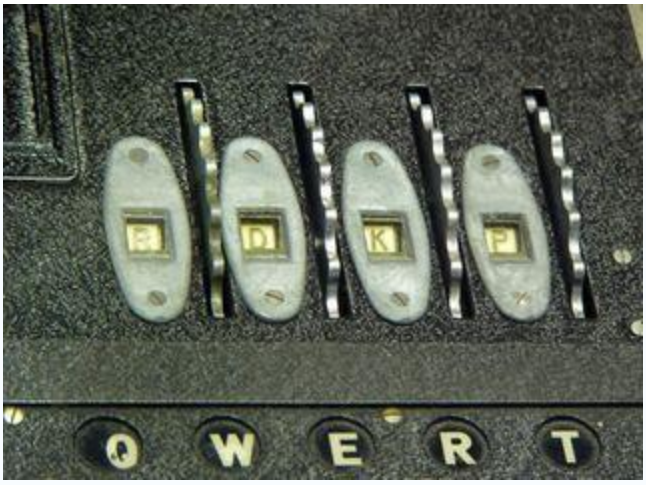


Figure 2. With the inner lid placed down, the Enigma is ready for use. The finger wheels of the rotors protrude through the lid, allowing the operator to manually set the rotors, and the current position — here RDKP — is visible to the operator through a set of windows.

One of the earliest indicator procedures was exploited to make the initial breaks into the Enigma by Polish cryptanalysts. The procedure was for the operator to set up his machine in accordance with his settings list, which included a global initial position for the rotors (*Grundstellung* — "ground setting"), AOH, say. The operator would turn his rotors until AOH was visible through the rotor windows. At this point, the operator would choose his own, arbitrary starting position for that particular message. An operator might select EIN, and this became the *message settings* for that encryption session. The operator would then type EIN into the machine, twice, to allow for detecting transmission errors. The results would be an encrypted indicator — the EIN typed twice might turn into XHTLOA, which would be transmitted along with the message. Finally, the operator would then spin the rotors to his message settings, EIN in this example, and the text of the actual message was typed in.

At the receiving end the operation was reversed. The operator set the machine to the initial settings and typed in the first six letters of the message (XHTLOA). In this example, EINEIN would be produced. By moving his rotors to EIN, the receiving operator would then type in the rest of the ciphertext, deciphering the message.

The weakness came from two factors: the use of a global ground setting — this was later changed so that the operator selected his initial position to encrypt the indicator, and sent the initial position in the clear. The second problem was the repetition of the indicator, which was actually a security flaw. The message key was encoded twice, resulting in a relation between first and fourth, second and fifth, and third and sixth character. This security problem enabled the Polish Cipher Bureau to break the pre-war Enigma messages. However, from 1940 on, the Germans changed the procedures to increase the security.

During the Second World War, German operators used the codebooks only to set up the rotors and ringsettings. For each message, he selected a random startposition, let's say WZA, and random message key, let's say SXT. He moved the rotors in the WZA startposition, and encoded the messagekey SXT. Let us presume that the result was UHL. He sets up the message key SXT as startposition, and encodes the message. Next, he transmits the startposition WZA, the encoded message key UHL together with the message. The receiver sets up the startposition according the first trigram, WZA and decodes the second trigram, UHL, to obtain the SXT message key. Next, he uses this SXT message key as startposition to decode the message. This way, each ground setting was different and the new procedure avoided the security flaw of double encoded message keys.

This procedure was used by Wehrmacht and Luftwaffe only. The Kriegsmarine procedures on sending messages with the Enigma were far more complex and elaborate. Prior to encryption with the Enigma, the message was encoded with the Kurzsignalheft code book. The Kurzsignalheft contained tables that converted sentences into four-letter groups. All kinds of expressions in many different topics were listed. Logistic matters such as refueling and rendez-vous with supply ships, positions and grid lists, names of harbors, countries, weapons, weather conditions, enemy positions and ships, date and time tables. All possible situations and topics were listed. Another codebook contained the Kenngruppen and Spruchschlüssel, resp key identification and message key. More details on Kurzsignale on German U-Boats

Abbreviations and guidelines

The Army Enigma machine only used the 26 alphabet characters. Signs were replaced by rare character combinations. A space was omitted or replaced by an X. The X was generally used as point or full stop. Some signs were different in other parts of the armed forces. The Wehrmacht replaced a comma by ZZ and the question sign by FRAGE or FRAQ. The Kriegsmarine however, replaced the comma by Y and the question sign by UD. The combination CH, as in Acht (eight) or Richtung (direction) were replaced by Q (AQT, RIQTUNG). Two, three or four zeros were replaced by CENTA MILLE and MYRIA.

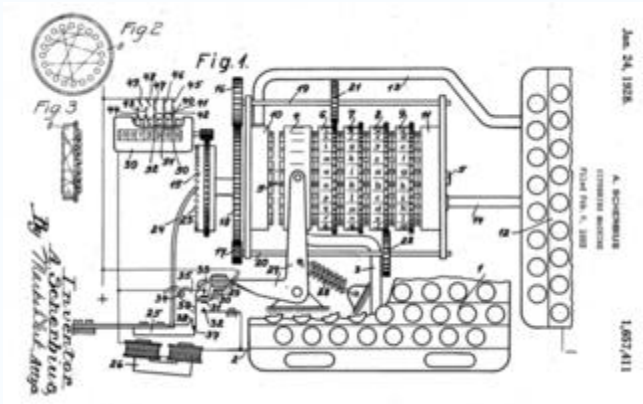
Wehrmacht and Luftwaffe transmitted the messages in groups of five characters. The Kriegsmarine, using the four rotor Enigma, applied four letter groups. Frequently used names or words were to be varied as much as possible. Words like Minensuchboot (minesweeper) could be written as MINENSUCHBOOT, MINBOOT, MMMBOOT or MMM354. To make cryptanalysis harder, more than 250 characters in one message were forbidden. Longer messages were divided in several parts, each using its own message key. For more details see Tony Sale's translations of "General Procedure"[4] and "Officer and Staff procedure"[5].

History and development of the machine

Far from being a single design, there are numerous models and variants of the Enigma family. The earliest Enigma machines were commercial models dating from the early 1920s. Starting in the mid-1920s, the various branches of the German military began to use Enigma, making a number of changes in order to increase its security. In addition, a number of other nations either adopted or adapted the Enigma design for their own cipher machines.

A selection of seven Enigma machines and paraphernalia exhibited at the USA's National Cryptologic Museum. From left to right, the models are: 1) Commercial Enigma; 2) Enigma T; 3) Enigma G; 4) Unidentified; 5) Luftwaffe (Air Force) Enigma; 6) Heer (Army) Enigma; 7) Kriegsmarine (Naval) Enigma — M4.

Commercial Enigma



Scherbius' Enigma patent — U.S. Patent 1,657,411, granted in 1928

On February 23, 1918, German engineer Arthur Scherbius applied for a patent for a cipher machine using rotors, and, with E. Richard Ritter, founded the firm of Scherbius & Ritter. They approached the German Navy and Foreign Office with their design, but neither was interested. They then assigned the patent rights to Gewerkschaft Securitas, who founded the Chiffriermaschinen Aktien-Gesellschaft (Cipher Machines Stock Corporation) on 9 July 1923; Scherbius and Ritter were on the board of directors.

The Enigma logo

Chiffriermaschinen AG began advertising a rotor machine — **Enigma model A** — which was exhibited at the Congress of the International Postal Union in 1923 and 1924. The machine was heavy and bulky, incorporating a typewriter. It measured 65×45×35 cm and weighed about 50 kg. A **model B** was introduced, and was of a similar construction[6]. While bearing the Enigma name, both models A and B were quite unlike later versions: they differed in physical size and shape, but also cryptographically, in that they lacked the reflector.

The reflector — an idea suggested by Scherbius' colleague Willi Korn — was first introduced in the **Enigma C** (1926) model. The reflector is a key feature of the Enigma machines.


A rare 8-rotor printing Enigma.

Model C was smaller and more portable than its predecessors. It lacked a typewriter, relying instead on the operator reading the lamps; hence the alternative name of "glowlamp Enigma" to distinguish from models A and B. The Enigma C quickly became extinct, giving way to the **Enigma D** (1927). This version was widely used, with copies going to Sweden, the Netherlands, England, Japan, Italy, Spain, U.S. and Poland.

Military Enigma

The German Navy were the first branch of the German military to adopt Enigma. This version, named **Funkschlüssel C** (*Radio cipher C*), had been put into production by 1925 and was introduced into service in 1926[7]. The keyboard and lampboard contained 29 letters — A-Z, Ä, Ö and Ü — which were arranged alphabetically, as opposed to the QWERTZU ordering[8]. The rotors had 28 contacts, with the letter X wired to bypass the rotors unencrypted[9]. Three rotors were chosen from a set of five[10] and the reflector could be inserted in one of four different positions, denoted α, β, γ and δ[11]. The machine was revised slightly in July 1933[12].

By 15 July 1928[13], the German Army (*Reichswehr*) had introduced their own version of the Enigma — the **Enigma G**, revised to the **Enigma I** by June 1930[14]. Enigma I is also known as the **Wehrmacht**, or **Services** Enigma, and was used extensively by the German military services and other government organisations, both prior to and during World War II. The major difference between Enigma I and commercial Enigma models was the addition of a plugboard to swap pairs of letters, greatly increasing the cryptographic strength of the machine. Other differences included the use of a fixed reflector, and the relocation of the stepping notches from the rotor body to the movable letter rings[14]. The Navy eventually agreed and in 1934[15] brought into service the Navy version of the

Army Enigma, designated **Funkschlüssel M** or **M3**. While the Army used only three rotors at that time, for greater security the Navy specified a choice of three from a possible five[16].

In December 1938, the Army issued two extra rotors so that the three rotors were chosen from a set of five[14]. In 1938, the Navy added two more rotors, and then another in 1939 to allow a choice of three rotors from a set of eight[16]. In August 1935, the Air Force also introduced the Wehrmacht Enigma for their communications[14]. A four rotor Enigma was introduced by the Navy for U-boat traffic on 1 February 1942, called **M4** (the network was known as *Triton*, or *Shark* to the Allies). The extra rotor was fitted in the same space by splitting the reflector into a combination of a thin reflector and a thin fourth rotor.

There was also a large, eight-rotor printing model, the **Enigma II**. During 1933, Polish codebreakers detected that it was in use for high-level military communications, but that it was soon withdrawn from use after it was found to be unreliable and jam frequently[17].

Enigma G, used by the Abwehr, had four-rotors, no plugboard, and multiple notches on the rotors.

The Abwehr used the **Enigma G** (the **Abwehr Enigma**). This Enigma variant was a four-wheel unsteckered machine with multiple notches on the rotors. This model was equipped with a counter which incremented upon each key press, and so is also known as the **counter machine** or the **Zahlwerk Enigma**.

The four-wheel Swiss Enigma K, made in Germany, used re-wired rotors.

Other countries also used Enigma machines. The Italian Navy adopted the commercial Enigma as "Navy Cipher D"; the Spanish also used commercial Enigma during their Civil War. British

codebreakers succeeded in breaking these machines, which lacked a plugboard. The Swiss used a version of Enigma called **model K** or **Swiss K** for military and diplomatic use, which was very similar to the commercial Enigma D. The machine was broken by a number of parties, including Poland, France, Britain and the United States (the latter codenamed it INDIGO). An **Enigma T** model (codenamed **Tirpitz**) was manufactured for use by the Japanese.

It has been estimated that 100,000 Enigma machines were constructed[18]. After the end of the Second World War, the Allies sold captured Enigma machines, still widely considered secure, to a number of developing countries[18].

Enigma derivatives

The Enigma was influential in the field of cipher machine design, and a number of other rotor machines are derived from it. The British Typex was originally designed from the Enigma patents — Typex even includes features from the patent descriptions that were omitted from the actual Enigma machine. Due to the need for secrecy about its cipher systems, no royalties were paid for the use of the patents by the British government. A Japanese Enigma clone was codenamed GREEN by American cryptographers. Little-used, it contained four rotors mounted vertically. In the US, cryptologist William Friedman designed the M-325, a machine similar to Enigma in logical operation, although not in construction.

A unique rotor machine was constructed in 2002 by Netherlands-based Tatjana van Vark[19]. This unusual device is inspired by Enigma, but makes use of 40-point rotors, allowing letters, numbers and some punctuation; each rotor contains 509 parts[20].

The Japanese developed an Enigma clone, codenamed GREEN by American cryptographers, although it was little used.

Tatjana van Vark's Enigma-inspired rotor machine, constructed in 2002. The rotors of this machine contain 40 contacts, compared to the original Enigma's 26.

Surviving Enigmas

The effort to break the Enigma was not disclosed until the 1970s. Since then, interest in the Enigma machine has grown considerably and a number of Enigmas are on public display in museums in the US and Europe. The Deutsches Museum in Munich has both the three and four-wheel German military variants, as well as several older civilian versions. There are also examples in the NSA's National Cryptologic Museum at Fort Meade and at the Computer History Museum in the United States, at Bletchley Park in the United Kingdom, the Australian War Memorial at Canberra in Australia, as well as a number of other locations in Germany, the US, the UK, and a few other countries in Europe. A number are also in private hands[21].

Occasionally, Enigma machines are sold at auction; prices of US$20,000 are not unusual[22].

Replicas of the machine are available in various forms, including an exact reconstructed copy of the Naval M4 model, an Enigma implemented in electronics (Enigma-E), various computer software simulators and paper-and-scissors analogues.

A rare Abwehr Enigma machine, designated G312, was stolen from the Bletchley Park museum on 1 April 2000. In September, a man identifying himself as "The Master" sent a note demanding £25,000 and threatened to destroy the machine if the ransom was not paid. In early October 2000, Bletchley Park officials announced that they would pay the ransom but the deadline set passed with no word from the thief. Shortly after the ransom deadline passed the machine was sent anonymously to BBC journalist Jeremy Paxman, but three rotors were missing. In November 2000, an antiques dealer named Dennis Yates was arrested after telephoning *The Sunday Times* to arrange the return of the missing parts. The Enigma machine was returned to Bletchley park after the incident. In October 2001, Yates was sentenced to ten months in prison after admitting handling the stolen machine and of blackmailing Bletchley Park Trust director Christine Large, although he maintained that he was acting as an intermediary for a third party. Yates was released from prison after serving three months.

See also

- Operation Most III

World War II Era Encryption Devices:

- Sigaba (*United States*)
- Typex (*Britain*)
- Lorenz SZ 40/42 (*Germany*) (Allied code-name: 'Tunny')
- Siemens and Halske T52 (*Germany*) (Allied code-name: 'Sturgeon').
- Geheimschreiber

External links

- **Enigma machine**
  - Enigma rotor details
- Cryptanalysis of the Enigma
  - Cyclometer
  - Perforated sheets
  - Bomba
  - Bombe
  - Ultra

- Several images of Enigma
- Detailed photos of various Enigma models and parts
- Pictures of a four-rotor naval enigma, including Flash (SWF) views of the machine

Descriptions

- *The Enigma cipher machine*, by Tony Sale
- *Enigma — a very famous story of cryptology* by Martin Oberzalek
- The origins of the Enigma/ULTRA by Dr. Wladyslaw Kozaczuk

Simulators and replicas

- A project to construct an accurate M4 Enigma replica
- Enigma-E — a DIY electronics kit which simulates an Enigma machine
- Enigma simulator (Macromedia Flash)
- Enigma simulator Wehrmacht, Luftwaffe, Kriegmarine M3 and M4 (Microsoft Windows software)
- Enigma simulator (Java applet)
- Enigma simulator (Paper cut-out)
- Wiring of the Enigma rotors: [10], [11]

Miscellaneous

- David Hamer's Enigma pages — includes a list of known surviving Enigmas and selling prices
- Archives of all German military manuals — also for secret manuals of Enigma and Cryptography
- Enigma Cipher Challenge — competition to deciphering 10 messages
- Samples of real Enigma messages