Enigma machine

The **Enigma machine** is a cipher device developed and used in the early- to mid-20th century to protect commercial, diplomatic, and military communication. It was employed extensively by Nazi Germany during World War II, in all branches of the German military. The Enigma machine was considered so secure that it was used to encipher the most top-secret messages.[1]

Military Enigma machine, model "Enigma I", used during the late 1930s and during the war; displayed at Museo Nazionale Scienza e Tecnologia Leonardo da Vinci, Milan, Italy

The Enigma has an electromechanical rotor mechanism that scrambles the 26 letters of the alphabet. In typical use, one person enters text on the Enigma's keyboard and another person writes down which of the 26 lights above the keyboard illuminated at each key press. If plain text is entered, the illuminated letters are the ciphertext. Entering ciphertext transforms it back into readable plaintext. The rotor mechanism changes the electrical connections between the keys and the lights with each keypress.

The security of the system depends on machine settings that were generally changed daily, based on secret key lists distributed in advance, and on other settings that were changed for each message. The receiving station would have to know and use the exact settings employed by the transmitting station to successfully decrypt a message.

While Nazi Germany introduced a series of improvements to the Enigma over the years, and these hampered decryption efforts, they did not prevent Poland from cracking the machine as early as December 1932 and reading messages prior to and into the war. Poland's sharing of her achievements enabled the western Allies to exploit Enigma-enciphered messages as a major source of intelligence.[2] Many commentators say the flow of Ultra communications intelligence from the decrypting of Enigma, Lorenz, and other ciphers shortened the war substantially and may even have altered its outcome.[3]

History

The Enigma machine was invented by German engineer Arthur Scherbius at the end of World War I.[4] The German firm Scherbius & Ritter, co-founded by Scherbius, patented ideas for a cipher machine in 1918 and began marketing the finished product under the brand name *Enigma* in 1923, initially targeted at commercial markets.[5] Early models were used commercially from the early 1920s, and adopted by military and government services of several countries, most notably Nazi Germany before and during World War II.[6]

Several different Enigma models were produced, but the German military models, having a plugboard, were the most complex. Japanese and Italian models were also in use.[7] With its adoption (in slightly modified form) by the German Navy in 1926 and the German Army and Air Force soon after, the name *Enigma* became widely known in military circles. Pre-war German military planning emphasized fast, mobile forces and tactics, later known as blitzkrieg, which depend on radio communication for command and coordination. Since adversaries would likely intercept radio signals, messages had to be protected with secure encipherment. Compact and easily portable, the Enigma machine filled that need.

Breaking Enigma

A memorial in Bydgoszcz, Poland, to Marian Rejewski, the mathematician who, in 1932, first broke Enigma and, in July 1939, helped educate the French and British about Polish methods of Enigma decryption

Around December 1932 Marian Rejewski, a Polish mathematician and cryptologist at the Polish Cipher Bureau, used the theory of permutations,[8] and flaws in the German military-message encipherment procedures, to break message keys of the plugboard Enigma machine.[9] France's spy Hans-Thilo Schmidt obtained access to German cipher materials that included the daily keys used in September and October 1932. Those keys included the plugboard settings. The French passed the material to the Poles, and Rejewski used some of that material and the message traffic in September and October to solve for the unknown rotor wiring. Consequently the Polish mathematicians were able to build their own Enigma machines, dubbed "Enigma doubles". Rejewski was aided by fellow mathematician-cryptologists Jerzy Różycki and Henryk Zygalski, both of whom had been recruited with Rejewski from Poznań University, which had been selected for its students' knowledge of the German language, since that area was held by Germany prior to World War I. The Polish Cipher Bureau developed techniques to defeat the plugboard and find all components of the daily key, which enabled the Cipher Bureau to read German Enigma messages starting from January 1933.

Over time, the German cryptographic procedures improved, and the Cipher Bureau developed techniques and designed mechanical devices to continue reading Enigma traffic. As part of that effort, the Poles exploited quirks of the rotors, compiled catalogues, built a cyclometer (invented by Rejewski) to help make a catalogue with 100,000 entries, invented and produced Zygalski sheets, and built the electromechanical cryptologic *bomba* (invented by Rejewski) to search for rotor settings. In 1938 the Poles had six *bomby* (plural of *bomba*), but when that year the Germans added two more rotors, ten times as many *bomby* would have been needed to read the traffic.[10]

On 26 and 27 July 1939,[11] in Pyry, just south of Warsaw, the Poles initiated French and British military intelligence representatives into the Polish Enigma-decryption techniques and equipment, including Zygalski sheets and the cryptologic bomb, and promised each delegation a Polish-reconstructed Enigma (the devices were soon delivered).[12]

In September 1939, British Military Mission 4, which included Colin Gubbins and Vera Atkins, went to Poland, intending to evacuate cipher-breakers Marian Rejewski, Jerzy Różycki, and Henryk Zygalski from the country. The cryptologists, however, had been evacuated by their own superiors

into Romania, at the time a Polish-allied country. On the way, for security reasons, the Polish Cipher Bureau personnel had deliberately destroyed their records and equipment. From Romania they traveled on to France, where they resumed their cryptological work, collaborating by teletype with the British, who began work on decrypting German Enigma messages, using the Polish equipment and techniques.[13]

Gordon Welchman, who became head of Hut 6 at Bletchley Park, has written: "Hut 6 Ultra would never have gotten off the ground if we had not learned from the Poles, in the nick of time, the details both of the German military version of the commercial Enigma machine, and of the operating procedures that were in use."[14] The Polish transfer of theory and technology at Pyry formed the crucial basis for the subsequent World War II British Enigma-decryption effort at Bletchley Park, where Welchman worked.

During the war, British cryptologists decrypted a vast number of messages enciphered on Enigma. The intelligence gleaned from this source, codenamed "Ultra" by the British, was a substantial aid to the Allied war effort.[a]

Though Enigma had some cryptographic weaknesses, in practice it was German procedural flaws, operator mistakes, failure to systematically introduce changes in encipherment procedures, and Allied capture of key tables and hardware that, during the war, enabled Allied cryptologists to succeed.[15][16]

From October 1944, the German Abwehr used the Schlüsselgerät 41.

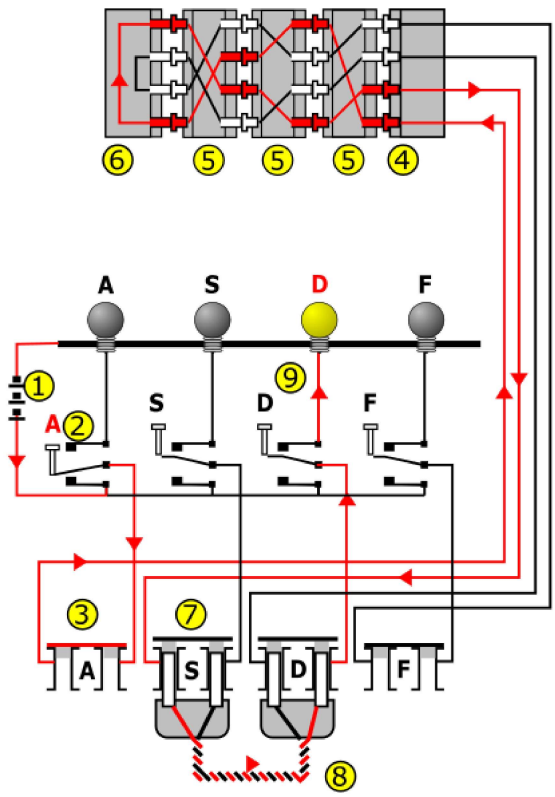
Design

Like other rotor machines, the Enigma machine is a combination of mechanical and electrical subsystems. The mechanical subsystem consists of a keyboard; a set of rotating disks called *rotors* arranged adjacently along a spindle; one of various stepping components to turn at least one rotor with each key press, and a series of lamps, one for each letter. These design features are the reason that the Enigma machine was originally referred to as the rotor-based cipher machine during its intellectual inception in 1915.[17]

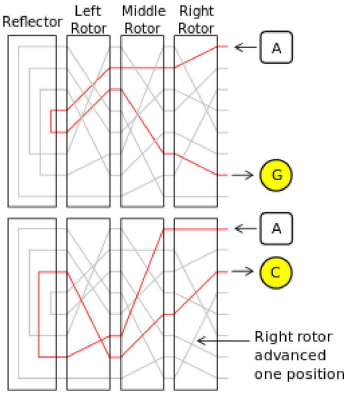
Enigma in use, 1943

Electrical pathway

An electrical pathway is a route for current to travel. By manipulating this phenomenon the Enigma machine was able to scramble messages.[17] The mechanical parts act by forming a varying electrical circuit. When a key is pressed, one or more rotors rotate on the spindle. On the sides of the rotors are a series of electrical contacts that, after rotation, line up with contacts on the other rotors or fixed wiring on either end of the spindle. When the rotors are properly aligned, each key on the keyboard is connected to a unique electrical pathway through the series of contacts and internal wiring. Current, typically from a battery, flows through the pressed key, into the newly configured set of circuits and back out again, ultimately lighting one display lamp, which shows 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, so *Z* would be the first letter of the ciphertext. The operator would next press *N*, and then *X* in the same fashion, and so on.



Enigma wiring diagram with arrows and the numbers 1 to 9 showing how current flows from key depression to a lamp being lit. The *A* key is encoded to the *D* lamp. D yields A, but A never yields A; this property was due to a patented feature unique to the Enigmas, and could be exploited by cryptanalysts in some situations.



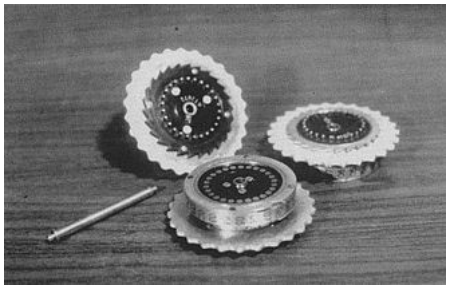
The scrambling action of Enigma's rotors is shown for two consecutive letters with the right-hand rotor moving one position between them.

Current flows from the battery (1) through a depressed bi-directional keyboard switch (2) to the plugboard (3). Next, it passes through the (unused in this instance, so shown closed) plug "A" (3) via the entry wheel (4), through the wiring of the three (Wehrmacht Enigma) or four (*Kriegsmarine* M4 and *Abwehr* variants) installed rotors (5), and enters the reflector (6). The reflector returns the current, via an entirely different path, back through the rotors (5) and entry wheel (4), proceeding through plug "S" (7) connected with a cable (8) to plug "D", and another bi-directional switch (9) to light the appropriate lamp.[18]

The repeated changes of electrical path through an Enigma scrambler implement a polyalphabetic substitution cipher that provides Enigma's security. The diagram on the right shows how the electrical pathway changes with each key depression, which causes rotation of at least the right-hand rotor. Current passes into the set of rotors, into and back out of the reflector, and out through the rotors again. The greyed-out lines are other possible paths within each rotor; these are hard-wired from one side of each rotor to the other. The letter *A* encrypts differently with consecutive key presses, first to *G*, and then to *C*. This is because the right-hand rotor steps (rotates one position) on each key press, sending the signal on a completely different route. Eventually other rotors step with a key press.

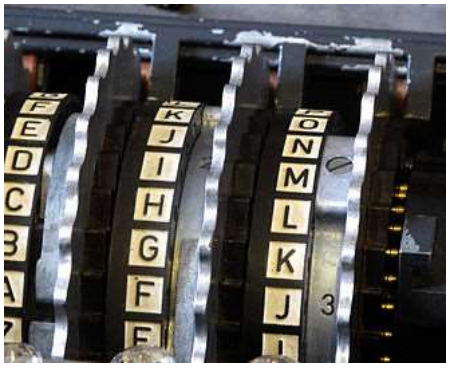
Rotors

The rotors (alternatively *wheels* or *drums*, *Walzen* in German) form the heart of an Enigma machine. Each rotor is a disc approximately 10 cm (3.9 in) in diameter made from Ebonite or Bakelite with 26 brass, spring-loaded, electrical contact pins arranged in a circle on one face, with the other face housing 26 corresponding electrical contacts in the form of circular plates. The pins and contacts represent the alphabet — typically the 26 letters A–Z, as will be assumed for the rest of this description. When the rotors are mounted side by side on the spindle, the pins of one rotor rest against the plate contacts of the neighbouring rotor, forming an electrical connection. Inside the body of the rotor, 26 wires connect each pin on one side to a contact on the other in a complex pattern. Most of the rotors are identified by Roman numerals, and each issued copy of rotor I, for instance, is wired identically to all others. The same is true for the special thin beta and gamma rotors used in the M4 naval variant.



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, and so on. Enigma's security comes from using several rotors in series (usually three or four) and the regular stepping movement of the rotors, thus implementing a polyalphabetic substitution cipher.



Enigma rotor assembly. In the Wehrmacht Enigma, the three installed movable rotors are sandwiched between two fixed wheels: the entry wheel, on the right, and the reflector on the left.

Each rotor can be set to one of 26 possible starting positions when placed in an Enigma machine. After insertion, a rotor can be turned to the correct position by hand, using the grooved finger-wheel which protrudes from the internal Enigma cover when closed. In order for the operator to know the rotor's position, each has an *alphabet tyre* (or letter ring) attached to the outside of the rotor disc, with 26 characters (typically letters); one of these is visible through the window for that slot in the cover, thus indicating the rotational position of the rotor. In early models, the alphabet ring was fixed to the rotor disc. A later improvement was the ability to adjust the alphabet ring relative to the rotor disc. The position of the ring was known as the *Ringstellung* ("ring setting"), and that setting was a part of the initial setup needed prior to an operating session. In modern terms it was a part of the initialization vector.

Two Enigma rotors showing electrical contacts, stepping ratchet (on the left) and notch (on the right-hand rotor opposite **D**).

Each rotor contains one or more notches that control rotor stepping. In the military variants, the notches are located on the alphabet ring.

The Army and Air Force Enigmas were used with several rotors, initially three. On 15 December 1938, this changed to five, from which three were chosen for a given session. Rotors were marked with Roman numerals to distinguish them: I, II, III, IV and V, all with single notches located at different points on the alphabet ring. This variation was probably intended as a security measure, but ultimately allowed the Polish Clock Method and British Banburismus attacks.

The Naval version of the *Wehrmacht* Enigma had always been issued with more rotors than the other services: At first six, then seven, and finally eight. The additional rotors were marked VI, VII and VIII, all with different wiring, and had two notches, resulting in more frequent turnover. The four-rotor Naval Enigma (M4) machine accommodated an extra rotor in the same space as the three-rotor version. This was accomplished by replacing the original reflector with a thinner one and by adding a

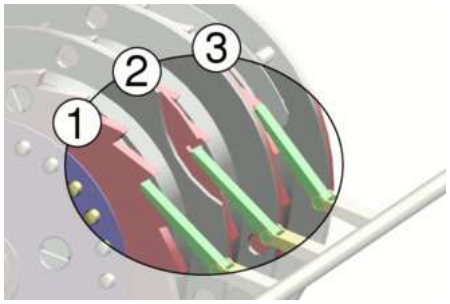
thin fourth rotor. That fourth rotor was one of two types, *Beta* or *Gamma*, and never stepped, but could be manually set to any of 26 positions. One of the 26 made the machine perform identically to the three-rotor machine.

Stepping

To avoid merely implementing a simple (solvable) substitution cipher, every key press caused one or more rotors to step by one twenty-sixth of a full rotation, before the electrical connections were made. This changed the substitution alphabet used for encryption, ensuring that the cryptographic substitution was different at each new rotor position, producing a more formidable polyalphabetic substitution cipher. The stepping mechanism varied slightly from model to model. The right-hand rotor stepped once with each keystroke, and other rotors stepped less frequently.

Turnover

The advancement of a rotor other than the left-hand one was called a *turnover* by the British. This was achieved by a ratchet and pawl mechanism. Each rotor had a ratchet with 26 teeth and every time a key was pressed, the set of spring-loaded pawls moved forward in unison, trying to engage with a ratchet. The alphabet ring of the rotor to the right normally prevented this. As this ring rotated with its rotor, a notch machined into it would eventually align itself with the pawl, allowing it to engage with the ratchet, and advance the rotor on its left. The right-hand pawl, having no rotor and ring to its right, stepped its rotor with every key depression.[19] For a single-notch rotor in the right-hand position, the middle rotor stepped once for every 26 steps of the right-hand rotor. Similarly for rotors two and three. For a two-notch rotor, the rotor to its left would turn over twice for each rotation.



The Enigma stepping motion seen from the side away from the operator. All three ratchet pawls (green) push in unison as a key is depressed. For the first rotor (1), which to the operator is the right-hand rotor, the ratchet (red) is always engaged, and steps with each keypress. Here, the middle rotor (2) is engaged, because the notch in the first rotor is aligned with the pawl; it will step (*turn over*) with the first rotor. The third rotor (3) is not engaged, because the notch in the second rotor is not aligned to the pawl, so it will not engage with the rachet.

The first five rotors to be introduced (I–V) contained one notch each, while the additional naval rotors VI, VII and VIII each had two notches. The position of the notch on each rotor was determined by the letter ring which could be adjusted in relation to the core containing the interconnections. The points on the rings at which they caused the next wheel to move were as follows.[20]

Position of turnover notches

Rotor	Turnover position(s)	BP mnemonic
I	R	Royal
II	F	Flags
III	W	Wave
IV	K	Kings
V	A	Above
VI, VII and VIII	A and N	

The design also included a feature known as *double-stepping*. This occurred when each pawl aligned with both the ratchet of its rotor and the rotating notched ring of the neighbouring rotor. If a pawl engaged with a ratchet through alignment with a notch, as it moved forward it pushed against both the ratchet and the notch, advancing both rotors. In a three-rotor machine, double-stepping affected rotor two only. If, in moving forward, the ratchet of rotor three was engaged, rotor two would move again on the subsequent keystroke, resulting in two consecutive steps. Rotor two also pushes rotor one forward after 26 steps, but since rotor one moves forward with every keystroke anyway, there is no double-stepping.[19] This double-stepping caused the rotors to deviate from odometer-style regular motion.

With three wheels and only single notches in the first and second wheels, the machine had a period of 26×25×26 = 16,900 (not 26×26×26, because of double-stepping).[19] Historically, messages were limited to a few hundred letters, and so there was no chance of repeating any combined rotor position during a single session, denying cryptanalysts valuable clues.

To make room for the Naval fourth rotors, the reflector was made much thinner. The fourth rotor fitted into the space made available. No other changes were made, which eased the changeover. Since there were only three pawls, the fourth rotor never stepped, but could be manually set into one of 26 possible positions.

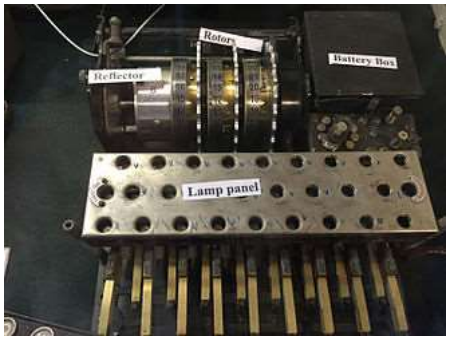
A device that was designed, but not implemented before the war's end, was the *Lückenfüllerwalze* (gap-fill wheel) that implemented irregular stepping. It allowed field configuration of notches in all 26 positions. If the number of notches was a relative prime of 26 and the number of notches were different for each wheel, the stepping would be more unpredictable. Like the Umkehrwalze-D it also allowed the internal wiring to be reconfigured.[21]

Entry wheel

The current entry wheel (*Eintrittswalze* in German), or entry stator, connects the plugboard to the rotor assembly. If the plugboard is not present, the entry wheel instead connects the keyboard and lampboard to the rotor assembly. While the exact wiring used is of comparatively little importance to security, it proved an obstacle to Rejewski's progress during his study of the rotor wirings. The

commercial Enigma connects the keys in the order of their sequence on a QWERTZ keyboard: *Q*→*A*, *W*→*B*, *E*→*C* and so on. The military Enigma connects them in straight alphabetical order: *A*→*A*, *B*→*B*, *C*→*C*, and so on. It took inspired guesswork for Rejewski to penetrate the modification.

Reflector



Internal mechanism of an Enigma machine showing the type B reflector and rotor stack.

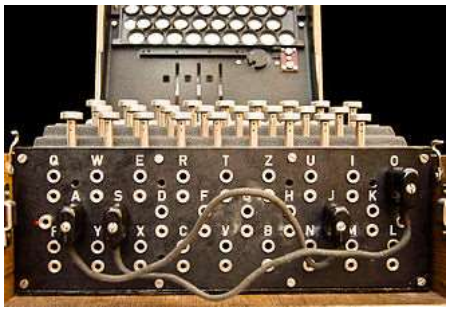
With the exception of models *A* and *B*, the last rotor came before a 'reflector' (German: *Umkehrwalze*, meaning 'reversal rotor'), a patented feature[22] unique to Enigma among the period's various rotor machines. The reflector connected outputs of the last rotor in pairs, redirecting current back through the rotors by a different route. The reflector ensured that Enigma would be self-reciprocal; thus, with two identically configured machines, a message could be encrypted on one and decrypted on the other, without the need for a bulky mechanism to switch between encryption and decryption modes. The reflector allowed a more compact design, but it also gave Enigma the property that no letter ever encrypted to itself. This was a severe cryptological flaw that was subsequently exploited by codebreakers.

In Model 'C', the reflector could be inserted in one of two different positions. In Model 'D', the reflector could be set in 26 possible positions, although it did not move during encryption. In the *Abwehr* Enigma, the reflector stepped during encryption in a manner similar to the other wheels.

In the German Army and Air Force Enigma, the reflector was fixed and did not rotate; there were four versions. The original version was marked 'A',[23] and was replaced by *Umkehrwalze B* on 1 November 1937. A third version, *Umkehrwalze C* was used briefly in 1940, possibly by mistake, and was solved by Hut 6.[24] The fourth version, first observed on 2 January 1944, had a rewireable reflector, called *Umkehrwalze D*, nick-named Uncle Dick by the British, allowing the Enigma operator to alter the connections as part of the key settings.

Plugboard

The plugboard (*Steckerbrett* in German) permitted 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 1928,[25] and was soon adopted by the *Reichsmarine* (German Navy). The plugboard contributed more cryptographic strength than an extra rotor, as it had 150 trillion possible settings (see below).[26] Enigma without a plugboard (known as *unsteckered Enigma*) could be solved relatively straightforwardly using hand methods; these techniques were generally defeated by the plugboard, driving Allied cryptanalysts to develop special machines to solve it.



The plugboard (*Steckerbrett*) was positioned at the front of the machine, below the keys. When in use during World War II, there were ten connections. In this photograph, just two pairs of letters have been swapped (A↔J and S↔O).

A cable placed onto the plugboard connected letters in pairs; for example, *E* and *Q* might be a steckered pair. The effect was to swap those letters before and after the main rotor scrambling unit. For example, when an operator pressed *E*, the signal was diverted to *Q* before entering the rotors. Up to 13 steckered pairs might be used at one time, although only 10 were normally used.

Current flowed from the keyboard through the plugboard, and proceeded to the entry-rotor or *Eintrittswalze*. Each letter on the plugboard had two jacks. Inserting a plug disconnected 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 was inserted into another letter's jacks, thus switching the connections of the two letters.

Accessories

Other features made various Enigma machines more secure or more convenient.[27]

The *Schreibmax* was a printing unit which could be attached to the Enigma, removing the need for laboriously writing down the letters indicated on the light panel.

Schreibmax

Some M4 Enigmas used the *Schreibmax*, a small printer that could print the 26 letters on a narrow paper ribbon. This eliminated the need for a second operator to read the lamps and transcribe the letters. 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 light bulbs had to be removed. It improved both convenience and operational security; the printer could be installed remotely such that the signal officer operating the machine no longer had to see the decrypted plaintext.

Fernlesegerät

Another accessory was the remote lamp panel *Fernlesegerät*. For machines equipped with the extra panel, the wooden case of the Enigma was wider and could store the extra panel. A lamp panel version could be connected afterwards, but that required, as with the *Schreibmax*, that the lamp panel and light bulbs be removed.[18] The remote panel made it possible for a person to read the decrypted plaintext without the operator seeing it.

Uhr

In 1944, the *Luftwaffe* introduced a plugboard switch, called the *Uhr* (clock), a small box containing a switch with 40 positions. It replaced the standard plugs. After connecting the plugs, as determined in the daily key sheet, the operator turned the switch into one of the 40 positions, each producing a different combination of plug wiring. Most of these plug connections were, unlike the default plugs, not pair-wise.[18] In one switch position, the *Uhr* did not swap letters, but simply emulated the 13 stecker wires with plugs.

Mathematical analysis

The Enigma transformation for each letter can be specified mathematically as a product of permutations.[8] Assuming a three-rotor German Army/Air Force Enigma, let P denote the plugboard transformation, U denote that of the reflector, and L, M, R denote those 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 n positions, the transformation becomes

$$\rho^{n}R\rho^{-n},$$

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 transformation can then be described as

$$E = P\left(\rho^{n}R\rho^{-n}\right)\left(\rho^{j}M\rho^{-j}\right)\left(\rho^{k}L\rho^{-k}\right)U\left(\rho^{k}L^{-1}\rho^{-k}\right)\left(\rho^{j}M^{-1}\rho^{-j}\right)\left(\rho^{n}R^{-1}\rho^{-n}\right)P^{-1}.$$

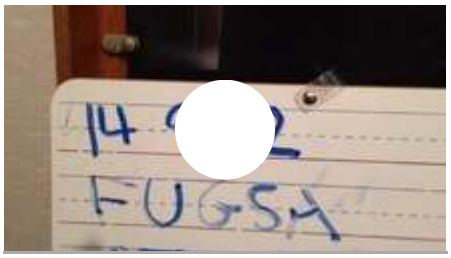
Combining three rotors from a set of five, each of the 3 rotor settings with 26 positions, and the plugboard with ten pairs of letters connected, the military Enigma has 158,962,555,217,826,360,000 different settings (nearly 159 quintillion or about 67 bits).[26]

The Enigma Uhr attachment

Operation

Basic operation

A German Enigma operator would be given a plaintext message to encrypt. After setting up his machine, he would type the message on the Enigma keyboard. For each letter pressed, one lamp lit indicating a different letter according to a pseudo-random substitution determined by the electrical pathways inside the machine. The letter indicated by the lamp would be recorded, typically by a second operator, as the cyphertext letter. The action of pressing a key also moved one or more rotors so that the next key press used a different electrical pathway, and thus a different substitution would occur even if the same plaintext letter were entered again. For each key press there was rotation of at least the right hand rotor and less often the other two, resulting in a different substitution alphabet being used for every letter in the message. This process continued until the message was completed. The cyphertext recorded by the second operator would then be transmitted, usually by radio in Morse code, to an operator of another Enigma

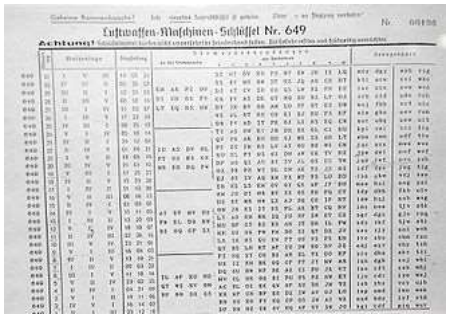


Enciphering and deciphering using an Enigma machine

machine. This operator would type in the cyphertext and — as long as all the settings of the deciphering machine were identical to those of the enciphering machine — for every key press the reverse substitution would occur and the plaintext message would emerge.

Details

German Kenngruppenheft (a U-boat codebook with grouped key codes).



Monthly key list number 649 for the German Air Force Enigma, including settings for the reconfigurable reflector (which only change once every eight days).

In use, the Enigma required a list of daily key settings and auxiliary documents. In German military practice, communications were divided into separate networks, each using different settings. These communication nets were termed *keys* at Bletchley Park, and were assigned code names, such as *Red*, *Chaffinch*, and *Shark*. Each unit operating in a network was given the same settings list for its Enigma, valid for a period of time. The procedures for German Naval Enigma were more elaborate and more secure than those in other services and employed auxiliary codebooks. Navy codebooks were printed in red, water-soluble ink on pink paper so that they could easily be destroyed if they were endangered or if the vessel was sunk.

An Enigma machine's setting (its cryptographic key in modern terms; *Schlüssel* in German) specified each operator-adjustable aspect of the machine:

- Wheel order (*Walzenlage*) – the choice of rotors and the order in which they are fitted.
- Ring settings (*Ringstellung*) – the position of each alphabet ring relative to its rotor wiring.
- Plug connections (*Steckerverbindungen*) – the pairs of letters in the plugboard that are connected together.
- In very late versions, the wiring of the reconfigurable reflector.
- Starting position of the rotors (*Grundstellung*) – chosen by the operator, should be different for each message.

For a message to be correctly encrypted and decrypted, both sender and receiver had to configure their Enigma in the same way; rotor selection and order, ring positions, plugboard connections and starting rotor positions must be identical. Except for the starting positions, these settings were established beforehand, distributed in key lists and changed daily. For example, the settings for the 18th day of the month in the German Luftwaffe Enigma key list number 649 (see image) were as follows:

- Wheel order: IV, II, V
- Ring settings: 15, 23, 26
- Plugboard connections: EJ OY IV AQ KW FX MT PS LU BD
- Reconfigurable reflector wiring: IU AS DV GL FT OX EZ CH MR KN BQ PW
- Indicator groups: lsa zbw vcj rxn

Enigma was designed to be secure even if the rotor wiring was known to an opponent, although in practice considerable effort protected the wiring configuration. If the wiring is secret, the total number of possible configurations has been calculated to be around 3×10^{114} (approximately 380

bits); with known wiring and other operational constraints, this is reduced to around 10^{23} (76 bits).[28] Because of the large number of possibilities, users of Enigma were confident of its security; it was not then feasible for an adversary to even begin to try a brute-force attack.

Indicator

Most of the key was kept constant for a set time period, typically a day. A different initial rotor position was used for each message, a concept similar to an initialisation vector in modern cryptography. The reason is that encrypting many messages with identical or near-identical settings (termed in cryptanalysis as being *in depth*), would enable an attack using a statistical procedure such as Friedman's Index of coincidence.[29] The starting position for the rotors was transmitted just before the ciphertext, usually after having been enciphered. The exact method used was termed the *indicator procedure*. Design weakness and operator sloppiness in these indicator procedures were two of the main weaknesses that made cracking Enigma possible.

Figure 2. With the inner lid down, the Enigma was ready for use. The finger wheels of the rotors protruded through the lid, allowing the operator to set the rotors, and their current position, here *RDKP*, was visible to the operator through a set of windows.

One of the earliest *indicator procedures* for the Enigma was cryptographically flawed and allowed Polish cryptanalysts to make the initial breaks into the plugboard Enigma. The procedure had the operator set his machine in accordance with the secret settings that all operators on the net shared. The settings included an initial position for the rotors (the *Grundstellung*), say, *AOH*. The operator turned his rotors until *AOH* was visible through the rotor windows. At that point, the operator chose his own arbitrary starting position for the message he would send. An operator might select *EIN*, and that became the *message setting* for that encryption session. The operator then typed *EIN* into the machine twice, this producing the encrypted indicator, for example *XHTLOA*. This was then transmitted, at which point the operator would turn the rotors to his message settings, *EIN* in this example, and then type the plaintext of the message.

At the receiving end, the operator set the machine to the initial settings (*AOH*) and typed in the first six letters of the message (*XHTLOA*). In this example, *EINEIN* emerged on the lamps, so the operator would learn the *message setting* that the sender used to encrypt this message. The receiving operator would set his rotors to *EIN*, type in the rest of the ciphertext, and get the deciphered message.

This indicator scheme had two weaknesses. First, the use of a global initial position (*Grundstellung*) meant all message keys used the same polyalphabetic substitution. In later indicator procedures, the operator selected his initial position for encrypting the indicator and sent that initial position in the clear. The second problem was the repetition of the indicator, which was a serious security flaw. The message setting was encoded twice, resulting in a relation between first and fourth, second and fifth, and third and sixth character. These security flaws enabled the Polish Cipher Bureau to break into the pre-war Enigma system as early as 1932. The early indicator procedure was subsequently described by German cryptanalysts as the "faulty indicator technique".[30]

During World War II, codebooks were only used each day to set up the rotors, their ring settings and the plugboard. For each message, the operator selected a random start position, let's say *WZA*, and a random message key, perhaps *SXT*. He moved the rotors to the *WZA* start position and encoded the

message key *SXT*. Assume the result was *UHL*. He then set up the message key, *SXT*, as the start position and encrypted the message. Next, he transmitted the start position, *WZA*, the encoded message key, *UHL*, and then the ciphertext. The receiver set up the start position according to the first trigram, *WZA*, and decoded the second trigram, *UHL*, to obtain the *SXT* message setting. Next, he used this *SXT* message setting as the start position to decrypt the message. This way, each ground setting was different and the new procedure avoided the security flaw of double encoded message settings.[31]

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 the message was encoded using the *Kurzsignalheft* code book. The *Kurzsignalheft* contained tables to convert sentences into four-letter groups. A great many choices were included, for example, logistic matters such as refuelling and rendezvous with supply ships, positions and grid lists, harbour names, countries, weapons, weather conditions, enemy positions and ships, date and time tables. Another codebook contained the *Kenngruppen* and *Spruchschlüssel*: the key identification and message key.[32]

Additional details

The Army Enigma machine used only the 26 alphabet characters. Punctuation was replaced with rare character combinations. A space was omitted or replaced with an X. The X was generally used as full-stop.

Some punctuation marks were different in other parts of the armed forces. The *Wehrmacht* replaced a comma with ZZ and the question mark with FRAGE or FRAQ.

The *Kriegsmarine* replaced the comma with Y and the question mark with UD. The combination CH, as in "*Acht*" (eight) or "*Richtung*" (direction), was replaced with Q (AQT, RIQTUNG). Two, three and four zeros were replaced with CENTA, MILLE and MYRIA.

The *Wehrmacht* and the *Luftwaffe* transmitted messages in groups of five characters and counted the letters.

The *Kriegsmarine* used four-character groups and counted those groups.

Frequently used names or words were varied as much as possible. Words like *Minensuchboot* (minesweeper) could be written as MINENSUCHBOOT, MINBOOT or MMMBOOT. To make cryptanalysis harder, messages were limited to 250 characters. Longer messages were divided into several parts, each using a different message key.[33][34]

Example enciphering process

The character substitutions by the Enigma machine as a whole can be expressed as a string of letters with each position occupied by the character that will replace the character at the corresponding position in the alphabet. For example, a given machine configuration that enciphered A to L, B to U, C to S, ..., and Z to J could be represented compactly as

```
LUSHQOXDMZNAIKFREPCYBWVGTJ
```

and the enciphering of a particular character by that configuration could be represented by highlighting the enciphered character as in

```
D > LUS(H)QOXDMZNAIKFREPCYBWVGTJ
```

Since the operation of an Enigma machine enciphering a message is a series of such configurations, each associated with a single character being enciphered, a sequence of such representations can be used to represent the operation of the machine as it enciphers a message. For example, the process of enciphering the first sentence of the main body of the famous "Dönitz message"[35] to

```
RBBF PMHP HGCZ XTDY GAHG UFXG EWKB LKGJ
```

can be represented as

```
0001 F > KGWNT(R)BLQPAHYDVJIFXEZOCSMU CDTK 25 15 16 26
0002 O > UORYTQSLWXZHNM(B)VFCGEAPIJDK CDTL 25 15 16 01
0003 L > HLNRSKJAMGF(B)ICUQPDEYOZXWTV CDTM 25 15 16 02
0004 G > KPTXIG(F)MESAUHYQBOVJCLRZDNW CDUN 25 15 17 03
0005 E > XDYB(P)WOSMUZRIQGENLHVJTFACK CDUO 25 15 17 04
0006 N > DLIAJUOVCEXBN(M)GQPWZYFHRKTS CDUP 25 15 17 05
0007 D > LUS(H)QOXDMZNAIKFREPCYBWVGTJ CDUQ 25 15 17 06
0008 E > JKGO(P)TCIHABRNMDEYLZFXWVUQS CDUR 25 15 17 07
0009 S > GCBUZRASYXVMLPQNOF(H)WDKTJIE CDUS 25 15 17 08
0010 I > XPJUOWIY(G)CVRTQEBNLZMDKFAHS CDUT 25 15 17 09
0011 S > DISAUYOMBPNTHKGJRQ(C)LEZXWFV CDUU 25 15 17 10
0012 T > FJLVQAKXNBGCPIRMEOY(Z)WDUHST CDUV 25 15 17 11
0013 S > KTJUQONPZCAMLGFHEW(X)BDYRSVI CDUW 25 15 17 12
0014 O > ZQXUVGFNWRLKPH(T)MBJYODEICSA CDUX 25 15 17 13
0015 F > XJWFR(D)ZSQBLKTVPOIEHMYNCAUG CDUY 25 15 17 14
0016 O > FSKTJARXPECNUL(Y)IZGBDMWVHOQ CDUZ 25 15 17 15
0017 R > CEAKBMRYUVDNFLTXW(G)ZOIJQPHS CDVA 25 15 18 16
0018 T > TLJRVQHGUCXBZYSWFDO(A)IEPKNM CDVB 25 15 18 17
0019 B > Y(H)LPGTEBKWICSVUDRQMFONJZAX CDVC 25 15 18 18
0020 E > KRUL(G)JEWNFADVIPOYBXZCMHSQT CDVD 25 15 18 19
0021 K > RCBPQMVZXY(U)OFSLDEANWKGTIJH CDVE 25 15 18 20
0022 A > (F)CBJQAWTVDYNXLUSEZPHOIGMKR CDVF 25 15 18 21
0023 N > VFTQSBPORUZWY(X)HGDIECJALNMK CDVG 25 15 18 22
0024 N > JSRHFENDUAZYQ(G)XTMCBPIWVOLK CDVH 25 15 18 23
0025 T > RCBUTXVZJINQPKWMLAY(E)DGOFSH CDVI 25 15 18 24
0026 Z > URFXNCMYLVPIGESKTBOQAJZDH(W) CDVJ 25 15 18 25
0027 U > JIOZFEWMBAUSHPCNRQLV(K)TGYXD CDVK 25 15 18 26
0028 G > ZGVRKO(B)XLNEIWJFUSDQYPCMHTA CDVL 25 15 18 01
0029 E > RMJV(L)YQZKCIEBONUGAWXPDSTFH CDVM 25 15 18 02
0030 B > G(K)QRFEANZPBMLHVJCDUXSOYTWI CDWN 25 15 19 03
0031 E > YMZT(G)VEKQOHPBSJLIUNDRFXWAC CDWO 25 15 19 04
0032 N > PDSBTIUQFNOVW(J)KAHZCEGLMYXR CDWP 25 15 19 05
```

where the letters following each mapping are the letters that appear at the windows at that stage (the only state changes visible to the operator) and the numbers show the underlying physical position of each rotor.

The character mappings for a given configuration of the machine are in turn the result of a series of such mappings applied by each pass through a component of the machine: the enciphering of a character resulting from the application of a given component's mapping serves as the input to the mapping of the subsequent component. For example, the 4th step in the enciphering above can be expanded to show each of these stages using the same representation of mappings and highlighting for the enciphered character:

```
 G > ABCDEF(G)HIJKLMNOPQRSTUVWXYZ
   P EFMQAB(G)UINKXCJORDPZTHWVLYS         AE.BF.CM.DQ.HU.JN.LX.PR.SZ.VW
   1 OFRJVM(A)ZHQNBXPYKCULGSWETDI  N  03  VIII
   2 (N)UKCHVSMDGTZQFYEWPIALOXRJB  U  17  VI
   3 XJMIYVCARQOWH(L)NDSUFKGBEPZT  D  15  V
   4 QUNGALXEPKZ(Y)RDSOFTVCMBIHWJ  C  25  β
   R RDOBJNTKVEHMLFCWZAXGYIPS(U)Q         c
   4 EVTNHQDXWZJFUCPIAMOR(B)SYGLK         β
   3 H(V)GPWSUMDBTNCOKXJIQZRFLAEY         V
   2 TZDIPNJESYCUHAVRMXGKB(F)QWOL         VI
   1 GLQYW(B)TIZDPSFKANJCUXREVMOH         VIII
   P E(F)MQABGUINKXCJORDPZTHWVLYS         AE.BF.CM.DQ.HU.JN.LX.PR.SZ.VW
 F < KPTXIG(F)MESAUHYQBOVJCLRZDNW
```

Here the enciphering begins trivially with the first "mapping" representing the keyboard (which has no effect), followed by the plugboard, configured as AE.BF.CM.DQ.HU.JN.LX.PR.SZ.VW which has no effect on 'G', followed by the VIII rotor in the 03 position, which maps G to A, then the VI rotor in the 17 position, which maps A to N, ..., and finally the plugboard again, which maps B to F, producing the overall mapping indicated at the final step: G to F.

Note that this model has 4 rotors (lines 1 through 4) and that the reflector (line R) also permutes (garbles) letters.

Models

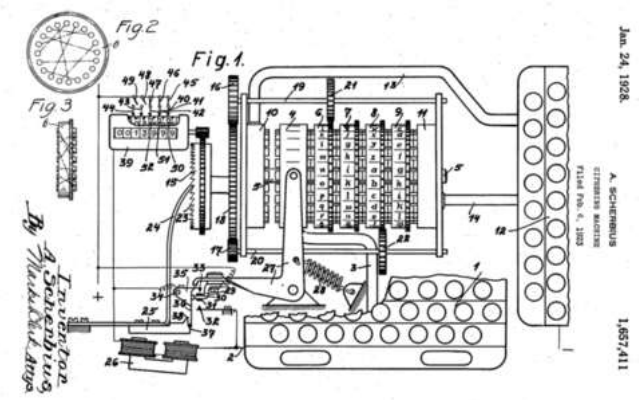
The Enigma family included multiple designs. The earliest were commercial models dating from the early 1920s. Starting in the mid-1920s, the German military began to use Enigma, making a number of security-related changes. Various nations either adopted or adapted the design for their own cipher machines.

A selection of seven Enigma machines and paraphernalia exhibited at the U.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.

An estimated 40,000 Enigma machines were constructed.[36][37] After the end of World War II, the Allies sold captured Enigma machines, still widely considered secure, to developing countries.[38]

Commercial Enigma

On 23 February 1918,[39] Arthur Scherbius applied for a patent for a ciphering machine that used rotors.[40] Scherbius and E. Richard Ritter founded the firm of Scherbius & Ritter. They approached the German Navy and Foreign Office with their design, but neither agency was interested. Scherbius & Ritter 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.



Scherbius Enigma patent, U.S. Patent 1,657,411 (https://patents.google.com/patent/US1657411), granted in 1928.

Enigma Handelsmaschine (1923)

Chiffriermaschinen AG began advertising a rotor machine, *Enigma Handelsmaschine*, which was exhibited at the Congress of the International Postal Union in 1924. The machine was heavy and bulky, incorporating a typewriter. It measured 65×45×38 cm and weighed about 50 kilograms (110 lb).

Schreibende Enigma (1924)

This was also a model with a type writer. There where a number of problems associated with the printer and the construction was not stable until 1926. Both early versions of Enigma lacked the reflector and had to be switched between chiffering and dechiffering.

Glühlampenmaschine, Enigma A (1924)

The reflector, suggested by Scherbius' colleague Willi Korn,[22] was introduced with the glow lamp version.

The machine was also known as the military Enigma. It had two rotors and a manually rotatable reflector. The typewriter was omitted and glow lamps were used for output. The operation was somewhat different from later models. Before the next key pressure, the operator had to press a button to advance the right rotor one step.

Enigma B (1924)

Enigma *model B* was introduced late in 1924, and was of a similar construction.[41] 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. This model of Enigma machine

was referred to as the Glowlamp Enigma or *Glühlampenmaschine* since it produced its output on a lamp panel rather than paper. This method of output was much more reliable and cost effective. Hence this machine was 1/8th the price of its predecessor.[17]

Typical glowlamps (with flat tops), as used for Enigma.

Enigma C (1926)

Model C was the third model of the so-called "glowlamp Enigmas" (after A and B) and it again lacked a typewriter.[17]

Enigma D (1927)

The *Enigma C* quickly gave way to *Enigma D* (1927). This version was widely used, with shipments to Sweden, the Netherlands, United Kingdom, Japan, Italy, Spain, United States and Poland. In 1927 Hugh Foss at the British Government Code and Cypher School was able to show that commercial Enigma machines could be broken, provided suitable cribs were available.[42] Soon, the Enigma D would pioneer the use of a standard keyboard layout to be used in German computing. This "QWERTZ" layout is very similar to the American QWERTY keyboard format used in many languages.

"Navy Cipher D"

Other countries used Enigma machines. The Italian Navy adopted the commercial Enigma as "Navy Cipher D". The Spanish also used commercial Enigma machines during their Civil War. British codebreakers succeeded in breaking these machines, which lacked a plugboard.[43] Enigma machines were also used by diplomatic services.

Enigma H (1929)

There was also a large, eight-rotor printing model, the *Enigma H*, called *Enigma II* by the *Reichswehr*. In 1933 the Polish Cipher Bureau detected that it was in use for high-level military communication, but it was soon withdrawn, as it was unreliable and jammed frequently.[44]


A rare 8-rotor printing Enigma model H (1929).

Enigma K

The Swiss used a version of Enigma called *Model K* or *Swiss K* for military and diplomatic use, which was very similar to commercial Enigma D. The machine's code was cracked by Poland, France, the United Kingdom and the United States; the latter code-named it INDIGO. An *Enigma T* model, code-named *Tirpitz*, was used by Japan.

Military Enigma

The various services of the Wehrmacht used various Enigma versions, and replaced them frequently, sometimes with ones adapted from other services. Enigma seldom carried high-level strategic messages, which when not urgent went by courier, and when urgent went

by other cryptographic systems including the Geheimschreiber.

Funkschlüssel C

The Reichsmarine was the first military branch 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.[45]

The keyboard and lampboard contained 29 letters — A-Z, Ä, Ö and Ü — that were arranged alphabetically, as opposed to the QWERTZUI ordering.[46] The rotors had 28 contacts, with the letter *X* wired to bypass the rotors unencrypted.[16] Three rotors were chosen from a set of five[47] and the reflector could be inserted in one of four different positions, denoted α, β, γ and δ.[48] The machine was revised slightly in July 1933.[49]

Enigma G (1928–1930)

By 15 July 1928,[50] the German Army (*Reichswehr*) had introduced their own exclusive version of the Enigma machine, the *Enigma G*.

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 that incremented upon each key press, and so is also known as the "counter machine" or the *Zählwerk* Enigma.

Wehrmacht Enigma I (1930–1938)

Enigma machine G was modified to the *Enigma I* by June 1930.[51] Enigma I is also known as the *Wehrmacht*, or "Services" Enigma, and was used extensively by German military services and other government organisations (such as the railways[52]) before and during World War II.

The major difference between *Enigma I* (German Army version from 1930), and commercial Enigma models was the addition of a plugboard to swap pairs of letters, greatly increasing cryptographic strength.

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. The machine measured 28 cm × 34 cm × 15 cm (11.0 in × 13.4 in × 5.9 in) and weighed around 12 kg (26 lb).[53]

In August 1935, the Air Force introduced the Wehrmacht Enigma for their communications.[51]

Heinz Guderian in the Battle of France, with an Enigma machine. Note one soldier is keying in text while another writes down the results.

M3 (1934)

By 1930, the Reichswehr had suggested that the Navy adopt their machine, citing the benefits of increased security (with the plugboard) and easier interservice communications.[54] The Reichsmarine eventually agreed and in 1934[55] brought into service the Navy version of the Army

Enigma, designated *Funkschlüssel* ' or *M3*. While the Army used only three rotors at that time, the Navy specified a choice of three from a possible five.[56]

Enigma in use on the Russian front

Two extra rotors (1938)

In December 1938, the Army issued two extra rotors so that the three rotors were chosen from a set of five.[51] 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.[56]

M4 (1942)

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.

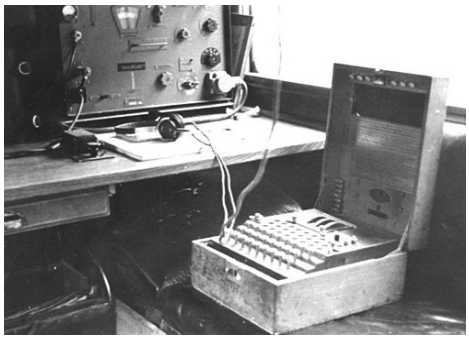
Enigma G, used by the *Abwehr*, had four rotors, no plugboard, and multiple notches on the rotors.

The German-made Enigma-K used by the Swiss Army had three rotors and a reflector, but no plugboard. It had locally re-wired rotors and an additional lamp panel.

An Enigma model T (Tirpitz), a modified commercial Enigma K manufactured for use by the Japanese.

An Enigma machine in the UK's Imperial War Museum

Enigma in use in Russia



Enigma in radio car of the 7th Panzer Div. staff, August 1941

Surviving machines

A three-rotor Enigma machine on display at Computer Museum of America and its two additional rotors.

The effort to break the Enigma was not disclosed until the 1970s. Since then, interest in the Enigma machine has grown. Enigmas are on public display in museums around the world, and several are in the hands of private collectors and computer history enthusiasts.[57]

The *Deutsches Museum* in Munich has both the three- and four-rotor German military variants, as well as several civilian versions. Enigma machines are exhibited at the National Codes Centre in Bletchley Park, the Government Communications Headquarters, the Science Museum in London, Discovery Park of America in Tennessee, the Polish Army Museum in Warsaw, the Swedish Army Museum (*Armémuseum*) in Stockholm, the Military Museum of A Coruña in Spain, the Nordland Red Cross War Memorial Museum in Narvik,[58] Norway, The Artillery, Engineers and Signals Museum in Hämeenlinna, Finland[59] the Technical University of Denmark in Lyngby,

Surviving three-rotor Enigma on display at Discovery Park of America in Union City, Tennessee, U.S.

Denmark, in Skanderborg Bunkerne at Skanderborg, Denmark, and at the Australian War Memorial and in the foyer of the Australian Signals Directorate, both in Canberra, Australia. The Jozef Pilsudski Institute in London exhibited a rare Polish Enigma double assembled in France in 1940.[60][61] In 2020, thanks to the support of the Ministry of Culture and National Heritage, it became the property of the Polish History Museum.[62]

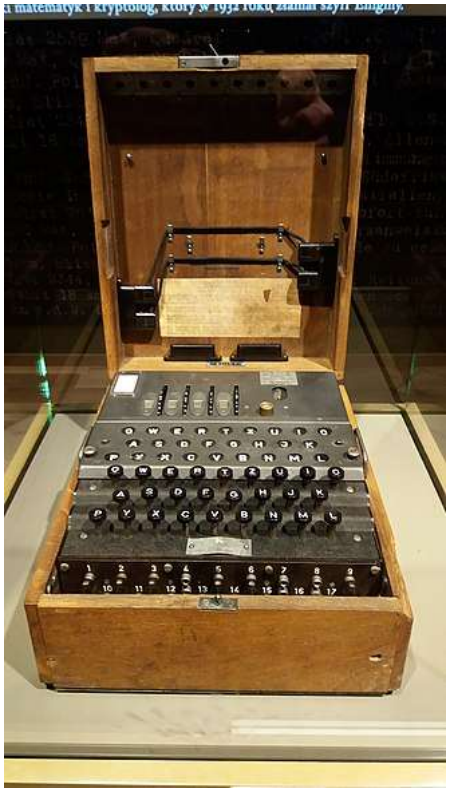
A four-rotor *Kriegsmarine* (German Navy, 1. February 1942 to 1945) Enigma machine on display at the U.S. National Cryptologic Museum

In the United States, Enigma machines can be seen at the Computer History Museum in Mountain View, California, and at the National Security Agency's National Cryptologic Museum in Fort Meade, Maryland, where visitors can try their hand at enciphering and deciphering messages. Two machines that were acquired after the capture of *U-505* during World War II are on display alongside the submarine at the Museum of Science and Industry in Chicago, Illinois. A three-rotor Enigma is on display at Discovery Park of America in Union City, Tennessee. A four-rotor device is on display in the ANZUS Corridor of the Pentagon on the second floor, A ring, between corridors 8 and 9. This machine is on loan from Australia. The United States Air Force Academy in Colorado Springs has a machine on display in the Computer Science Department. There is also a machine located at The National WWII Museum in New Orleans. The International Museum of World War II near Boston has seven Enigma machines on display, including a U-Boat four-rotor model, one of three surviving examples of an Enigma machine with a printer, one of fewer than ten surviving ten-rotor code machines, an example blown up by a retreating German Army unit, and two three-rotor Enigmas that visitors can operate to encode and decode messages. Computer Museum of America in Roswell, Georgia has a three-rotor model with two additional rotors. The machine is fully restored and CMoA has the original paperwork for the purchase on 7 March 1936 by the German Army. The National Museum of Computing also contains surviving Enigma machines in Bletchley, England.[63]

In Canada, a Swiss Army issue Enigma-K, is in Calgary, Alberta. It is on permanent display at the Naval Museum of Alberta inside the Military Museums of Calgary. A four-rotor Enigma machine is on display at the Military Communications and Electronics Museum at Canadian Forces Base (CFB) Kingston in Kingston, Ontario.

Occasionally, Enigma machines are sold at auction; prices have in recent years ranged from US$40,000[64][65] to US$547,500[66] in 2017. Replicas are available in various forms, including an exact reconstructed copy of the Naval M4 model, an Enigma implemented in electronics (Enigma-E), various 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 threatening 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 stated deadline passed with no word from the blackmailer. Shortly afterward, the machine was sent anonymously to BBC journalist Jeremy Paxman, missing three rotors.



A four-rotor *Kriegsmarine* Enigma machine on display at the Museum of the Second World War, Gdańsk, Poland

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 and served three months.[67]

In October 2008, the Spanish daily newspaper *El País* reported that 28 Enigma machines had been discovered by chance in an attic of Army headquarters in Madrid. These four-rotor commercial machines had helped Franco's Nationalists win the Spanish Civil War, because, though the British cryptologist Alfred Dilwyn Knox in 1937 broke the cipher generated by Franco's Enigma machines, this was not disclosed to the Republicans, who failed to break the cipher. The Nationalist government continued using its 50 Enigmas into the 1950s. Some machines have gone on display in Spanish military museums,[68][69] including one at the National Museum of Science and Technology (MUNCYT) in La Coruña and one at the Spanish Army Museum. Two have been given to Britain's GCHQ.[70]

The Bulgarian military used Enigma machines with a Cyrillic keyboard; one is on display in the National Museum of Military History in Sofia.[71]

On 3 December 2020, German divers working on behalf of the World Wide Fund for Nature discovered a destroyed Enigma machine in Flensburg Firth (part of the Baltic Sea) which is believed to be from a scuttled U-Boat.[72] This Enigma machine will be restored by and be the property of the Archaeology Museum of Schleswig Holstein.[73]

An M4 Enigma was salvaged in the 1980s from the German minesweeper R15, which was sunk off the Istrian coast in 1945. The machine was put on display in the Pivka Park of Military History in Slovenia on 13 April 2023.[74]

Derivatives

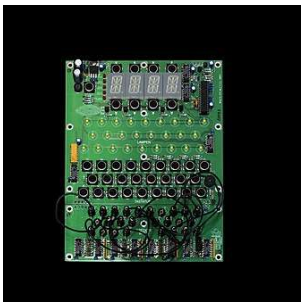
The Enigma was influential in the field of cipher machine design, spinning off other rotor machines. Once the British discovered Enigma's principle of operation, they created the Typex rotor cipher, which the Germans believed to be unsolvable.[75] Typex was originally derived from the Enigma patents;[76] Typex even includes features from the patent descriptions that were omitted from the actual Enigma machine. The British paid no royalties for the use of the patents.[76] In the United States, cryptologist William Friedman designed the M-325 machine,[77] starting in 1936,[78] that is logically similar.[79]

Machines like the SIGABA, NEMA, Typex, and so forth, are not considered to be Enigma derivatives as their internal ciphering functions are not mathematically identical to the Enigma transform.

A unique rotor machine called Cryptograph was constructed in 2002 by Netherlands-based Tatjana van Vark. This device makes use of 40-point rotors, allowing letters, numbers and some punctuation to be used; each rotor contains 509 parts.[80]

A Japanese Enigma clone, codenamed GREEN by American cryptographers.

Tatjana van Vark's Enigma-inspired rotor machine.



Electronic implementation of an Enigma machine, sold at the Bletchley Park souvenir shop

Simulators

See also

- Alastair Denniston
- Arlington Hall
- Arne Beurling
- Beaumanor Hall, a stately home used during the Second World War for military intelligence
- Cryptanalysis of the Enigma
- Erhard Maertens—investigated Enigma security
- Erich Fellgiebel
- Fritz Thiele
- Gisbert Hasenjaeger—responsible for Enigma security
- United States Naval Computing Machine Laboratory

Explanatory notes

a. Much of the German cipher traffic was encrypted on the Enigma machine, and the term "Ultra" has often been used almost synonymously with "Enigma decrypts". Ultra also encompassed decrypts of the German Lorenz SZ 40 and 42 machines that were used by the German High Command, and decrypts of Hagelin ciphers and other Italian ciphers and codes, as well as of Japanese ciphers and codes such as Purple and JN-25.

References

Citations

1. "EnigmaHistory" (https://www.cryptomuseum.com/crypto/enigma/hist.htm). *cryptomuseum.com*. Retrieved 16 December 2020.

2. Comer 2021.
3. Keegan, John, Sir (2003). *Intelligence in War*. New York: Alfred A. Knopf.
4. Singh, Simon (26 January 2011). *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* (https://books.google.com/books?id=fbp9V9dkaNkC). Knopf Doubleday Publishing Group. ISBN 978-0-307-78784-2.
5. "History of the Enigma" (http://www.cryptomuseum.com/crypto/enigma/hist.htm). Crypto Museum. Retrieved 1 December 2017.
6. Lord, Bob (1998–2010). "Enigma Manual" (http://www.ilord.com/enigma-manuals). Retrieved 31 May 2011.
7. "Four Rotor Enigma Machine" (https://www.spymuseum.org/exhibition-experiences/about-the-collection/collection-highlights/four-rotor-enigma-machine/). *International Spy Museum*. Retrieved 21 February 2023.
8. Rejewski 1980.
9. Vázquez & Jiménez–Seral 2018.
10. Kozaczuk 1984, p. 63.
11. Erskine 2006, pp. 294–305.
12. Kozaczuk 1984, pp. 59–60, 236.
13. Kozaczuk 1984, pp. 69–94.
14. Welchman 1982, p. 289.
15. Kahn 1991.
16. Stripp 1993.
17. "Enigma History" (https://www.cryptomuseum.com/crypto/enigma/hist.htm). *cryptomuseum.com*. Retrieved 16 December 2020.
18. Rijmenants, Dirk; Technical details of the Enigma machine (https://www.ciphermachinesandcryptology.com/en/enigmatech.htm) Cipher Machines & Cryptology
19. Hamer, David (January 1997). "Enigma: Actions Involved in the 'Double-Stepping' of the Middle Rotor" (https://web.archive.org/web/20110719081659/http://www.eclipse.net/~dhamer/downloads/rotorpdf.zip). *Cryptologia*. **21** (1): 47–50. doi:10.1080/0161-119791885779 (https://doi.org/10.1080%2F0161-119791885779). Archived from the original (http://www.eclipse.net/~dhamer/downloads/rotorpdf.zip) (zip) on 19 July 2011.
20. Sale, Tony. "Technical specifications of the Enigma rotors" (http://www.codesandciphers.org.uk/enigma/rotorspec.htm). *Technical Specification of the Enigma*. Retrieved 15 November 2009.
21. "Lückenfüllerwalze" (http://www.cryptomuseum.com/crypto/enigma/lf/index.htm). Cryptomuseum.com. Retrieved 17 July 2012.
22. De Leeuw, Karl Maria Michael; Bergstra, J A (2007). *The history of information security : a comprehensive handbook*. Amsterdam: Elsevier. p. 393. ISBN 9780080550589.
23. Marks & Weierud 2000.
24. Marks 2001, pp. 101–141.
25. Craig P. Bauer: *Secret History – The Story of Cryptology*. CRC Press, Boca Raton 2013, p. 248. ISBN 978-1-4665-6186-1.
26. Van Manen, Dirk-Jan; Johan O. A., Robertsson (2016). "Codes and Ciphers" (https://www.geoexpro.com/articles/2016/10/codes-and-ciphers-part-i). *Geo ExPro*. Retrieved 3 January 2022.
27. Reuvers, Paul (2008). "Enigma accessories" (http://www.jproc.ca/crypto/enigma_acc.html). Retrieved 22 July 2010.

28. Miller, A. Ray (January 1995). "The cryptographic mathematics of Enigma" (https://www.tandfonline.com/doi/abs/10.1080/0161-119591883773). *Cryptologia*. **19** (1): 65–80. doi:10.1080/0161-119591883773 (https://doi.org/10.1080%2F0161-119591883773).
29. Friedman, W.F. (1922). *The index of coincidence and its applications in cryptology*. Department of Ciphers. Publ 22. Geneva, Illinois, USA: Riverbank Laboratories. OCLC 55786052 (https://www.worldcat.org/oclc/55786052).
30. Huttenhain & Fricke 1945, pp. 4, 5.
31. Rijmenants, Dirk; Enigma message procedures (https://www.ciphermachinesandcryptology.com/en/enigmaproc.htm) Cipher Machines & Cryptology
32. Rijmenants, Dirk; Kurzsignalen on German U-boats (https://www.ciphermachinesandcryptology.com/en/kurzsignale.htm) Cipher Machines & Cryptology
33. "The translated 1940 *Enigma General Procedure*" (http://www.codesandciphers.org.uk/documents/egenproc/eniggnix.htm). codesandciphers.org.uk. Retrieved 16 October 2006.
34. "The translated 1940 *Enigma Officer and Staff Procedure*" (http://www.codesandciphers.org.uk/documents/officer/officerx.htm). codesandciphers.org.uk. Retrieved 16 October 2006.
35. "Message from Dönitz — 1 May 1945" (https://www.cryptomuseum.com/crypto/enigma/msg/p1030681.htm). Retrieved 27 November 2018.
36. Bauer 2000, p. 123.
37. *Reichswehr and Wehrmacht Enigma Orders* (https://cryptocellar.org/enigma/e-history/enigma-reichswehr-wehrmacht-orders.pdf) in Frode Weierud's CryptoCellar, accessed 29 June 2021.
38. Bauer 2000, p. 112.
39. "German patent No. 416219 from 23 February 1918" (https://www.cdvandt.org/Enigma%20DE416219C1.pdf) (PDF).
40. US 1657411 (https://worldwide.espacenet.com/textdoc?DB=EPODOC&IDX=US1657411), Scherbius, Arthur, "Ciphering Machine", issued 24 January 1928, assigned to Chiffriermaschinen AG
41. "image of Enigma Type B" (https://web.archive.org/web/20051021083422/http://www.armyradio.com/publish/Articles/The_Enigma_Code_Breach/Pictures/enigma_type_b.jpg). Archived from the original (http://www.armyradio.com/publish/Articles/The_Enigma_Code_Breach/Pictures/enigma_type_b.jpg) on 21 October 2005.
42. Bletchley Park Trust Museum display
43. Smith 2006, p. 23.
44. Kozaczuk 1984, p. 28.
45. Kahn 1991, pp. 39–41, 299.
46. Ulbricht 2005, p. 4.
47. Kahn 1991, pp. 40, 299.
48. Bauer 2000, p. 108.
49. Stripp 1993, plate 3.
50. Kahn 1991, pp. 41, 299.
51. Kruh & Deavours 2002, p. 97.
52. Smith 2000, p. 73.
53. Stripp 1993, p. 83.
54. Kahn 1991, p. 43.
55. Kahn 1991, p. 43 says August 1934. Kruh & Deavours 2002, p. 15 say October 2004.
56. Kruh & Deavours 2002, p. 98.

57. Ng, David. "Enigma machine from World War II finds unlikely home in Beverly Hills" (http://www.latimes.com/entertainment/arts/culture/la-et-cm-imitation-game-enigma-machine-david-bohnett-20150122-story.html). *Los Angeles Times*. 22 January 2015.
58. "War Museum" (http://www.warmuseum.no/no/English/).
59. "The National Signals Museum" (http://www.viestikiltojenliitto.fi/viestimuseo/_eng/index.html).
60. "Enigma exhibition in London pays tribute to Poles" (https://web.archive.org/web/20160423092753/http://thenews.pl/1/10/Artykul/244703,Enigma-exhibition-in-London-pays-tribute-to-Poles). *Polskie Radio dla Zagranicy*. Archived from the original (http://www.thenews.pl/1/10/Artykul/244703,Enigma-exhibition-in-London-pays-tribute-to-Poles) on 23 April 2016. Retrieved 5 April 2016.
61. "13 March 2016, 'Enigma Relay'– how Poles passed the baton to Brits in the run for WWII victory" (https://web.archive.org/web/20160422230532/http://pilsudski.org.uk/en/aktualnosci.php?news=205&wid=13&wai=&year=&back=%252Fen%252F). *J. Piłsudski Institute in London*. Archived from the original (http://pilsudski.org.uk/en/aktualnosci.php?news=205&wid=13&wai=&year=&back=%252Fen%252F) on 22 April 2016. Retrieved 5 April 2016.
62. "Enigma w kolekcji MHP - Muzeum Historii Polski" (http://muzhp.pl/pl/c/1887/enigma-w-kolekcji-mhp).
63. "The National Museum of Computing" (https://www.tnmoc.org/). *The National Museum of Computing*. Retrieved 16 December 2020.
64. Hamer, David; *Enigma machines – known locations* (http://www.eclipse.net/~dhamer/location.htm)* Archived (https://web.archive.org/web/20111104151545/http://www.eclipse.net/~dhamer/location.htm) 4 November 2011 at the Wayback Machine
65. Hamer, David; *Selling prices of Enigma and NEMA – all prices converted to US$ (http://www.eclipse.net/~dhamer/enigma_p.htm)* Archived (https://web.archive.org/web/20110927033657/http://www.eclipse.net/~dhamer/enigma_p.htm) 27 September 2011 at the Wayback Machine
66. Christi's; *4 Rotor enigma auction (https://web.archive.org/web/20170617050627/http://artdaily.com/news/96771/Christie-s-sets-world-auction-record-for-an-Enigma-Machine-sold-to-online-bidder#.WZ80cZN94RF)*
67. "Man jailed over Enigma machine" (http://news.bbc.co.uk/1/hi/uk/1609168.stm). *BBC News*. 19 October 2001. Retrieved 2 May 2010.
68. Graham Keeley. *Nazi Enigma machines helped General Franco in Spanish Civil War (http://www.timesonline.co.uk/tol/news/world/europe/article5003411.ece)*, The Times, 24 October 2008, p. 47.
69. "Taller de Criptografía – Enigmas españolas" (https://web.archive.org/web/20130611204718/http://www.cripto.es/museo/enigma-esp-fotos.htm). Cripto.es. Archived from the original (http://www.cripto.es/museo/enigma-esp-fotos.htm) on 11 June 2013. Retrieved 8 September 2013.
70. "Schneier on Security: Rare Spanish Enigma Machine" (http://www.schneier.com/blog/archives/2012/03/rare_spanish_en.html). Schneier.com. 26 March 2012. Retrieved 8 September 2013.
71. "Communication equipment" (https://web.archive.org/web/20150113062919/http://www.znam.bg/com/action/showAppArticle?appID=3&encID=2&article=3514226659&sectionID=1). znam.bg. 29 November 2003. Archived from the original (http://www.znam.bg/com/action/showAppArticle?appID=3&encID=2&article=3514226659&sectionID=1) on 13 January 2015. Retrieved 13 January 2015.
72. "Divers discover Nazi WW2 enigma machine in Baltic Sea" (https://www.reuters.com/article/us-germany-war-enigma-idUSKBN28D25F). *Reuters*. 3 December 2020. Archived (https://web.archive.org/web/20201203171005/https://www.reuters.com/article/us-germany-war-enigma-idUSKBN28D25F) from the original on 3 December 2020. Retrieved 3 December 2020.
73. Welle (www.dw.com), Deutsche. "German divers hand over Enigma encryption machine in Baltic | DW | 04.12.2020" (https://www.dw.com/en/german-divers-hand-over-enigma-encryption-machine-in-baltic/a-55829171). *DW.COM*.

74. "Revealing of Enigma in the Park of Military History Pivka" (https://www.parkvojaskezgodovine.si/en/23851/). 13 April 2023.
75. Ferris, John Robert (2005). *Intelligence and strategy : selected essays*. Cass series - Studies in intelligence. New York, NY: F. Cass. p. 165. ISBN 978-0415361958. OCLC 243558411 (https://www.worldcat.org/oclc/243558411).
76. Greenberg, Joel (2014). *Gordon Welchman: Bletchley Park's architect of ultra intelligence*. London: Pen & Sword Books Ltd. p. 85. ISBN 9781473885257. OCLC 1023312315 (https://www.worldcat.org/oclc/1023312315).
77. Karl Maria Michael de Leeuw; Jan Bergstra (28 August 2007). *The History of Information Security: A Comprehensive Handbook* (https://books.google.com/books?id=pQBrsonDp6cC&pg=PA407). Elsevier Science. pp. 407–. ISBN 978-0-08-055058-9.
78. Mucklow, Timothy (2015). *The SIGABA / ECM II Cipher Machine: "A Beautiful Idea* (https://www.nsa.gov/Portals/70/documents/about/cryptologic-heritage/historical-figures-publications/publications/technology/The_SIGABA_ECM_Cipher_Machine_A_Beautiful_Idea3.pdf) (PDF). Fort George G. Meade, MD: Center for Cryptologic History, NSA. p. 16.
79. Bauer, Friedrich Ludwig (2007). *Decrypted secrets: methods and maxims of cryptology* (4th revision and extended ed.). Berlin: Springer. p. 133. ISBN 9783540245025. OCLC 255507974 (https://www.worldcat.org/oclc/255507974).
80. van Vark, Tatjana *The coding machine (http://www.tatjavanvark.nl/tvv1/pht10.html)*

General and cited references

- Bauer, F. L. (2000). *Decrypted Secrets* (https://books.google.com/books?id=E-epCAAAQBAJ) (2nd ed.). Springer. ISBN 978-3-540-66871-8.
- Comer, Tony (27 January 2021). "Poland's Decisive Role in Cracking Enigma and Transforming the UK's SIGINT Operations" (https://rusi.org/commentary/poland-decisive-role-cracking-enigma-and-transforming-uk-sigint-operations). Commentary. RUSI. Retrieved 20 April 2022.
- Erskine, Ralph (December 2006). "The Poles Reveal their Secrets: Alastair Denniston's Account of the July 1939 Meeting at Pyry". *Cryptologia*. Philadelphia, Pennsylvania. **30** (4): 294–305. doi:10.1080/01611190600920944 (https://doi.org/10.1080%2F01611190600920944).
- Hamer, David H.; Sullivan, Geoff; Weierud, Frode (July 1998). "Enigma Variations: An Extended Family of Machines" (http://www.math.utoledo.edu/~codenth/Cryptanalysis/crypt_machs/ESIM/enigvar2.PDF) (PDF). *Cryptologia*. **XXII** (3): 211–229. doi:10.1080/0161-119891886885 (https://doi.org/10.1080%2F0161-119891886885). ISSN 0161-1194 (https://www.worldcat.org/issn/0161-1194). Retrieved 18 February 2016.
- Huttenhain, Orr; Fricke (1945). "OKW/Chi Cryptanalytic Research on Enigma, Hagelin and Cipher Teleprinter Messages" (https://drive.google.com/file/d/0B7sNVKDp-yiJOWYxZWFmNDgtODUyMS00Y2FiLThkNWItYmQ5N2JmMzEyMzIz/view). TICOM.
- Kahn, David (1991). *Seizing the Enigma: The Race to Break the German U-Boats Codes, 1939–1943* (https://books.google.com/books?id=j1MC2d2LPAcC). ISBN 978-0-395-42739-2.
- Kozaczuk, Władysław (1984). Kasparek, Christopher (ed.). *Enigma: How the German Machine Cipher Was Broken, and How It Was Read by the Allies in World War Two* (https://books.google.com/books?id=5hJnAAAAMAAJ). Frederick, MD: University Publications of America. ISBN 978-0-89093-547-7.
- Kozaczuk, Władysław. "The origins of the Enigma/ULTRA" (https://web.archive.org/web/20030717071218/http://www.enigmahistory.org/text.html). Archived from the original (http://www.enigmahistory.org/text.html) on 17 July 2003.

- Kruh, L.; Deavours, C. (2002). "The Commercial Enigma: Beginnings of Machine Cryptography". *Cryptologia*. **26**: 1–16. doi:10.1080/0161-110291890731 (https://doi.org/10.1080%2F0161-110291890731). S2CID 41446859 (https://api.semanticscholar.org/CorpusID:41446859).
- Marks, Philip (April 2001). "UMKEHRWALZE D: ENIGMA'S REWIRABLE REFLECTOR - PART I". *Cryptologia*. **25** (2): 101–141. doi:10.1080/0161-110191889842 (https://doi.org/10.1080%2F0161-110191889842). ISSN 0161-1194 (https://www.worldcat.org/issn/0161-1194).
- Marks, Philip; Weierud, Frode (2000). "Recovering the Wiring of Enigma's Umkehrwalze A" (https://web.archive.org/web/20120213152736/http://cryptocellar.web.cern.ch/cryptocellar/pubs/ukwa.pdf) (PDF). *Cryptologia*. **24** (1): 55–66. CiteSeerX 10.1.1.622.1584 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.622.1584). doi:10.1080/0161-110091888781 (https://doi.org/10.1080%2F0161-110091888781). S2CID 4473786 (https://api.semanticscholar.org/CorpusID:4473786). Archived from the original (http://cryptocellar.web.cern.ch/cryptocellar/pubs/ukwa.pdf) (PDF) on 13 February 2012.
- Rejewski, Marian (1980). "An Application of the Theory of Permutations in Breaking the Enigma Cipher" (https://cryptocellar.org/enigma/files/rew80.pdf) (PDF). *Applicationes Mathematicae*. **16** (4): 543–559. doi:10.4064/am-16-4-543-559 (https://doi.org/10.4064%2Fam-16-4-543-559). ISSN 1730-6280 (https://www.worldcat.org/issn/1730-6280).
- Smith, Michael (2000). *Station X: The Codebreakers of Bletchley Park* (https://books.google.com/books?id=Wv4mSVDtA-wC). Pan. ISBN 978-0-7522-7148-4.
- Smith, Michael (2006). "How it began: Bletchley Park Goes to War". In Copeland, B Jack (ed.). *Colossus: The Secrets of Bletchley Park's Codebreaking Computers* (https://books.google.com/books?id=e6ocfloTkJ4C). Oxford: Oxford University Press. ISBN 978-0-19-284055-4.
- Stripp, Alan (1993). Hinsley, F. H.; Stripp, Alan (eds.). *The Enigma Machine: Its Mechanism and Use* (https://books.google.com/books?id=j1MC2d2LPAcC). *Codebreakers: The Inside Story of Bletchley Park*.
- Ulbricht, Heinz (2005). *Die Chiffriermaschine Enigma — Trügerische Sicherheit: Ein Beitrag zur Geschichte der Nachrichtendienste* (http://opus.tu-bs.de/opus/volltexte/2005/705/pdf/enigmadiss.pdf) [*The Enigma Cipher Machine — Deceptive Security: A contribution to the history of intelligence services*] (PDF) (Thesis). PhD Thesis (in German). Universitätsbibliothek Braunschweig. doi:10.24355/dbbs.084-200511080100-324 (https://doi.org/10.24355%2Fdbbs.084-200511080100-324).
- Vázquez, Manuel; Jiménez–Seral, Paz (4 March 2018). "Recovering the military Enigma using permutations—filling in the details of Rejewski's solution". *Cryptologia*. **42** (2): 106–134. doi:10.1080/01611194.2016.1257522 (https://doi.org/10.1080%2F01611194.2016.1257522). S2CID 4451333 (https://api.semanticscholar.org/CorpusID:4451333).
- Welchman, Gordon (1982). *The Hut Six Story: Breaking the Enigma Codes*. McGraw-Hill. ISBN 978-0-07-069180-3.

Further reading

- Aldrich, Richard James (2010). *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency* (https://books.google.com/books?id=4I2PmCtrHOgC). HarperPress. ISBN 978-0-00-727847-3.
- Bertrand, Gustave (1973). *Enigma: ou, La plus grande énigme de la guerre 1939–1945* (https://books.google.com/books?id=o2UNAAAAIAAJ). Plon.
- Calvocoressi, Peter (2001). *Top Secret Ultra* (https://books.google.com/books?id=qxiHPwAACAAJ&pg=PA98). M & M Baldwin. pp. 98–103. ISBN 978-0-947712-41-9.

- Grime, James. "The Enigma Flaw" (https://web.archive.org/web/20130330065120/http://www.numberphile.com/videos/enigma_flaw.html). *Numberphile*. Brady Haran. Archived from the original (http://www.numberphile.com/videos/enigma_flaw.html) on 30 March 2013. Retrieved 7 April 2013.
- Heath, Nick, Hacking the Nazis: The secret story of the women who broke Hitler's codes (https://www.techrepublic.com/article/the-women-who-helped-crack-nazi-codes-at-bletchley-park) TechRepublic, 27 March 2015
- Herivel, John (2008). *Herivelismus: And the German Military Enigma* (https://books.google.com/books?id=voM0QwAACAAJ). M & M Baldwin.
- Keen, John (1 August 2012). *Harold 'Doc' Keen and the Bletchley Park Bombe* (https://books.google.com/books?id=tfq7MQEACAAJ). M & M Baldwin. ISBN 978-0-947712-48-8.
- Large, Christine (6 October 2003). *Hijacking Enigma: The Insider's Tale* (https://books.google.com/books?id=jAkiAQAAIAAJ). Wiley. ISBN 978-0-470-86346-6.
- Marks, Philip. "Umkehrwalze D: Enigma's Rewirable Reflector — Part I", *Cryptologia* 25(2), April 2001, pp. 101–141.
- Marks, Philip. "Umkehrwalze D: Enigma's Rewirable Reflector — Part II", *Cryptologia* 25(3), July 2001, pp. 177–212.
- Marks, Philip. "Umkehrwalze D: Enigma's Rewirable Reflector — Part III", *Cryptologia* 25(4), October 2001, pp. 296–310.
- Paillole, Paul (1985). *Notre espion chez Hitler* [*Our Spy with Hitler*] (in French). Robert Laffont.
- Perera, Tom (2010). *Inside ENIGMA*. Bedford, UK: Radio Society of Great Britain. ISBN 978-1-905086-64-1.
- Perera, Tom. *The Story of the ENIGMA: History, Technology and Deciphering*, 2nd Edition, CD-ROM, 2004, Artifax Books, ISBN 1-890024-06-6 sample pages (http://w1tp.com/enigma/ecds.htm)
- Rebecca Ratcliffe: Searching for Security. The German Investigations into Enigma's security. In: Intelligence and National Security 14 (1999) Issue 1 (Special Issue) S. 146–167.
- Ratcliffe, Rebecca (1 January 2005). Winkel, Brian J. (ed.). *How Statistics led the Germans to believe Enigma Secure and Why They Were Wrong: neglecting the practical Mathematics of Cipher machines* (https://books.google.com/books?id=1eVOAAAAMAAJ). *The German Enigma Cipher Machine: Beginnings, Success, and Ultimate Failure*. Artech House. ISBN 978-1-58053-996-8.
- Rejewski, Marian. "How Polish Mathematicians Deciphered the Enigma" (http://chc60.fgcu.edu/images/articles/rejewski.pdf), *Annals of the History of Computing 3*, 1981. This article is regarded by Andrew Hodges, Alan Turing's biographer, as "the definitive account" (see Hodges' *Alan Turing: The Enigma*, Walker and Company, 2000 paperback edition, p. 548, footnote 4.5).
- Quirantes, Arturo (April 2004). "Model Z: A Numbers-Only Enigma Version". *Cryptologia*. **28** (2): 153–156. doi:10.1080/0161-110491892845 (https://doi.org/10.1080%2F0161-110491892845). S2CID 44319455 (https://api.semanticscholar.org/CorpusID:44319455).
- Sebag-Montefiore, Hugh (2011). *Enigma: The Battle for the Code*. Orion. ISBN 978-1-78022-123-6.
- Ulbricht, Heinz. Enigma Uhr, *Cryptologia*, 23(3), April 1999, pp. 194–205.
- Turing, Dermot (2018). *X, Y & Z: The Real Story of How Enigma Was Broken*. Gloustershire England: History Press. ISBN 978-0-7509-8782-0. OCLC 1029570490 (https://www.worldcat.org/oclc/1029570490).
- Winterbotham, F. W. (1999). *The Ultra Secret*. Weidenfeld & Nicolson. ISBN 978-0-297-64405-7.
- Untold Story of Enigma Code-Breaker — The Ministry of Defence (U.K.) (https://web.archive.org/web/20051118083351/http://news.mod.uk/news/press/news_headline_story.asp?newsItem_id=3339)

External links

- Gordon Corera, Poland's overlooked Enigma codebreakers, BBC News Magazine, 4 July 2014 (https://www.bbc.com/news/magazine-28167071)
- Long-running list of places with Enigma machines on display (http://enigmadisplays.blogspot.ca/)
- Bletchley Park National Code Centre Home of the British codebreakers during the Second World War (http://www.bletchleypark.org.uk/) Archived (https://web.archive.org/web/20091209184137/http://www.bletchleypark.org.uk/) 9 December 2009 at the Wayback Machine
- Enigma machines on the Crypto Museum Web site (http://www.cryptomuseum.com/crypto/enigma/)
- Pictures of a four-rotor naval enigma, including Flash (SWF) views of the machine (http://cnm.open.ac.uk/projects/stationx/enigma/index.html) Archived (https://web.archive.org/web/20110724015209/http://cnm.open.ac.uk/projects/stationx/enigma/index.html) 24 July 2011 at the Wayback Machine
- Enigma Pictures and Demonstration by NSA Employee at RSA (http://www.cgisecurity.net/2008/04/getting-to-see-an-enigma-machine-at-rsa-2008-.html)
- Enigma machine (https://curlie.org/Science/Math/Applications/Communication_Theory/Cryptography/Historical/) at Curlie
- Kenngruppenheft (https://web.archive.org/web/20130426233328/http://www.wwiiarchives.net/servlet/action/document/index/97/0)
- Process of building an Enigma M4 replica (http://www.enigma-maschine.de/en/)
- Breaking German Navy Ciphers (http://www.enigma.hoerenberg.com/)