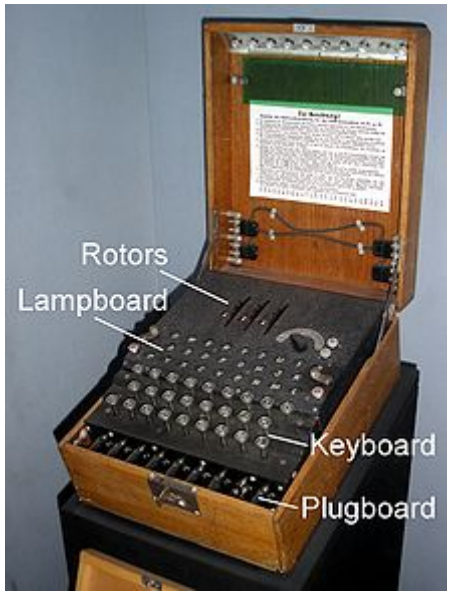
Enigma machine

The **Enigma machines** were a series of electro-mechanical rotor cipher machines developed and used in the early- to mid-20th century to protect commercial, diplomatic and military communication. Enigma was invented by the German engineer Arthur Scherbius at the end of World War I.[1] 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.[2] 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.

Military Enigma machine, model "Enigma I", used during the late 1930s and during the war; displayed at Museo scienza e tecnologia Milano, Italy

Around December 1932, Marian Rejewski, a Polish mathematician and cryptanalyst, while working at the Polish Cipher Bureau, used the theory of permutations and flaws in the German military message encipherment procedures to break the message keys of the plugboard Enigma machine. Rejewski achieved this result without knowledge of the wiring of the machine, so the result did not allow the Poles to decrypt actual messages. The French 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, which were called Enigma doubles. Rejewski was aided by cryptanalysts Jerzy Różycki and Henryk Zygalski, both of whom had been recruited with Rejewski from Poznań University. 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 the German Enigma messages. Over time, the German cryptographic procedures improved, and the Cipher Bureau developed techniques and designed mechanical devices to continue reading the Enigma traffic. As part of that effort, the Poles exploited quirks of the rotors, compiled catalogues, built a cyclometer to help make a catalogue with 100,000 entries, made Zygalski sheets and built the electro-mechanical cryptologic bomb to search for rotor settings. In 1938, the Germans added complexity to the Enigma machines that finally became too expensive for the Poles to counter. The Poles had six *bomby*, but when the Germans added two more rotors, ten times as many *bomby* were needed, but the Poles did not have the resources.[3]



Military Enigma machine (in wooden box)

On 26 and 27 July 1939,[4] in Pyry near Warsaw, the Poles initiated French and British military intelligence representatives into their Enigma-decryption techniques and equipment, including Zygalski sheets and the cryptologic bomb, and promised each delegation a Polish-reconstructed Enigma. The demonstration represented a vital basis for the later British continuation and effort.[5] 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.[6]

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 and "turned the tide" in the Allies' favour.[7][8]

Contents

Name

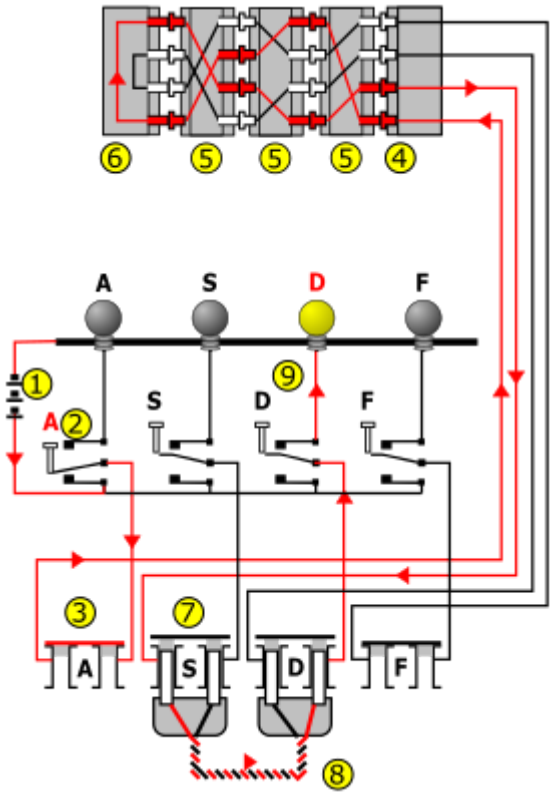
The German firm Scherbius & Ritter, co-founded by Arthur Scherbius, patented ideas for a cipher machine in 1918 and began marketing the finished product under the brand name *Enigma* in 1923, initially targeted at commercial markets.[9] With its adoption (in slightly modified form) by the German Navy in 1926 and the German Army and Air Force soon after, the name *Enigma* became widely known in military circles.

The word *enigma* is a Latin word, derived from the Ancient Greek word enigma (αίνιγμα) used in English, but not native German.

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

Electrical pathway

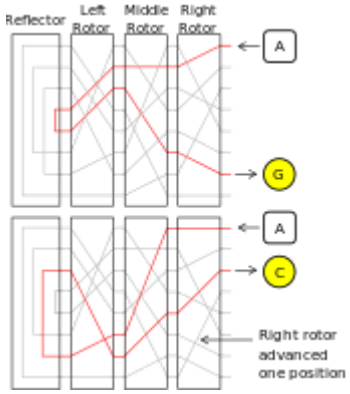


Enigma wiring diagram with arrows and the numbers 1 to 9 showing how current flows from key depression to a lamp being lit. The *A* key is encoded to the *D* lamp. D yields A, but A never yields A; this property was due to a patented feature unique to the Enigmas, and could be exploited by cryptanalysts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

Enigma in use, 1943

The mechanical parts act in such a way as to form 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.

Current flowed from the battery (1) through a depressed bi-directional keyboard switch (2) to the plugboard (3). Next, it passed 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 entered the reflector (6). The reflector returned 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.[10]



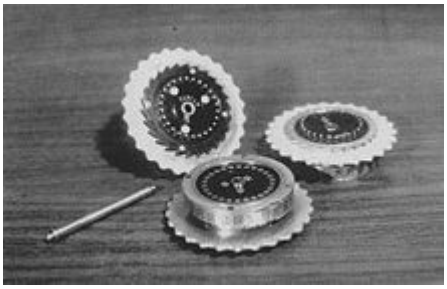
The scrambling action of Enigma's rotors is shown for two consecutive letters with the right-hand rotor moving one position between them.

The repeated changes of electrical path through an Enigma scrambler implemented a polyalphabetic substitution cipher that provided Enigma's security. The diagram on the right shows how the electrical pathway changed with each key depression, which caused rotation of at least the right-hand rotor. Current passed 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 has stepped, sending the signal on a completely different route. Eventually other rotors step with a key press.

Rotors

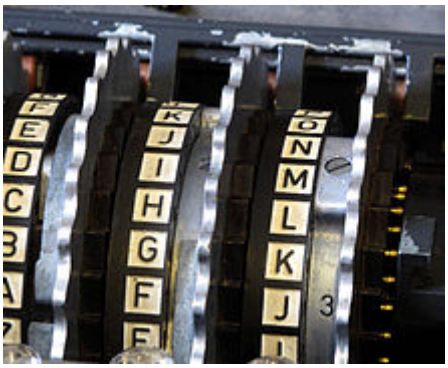
The rotors (alternatively *wheels* or *drums*, *Walzen* in German) formed the heart of an Enigma machine. Each rotor was a disc approximately 10 cm (3.9 in) in diameter made from hard rubber or bakelite with 26 brass, spring-loaded, electrical contact pins arranged in a circle on one face; the other side housing the corresponding number of circular plate electrical contacts. The pins and contacts represent the alphabet—typically the 26 letters A–Z (this will be assumed for the rest of this description). When the rotors were mounted side-by-side on the spindle, the pins of one rotor rested against the plate contacts of the neighbouring rotor, forming an electrical connection. Inside the body of the rotor, 26 wires connected each pin on one side to a contact on the other in a complex

pattern. Most of the rotors were identified by Roman numerals, and each issued copy of rotor I was wired identically to all others. The same was 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 came 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.

When placed in an Enigma, each rotor can be set to one of 26 possible positions. When inserted, it can be turned by hand using the grooved finger-wheel, which protrudes from the internal Enigma cover when closed. So that the operator can know the rotor's position, each had an *alphabet tyre* (or letter ring) attached to the outside of the rotor disc, with 26 characters (typically letters); one of these could be seen through the window, 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 was a part of the initial setting 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 contained a notch (or more than one) that controlled 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.

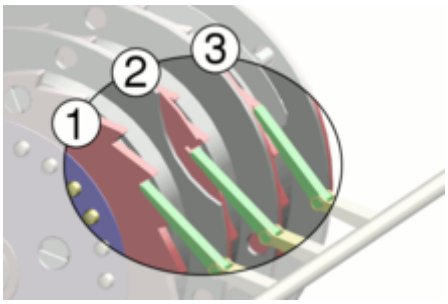
The Naval version of the *Wehrmacht* Enigma had always been issued with more rotors than the other services: at first six, then seven, and finally eight. The additional rotors were marked VI, VII and VIII, all with different wiring, and had two notches, resulting in more frequent turnover. The four-rotor 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 (and easily 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.[11] 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:[12]

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.[11] 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).[11] 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.

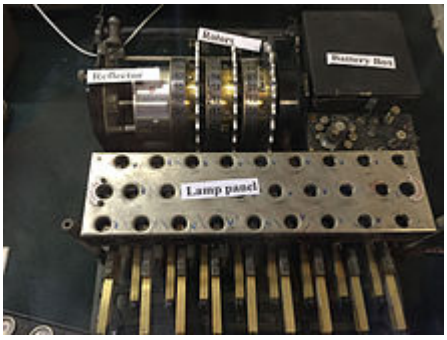
To make room for the Naval fourth rotors, the reflector was made much thinner. The fourth rotor fitted into the space made available. No other changes were made, which eased the changeover. Since there were only three pawls, the fourth rotor never stepped, but could be manually set into one of 26 possible 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.[13]

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: $Q \rightarrow A$, $W \rightarrow B$, $E \rightarrow C$ and so on. The military Enigma connects them in straight alphabetical order: $A \rightarrow A$, $B \rightarrow B$, $C \rightarrow C$, 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 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 is self-reciprocal: conveniently, encryption was the same as decryption. The reflector also gave Enigma the property that no letter ever encrypted to itself. This was a severe conceptual flaw and a cryptological mistake 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', 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.[14] The fourth version, first observed on 2 January 1944, had a rewireable reflector, called *Umkehrwalze D*, 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 1930, and was soon adopted by the *Reichsmarine* (German Navy). The plugboard contributed more cryptographic strength than an extra rotor. Enigma without a plugboard (known as *unsteckered Enigma*) can be solved relatively straightforwardly using hand methods; these techniques are 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 presses *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.[15]

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 lightbulbs be removed.[10] 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.[10] In one switch position, the *Uhr* did not swap letters, but simply emulated the 13 stecker wires with plugs.

The Enigma Uhr attachment

Mathematical analysis

The Enigma transformation for each letter can be specified mathematically as a product of permutations.[16] 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 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 transformation can then be described as

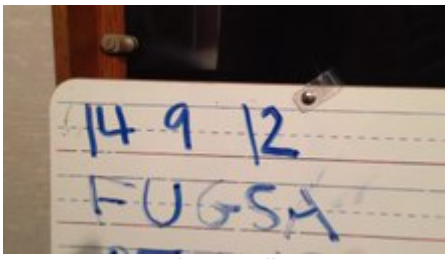
$$E = P(\rho^i R \rho^{-i})(\rho^j M \rho^{-j})(\rho^k L \rho^{-k}) U (\rho^k L^{-1} \rho^{-k})(\rho^j M^{-1} \rho^{-j})(\rho^i R^{-1} \rho^{-i}) P^{-1}.$$

Combining three rotors from a set of five, the 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 (nearly 159 quintillion) different settings.[17]

Operation

Basic operation

A German Enigma operator would be given a plaintext message to encrypt. For each letter typed in, a lamp indicated a different letter according to a pseudo-random substitution, based upon the wiring of the machine. The letter indicated by the lamp would be recorded as the enciphered substitution. The action of pressing a key also moved the rotor so that the next key press used a different electrical pathway, and thus a different substitution would occur. For each key press there was rotation of at least the right hand rotor, giving a different substitution alphabet. This continued for each letter in the message until the message was completed and a series of substitutions, each different from the others, had occurred to create a cyphertext from the plaintext. The cyphertext would then be transmitted as normal to an operator of another Enigma machine. This operator would key 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.



Play media
Enciphering and deciphering using an enigma machine

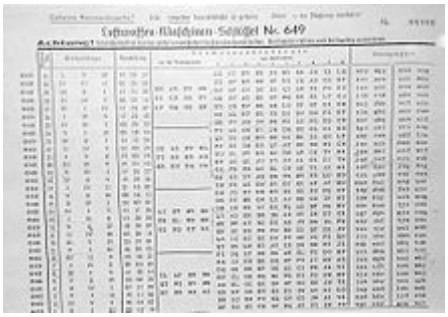
Details

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.


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

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.


Monthly key list Number 649 for the German Air Force Enigma, including settings for the reconfigurable reflector.

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 x 10^{114} (approximately 380 bits); with known wiring and other operational constraints, this is reduced to around 10^{23} (76 bits).[18] Users of Enigma were confident of its security because of the large number of possibilities; 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.[19] 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. The results were the encrypted indicator. The *EIN* typed twice might encrypt into *XHTLOA*, which would be transmitted along with the encrypted message. Finally, the operator then spun the rotors to his message settings, *EIN* in this example, and typed the plaintext of the message.

At the receiving end, the operator set the machine to the initial settings 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 select 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".[20]

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.[21]

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.[22]

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.

The *Kriegsmarine*, using the four rotor Enigma, had four-character groups. Frequently used names or words were varied as much as possible. Words like *Minensuchboot* (minesweeper) could be written as MINENSUCHBOOT, MINBOOT, MMMBOOT or MMM354. To make cryptanalysis harder, messages were limited to 250 characters. Longer messages were divided into several parts, each using a different message key.[23][24]

History

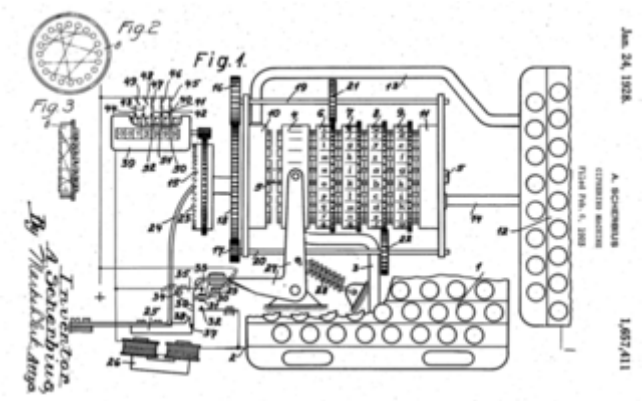
The Enigma family included multiple designs. The earliest were commercial models dating from the early 1920s. Starting in the mid-1920s, the German military began to use Enigma, making a number of security-related changes. Various nations either adopted or adapted the design for their own cipher machines.

A selection of seven Enigma machines and paraphernalia exhibited at the US 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 100,000 Enigma machines were constructed. After the end of World War II, the Allies sold captured Enigma machines, still widely considered secure, to developing countries.[25]

Commercial Enigma

On 23 February 1918, Arthur Scherbius applied for a patent for a ciphering machine that used rotors.[26] Scherbius and E. Richard Ritter and 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's Enigma patent—U.S. Patent 1,657,411, granted in 1928.

Enigma A (1923)

Chiffriermaschinen AG began advertising a rotor machine—*Enigma model A*—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).

Enigma B (1924)

In 1924 Enigma *model B* was introduced, and was of a similar construction.[27] 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.

Enigma C (1926)

The reflector—suggested by Scherbius's colleague Willi Korn—was introduced in *Enigma C* (1926).

Model C was smaller and more portable than its predecessors. It lacked a typewriter, relying on the operator; hence the informal name of "glowlamp Enigma" to distinguish it from models *A* and *B*.

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 that suitable cribs were available.[28]

"Navy Cipher D" – Italian Navy

Other countries 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.[29] Enigma 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 communications, but that it was soon withdrawn, as it was unreliable and jammed frequently.[30]

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 was cracked by Poland, France, the United Kingdom and the United States (the latter codenamed it INDIGO). An *Enigma T* model (codenamed *Tirpitz*) was used by Japan.

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

Typex

Once the British broke the Enigma, they fixed the problem with it and created their own, which the Germans believed to be unsolvable.[31]

Military Enigma

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.[32]

The keyboard and lampboard contained 29 letters—A-Z, Ä, Ö and Ü—which were arranged alphabetically, as opposed to the QWERTZUI ordering.[33] The rotors had 28 contacts, with the letter *X* wired to bypass the rotors unencrypted.[8] 3 rotors were chosen from a set of five[34] and the reflector could be inserted in one of four different positions, denoted α, β, γ and δ.[35] The machine was revised slightly in July 1933.[36]

Enigma G (1928–1930)

By 15 July 1928,[37] 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 which 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.[38] 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[39]) 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).[40]

In August 1935, the Air Force introduced the Wehrmacht Enigma for their communications.[38]

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.[41] The Reichsmarine eventually agreed and in 1934[42] 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.[43]

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.[38] 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.[43]

Heinz Guderian in the Battle of France, with an Enigma machine

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 (image Bundesarchiv)

Enigma

Breaking Enigma

Surviving machines

US Enigma replica on display at the National Cryptologic Museumin Fort Meade, Maryland, USA.

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.[44]

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, 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,[45] Norway, The Artillery, Engineers and Signals Museum in Hämeenlinna, Finland[46] the Technical University of Denmark in Lyngby, Denmark, and at the Australian War Memorial and in the foyer of the Defence Signals Directorate, both in Canberra, Australia. The Jozef Pilsudski Institute in London exhibits a rare Polish Enigma double assembled in France in 1940.[47][48]

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 at the Museum of Science and Industry in Chicago, Illinois. A four rotor device is on display in the ANZUS Corridor of the Pentagon on the second floor, A ring, between corridors 9 and 10. 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's also a machine located at the National World War II Museum in New Orleans. The Museum of World War II in 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 themselves.

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

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 4-rotor Enigma machine is on display at the Military Communications and Electronics Museum at Canadian Forces Base (CFB) Kingstonin Kingston, Ontario.

Occasionally, Enigma machines are sold at auction; prices have in recent years ranged from US$40,000[49][50] to US$547,500[51] in 2017. Replicas are available in various forms, including an exact reconstructed copy of the Naval M4 model, an Enigma implemente 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.

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 10 months in prison and served three months.[52]

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 4-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,[53][54] including one at the National Museum of Science and Technology (MUNCYT) in La Coruña. Two have been given to Britain's GCHQ.[55]

The Bulgarian military used Enigma machines with a Cyrillic keyboard; one is on display in the National Museum of Military History in Sofia.[56]

Derivatives

The Enigma was influential in the field of cipher machine design, spinning off other rotor machines. The British Typex was originally derived from the Enigma patents; 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, to protect secrecy. The Typex implementation is not the same as that found in German or other Axis versions.

A Japanese Enigma clone was codenamed GREEN by American cryptographers. Little used, it contained four rotors mounted vertically. In the U.S., cryptologist William Friedman designed the M-325, a machine logically similar, although not in construction.

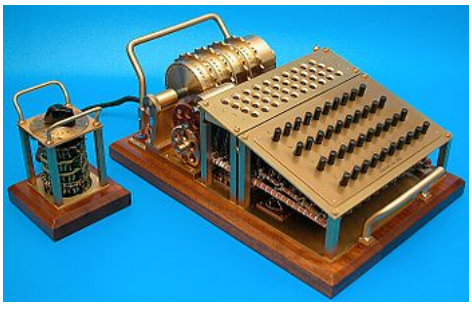
A unique rotor machine was constructed in 2002 by Netherlands-based Tatjana van Vark. This device makes use of 40-point rotors, allowing letters, numbers and some punctuation to be used; each rotor contains 509 parts.[57]

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

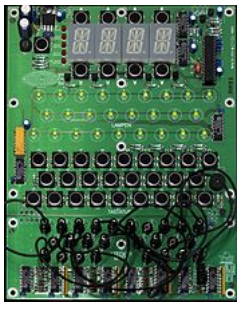
Several software implementations exist, but not all exactly match Enigma behaviour. The most commonly used software derivative (that is not compliant with any hardware implementation of the Enigma) is at EnigmaCo.de. Many Java applet Enigmas only accept single letter entry, complicating use even if the applet is Enigma compliant. Technically, Enigma@home is the largest scale deployment of a software Enigma, but the decoding software does not implement encipherment making it a derivative (as all original machines could cipher and decipher).

A user-friendly 3-rotor simulator, where users can select rotors, use the plugboard and define new settings for the rotors and reflectors is available.[58] The output appears in separate windows which can be independently made "invisible" to hide decryption.[59] Another includes an "autotyping" function which takes plaintext from a clipboard and converts it to cyphertext (or vice versa) at one of four speeds. The "very fast" option produces 26 characters in less than one second.[60]

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

Name	Platform	Machine types	Uhr	UKW-D
Franklin Heath Enigma Simulator[61]	Android	K Railway, Kriegsmarine M3,M4	No	No
EnigmAndroid[62]	Android	Wehrmacht I, Kriegsmarine M3, M4, Abwehr G31, G312, G260, D, K, Swiss-K, KD, R, T	No	No
Andy Carlson Enigma Applet (Standalone Version)[63]	Java	Kriegsmarine M3, M4	No	No
Minarke (Minarke Is Not A Real Kriegsmarine Enigma)[64]	C/Posix/CLI (MacOS, Linux, UNIX, etc.)	Wehrmacht, Kriegsmarine, M3, M4	No	No
Russell Schwager Enigma Simulator[65]	Java	Kriegsmarine M3	No	No
PA3DBJ G-312 Enigma Simulator[66]	Javascript	G312 Abwehr	No	No
Daniel Palloks Universal Enigma[67]	Javascript	Wehrmacht, Kriegsmarine M3, M4. D (commercial), K (Swiss), Railway, Tirpitz (Japan), A-865 Zählwerk, G-111 Hungary/Munich, G-260 Abwehr/Argentina, G-312 Abwehr/Bletchley	Yes	No
Universal Enigma Machine Simulator[68]	Javascript	D, I, Norway, M3, M4, Zählwerk, G, G-111, G260, G-312, K, Swiss-K, KD, Railway, T	Yes	Yes
Terry Long Enigma Simulator[69]	MacOS	Kriegsmarine M3	No	No
Paul Reuvers Enigma Simulator for RISC OS[70]	RISC OS	Kriegsmarine M3, M4, G-312 Abwehr	No	No
Dirk Rijmenants Enigma Simulator v7.0[71]	Windows	Wehrmacht, Kriegsmarine M3, M4	No	No
Frode Weierud Enigma Simulators[72]	Windows	Abwehr, Kriegsmarine M3, M4, Railway	No	No

In popular culture

Literature

- Hugh Whitemore's play, *Breaking the Code* (1986), focuses on the life and death of Alan Turing, who was the central force in continuing to solve the Enigma code in the United Kingdom, during World War II. Turing was played by Derek Jacobi, who also played Turing in a 1996 television adaptation of the play.
- Robert Harris' novel *Enigma* (1995) is set against the backdrop of World War II Bletchley Park and cryptologists working to read Naval Enigma in Hut 8.
- Neal Stephenson's novel *Cryptonomicon* (1999) prominently features the Enigma machine and efforts to break it, and portrays the German U-boat command under Karl Dönitz using it in apparently deliberate ignorance of its penetration.

Films

- *Sekret Enigmy* (1979; translation: *The Enigma Secret*), is a Polish film dealing with Polish aspects of the subject.[73]
- The plot of the film *U-571* (released in 2000) revolves around an attempt by American, rather than British, forces to seize an Enigma machine from a German U-boat.
- Harris' book, with substantial changes in plot, was adapted as the film *Enigma* (2001), directed by Michael Apted and starring Kate Winslet and Dougray Scott. The film was criticised for historical inaccuracies, including neglect of the role of Poland's *Biuro Szyfrów*. The film—like the book—makes a Pole the villain, who seeks to betray the secret of Enigma decryption.[74]
- The film *The Imitation Game* (2014) tells the story of Alan Turing and his attempts to crack the Enigma machine code during World War II.[44]

Television

- In the British television series *The Bletchley Circle*, the Typex was used by the protagonists during the war, and in Season 2, Episode 4, they visit Bletchley Park to seek one out, in order to crack the code of the black market procurer and smuggler Marta, who used the Typex to encode her ledger. The Circle, forced to settle for using an Enigma, instead, successfully cracks the code.
- In season 5, episode 23 ("Scrambled") of the American television series *Elementary* a drug smuggling gang uses a four-rotor Enigma machine as part of their effort to encrypt their communications.

See also

- Beaumanor Hall, a stately home used during the Second World War for military intelligence
- Joan Clarke
- Erich Fellgiebel
- Gisbert Hasenjaeger—responsible for Enigma security
- Fritz Thiele
- United States Naval Computing Machine Laboratory
- Arlington Hall
- Enigma - disambiguation page

References

Notes

1. 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.
2. Lord, Bob (1998–2010). "1937 Enigma Manual by: Jasper Rosal – English Translation" (http://www.ilord.com/enigma-manual1937-english.html). Retrieved 31 May 2011.
3. Kozaczuk 1984, p. 63.
4. Ralph Erskine: *The Poles Reveal their Secrets – Alastair Dennistons's Account of the July 1939 Meeting at Pyry*. Cryptologia. Rose-Hulman Institute of Technology. Taylor & Francis, Philadelphia PA 30.2006,4, p. 294.
5. 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." Gordon Welchman, *The Hut Six Story*, 1982, p. 289.
6. 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.
7. Kahn 1991.
8. Stripp 1993.

9. "History of the Enigma" (http://www.cryptomuseum.com/crypto/enigma/hist.htm). Crypto Museum. Retrieved 1 Dec 2017.
10. Rijmenants, Dirk; Technical details of the Enigma machine (http://users.telenet.be/d.rijmenants/en/enigmatech.htm) Cipher Machines & Cryptology
11. 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.
12. 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.
13. "Lückenfüllerwalze" (http://www.cryptomuseum.com/crypto/enigma/lf/index.htm). Cryptomuseum.com Retrieved 17 July 2012.
14. Philip Marks, "Umkehrwalze D: Enigma's Rewirable Reflector — Part I", Cryptologia 25(2), April 2001, pp. 101–141
15. Reuvers, Paul (2008). "Enigma accessories" (http://www.jproc.ca/crypto/enigma_acc.html). Retrieved 22 July 2010.
16. Rejewski 1980.
17. 158,962,555,217,826,360,000 – Numberphile (https://www.youtube.com/watch?v=G2_Q9FoD-oQ) on YouTube
18. Miller, A. Ray (2001). "The Cryptographic Mathematics of Enigma" (http://www.nsa.gov/about/_files/cryptologic_heritage/publications/wwii/engima_cryptographic_mathematics.pdf) (PDF). National Security Agency
19. 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)
20. Huttenhain & Fricke 1945, pp. 4,5.
21. Rijmenants, Dirk; Enigma message procedures (http://users.telenet.be/d.rijmenants/en/enigmaproc.htm) Cipher Machines & Cryptology
22. Rijmenants, Dirk; Kurzsignalen on German U-boats (http://users.telenet.be/d.rijmenants/en/kurzsignale.htm) Cipher Machines & Cryptology
23. "The translated 1940 *Enigma General Procedure*" (http://www.codesandciphers.org.uk/documents/egenproc/eniggnix.htm). codesandciphers.org.uk Retrieved 16 October 2006.
24. "The translated 1940 *Enigma Officer and Staff Procedure*" (http://www.codesandciphers.org.uk/documents/officer/officerx.htm). codesandciphers.org.uk Retrieved 16 October 2006.
25. Bauer 2000, p. 112.
26. US 1657411 (https://worldwide.espacenet.com/textdoc?DB=EPODOC&IDX=US1657411) Scherbius, Arthur, "Ciphering Machine", issued January 24, 1928, assigned to Chiffriermaschinen AG
27. "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.
28. Bletchley Park Trust Museum display
29. Smith 2006, p. 23.
30. Kozaczuk 1984, p. 28.
31. Numberphile (2013-01-14), *Flaw in the Enigma Code - Numberphile* (https://www.youtube.com/watch?v=V4V2bpZlqx8), retrieved 2017-02-14
32. Kahn 1991, pp. 39–41, 299.
33. Ulbricht 2005, p. 4.
34. Kahn 1991, pp. 40, 299.
35. Bauer 2000, p. 108.
36. Stripp 1993, plate 3.
37. Kahn 1991, pp. 41, 299.
38. Kruh & Deavours 2002, p. 97.
39. Smith 2000, p. 73.
40. Stripp, 1993
41. Kahn 1991, p. 43.

42. Kahn 1991, p. 43 says August 1934. Kruh & Deavours 2002, p. 15 say October 2004.
43. Kruh & Deavours 2002, p. 98.
44. 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.
45. "War Museum" (http://www.warmuseum.no/no/English/)
46. "The National Signals Museum" (http://www.viestikiltojenliitto.fi/viestimuseo/_eng/index.html).
47. "Enigma exhibition in London pays tribute to Poles" (http://www.thenews.pl/1/10/Artykul/244703,Enigma-exhibition-in-London-pays-tribute-to-Poles) *Polskie Radio dla Zagranicy*. Retrieved 2016-04-05.
48. "13 March 2016, 'Enigma Relay' – how Poles passed the baton to Brits in the run for WWII victory" (http://pilsudski.org.uk/en/aktualnosci.php?news=205&wid=13&wai=&year=&back=%252Fen%252F) *pilsudski.org.uk*. Retrieved 2016-04-05.
49. 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.
50. 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
51. 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)
52. "Man jailed over Enigma machine" (http://news.bbc.co.uk/1/hi/uk/1609168.stm) *BBC News*. 19 October 2001. Retrieved 2 May 2010.
53. 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.
54. "Taller de Criptografía – Enigmas españolas" (http://www.cripto.es/museo/enigma-esp-fotos.htm). Cripto.es. Retrieved 8 September 2013.
55. "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.
56. "Communication equipment" (http://www.znam.bg/com/action/showArticle?appID=3&encID=2&article=3514226659&sectionID=1). znam.bg. 29 November 2003.
57. van Vark, Tatjana *The coding machine* (http://www.tatjavanvark.nl/tvv1/pht10.html)
58. 3 rotor download (http://w1tp.com/enigma/enigma_w.zip)
59. Enigma at Multimania (http://membres.multimania.fr/pc1/enigma/)
60. Autotype download (http://w1tp.com/enigma/EnigmaSim.zip)
61. Franklin Heath Ltd. "Enigma Simulator – Android Apps on Google Play" (https://play.google.com/store/apps/details?id=uk.co.franklinheath.enigmasim&hl=en) *google.com*.
62. "F-Droid" (https://f-droid.org/repository/browse/?fdid=de.vanitasvitae.enigmandroid) *f-droid.org*.
63. Andy Carlson, Enigma Applet (Standalone Version) (http://www.mtholyoke.edu/~adurfee/cryptology/enigma_j.html)
64. John Gilbert, Minarke – A Terminal Friendly Enigma Emulator (http://sourceforge.net/projects/minarke)
65. Russell Schwager, Enigma Simulator Russell Schwager Enigma Simulator (http://russells.freeshell.org/enigma/)
66. PA3DBJ G-312, Enigma Simulator (http://home.caiway.nl/~antonh/enigma_ga.html)
67. Daniel Palloks, Universal Enigma (http://people.physik.hu-berlin.de/~palloks/js/enigma/index_en.html)
68. Summerside Makerspace, Universal Enigma Machine Simulator (http://summersidemakerspace.ca/projects/enigma-machine/)
69. Terry Long, Enigma Simulator (http://www.macupdate.com/app/mac/25427/enigma-simulator)
70. Paul Reuvers, Enigma Simulator for RISC OS (http://www.cryptomuseum.com/crypto/enigma/sim/riscos.htm)
71. Dirk Rijmenants, Enigma Simulator v7.0 (http://users.telenet.be/d.rijmenants/en/enigmasim.htm)
72. Frode Weierud Enigma Simulators (http://cryptocellar.org/simula/)
73. *Enigma machine* (http://www.imdb.com/title/tt0079878/) on IMDb

74. Laurence Peter (20 July 2009). "How Poles cracked Nazi Enigma secret" (http://news.bbc.co.uk/2/hi/europe/8158782.stm). BBC News.

Bibliography

- Bauer, F. L. (2000). *Decrypted Secrets* (2nd ed.). Springer. ISBN 3-540-66871-3.
- Hamer, David H.; Sullivan, Geoff; Weierud, Frode (July 1998). "Enigma Variations: An Extended Family of Machines" (PDF). *Cryptologia*. Abingdon: Taylor & Francis. **XXII** (3). doi:10.1080/0161-119891886885. ISSN 0161-1194. Retrieved 18 February 2016.
- Stripp, Alan (1993). Hinsley F. H.; Stripp, Alan, eds. *The Enigma Machine: Its Mechanism and Use*. *Codebreakers: The Inside Story of Bletchley Park*.
- Kahn, David (1991). *Seizing the Enigma: The Race to Break the German U-Boats Codes, 1939–1943*. ISBN 0-395-42739-8.
- 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*. Frederick, MD: University Publications of America. ISBN 0-89093-547-5.
- Kozaczuk, Władysław. "The origins of the Enigma/ULTRA". Archived from the original 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.
- Marks, Philip; Weierud, Frode (2000). "Recovering the Wiring of Enigma's Umkehrwalze A" (PDF). *Cryptologia*. **24** (1): 55–66. doi:10.1080/0161-110091888781. Archived from the original (PDF) on 13 February 2012.
- Rejewski, Marian (1980). "An Application of the Theory of Permutations in Breaking the Enigma Cipher". *Applicationes mathematicae* **16** (4). ISSN 1730-6280.
- Smith, Michael (2000). *Station X: The Codebreakers of Bletchley Park*. Pan. ISBN 0-7522-7148-2.
- Smith, Michael (2006). "How it began: Bletchley Park Goes to War". In Copeland, B Jack. *Colossus: The Secrets of Bletchley Park's Codebreaking Computers*. Oxford: Oxford University Press. ISBN 978-0-19-284055-4.
- Ulbricht, Heinz (2005). "Die Chiffriermaschine Enigma — Trügerische Sicherheit: Ein Beitrag zur Geschichte der Nachrichtendienste" [The Enigma Cipher Machine — Deceptive Security: A contribution to the history of intelligence services] (PDF). PhD Thesis (in German).

Further reading

- Aldrich, Richard James (2010). *GCHQ: The Uncensored Story of Britain's Most Secret Intelligence Agency*. HarperPress. ISBN 978-0-00-727847-3.
- Bertrand, Gustave (1973). *Enigma: ou, La plus grande énigme de la guerre 1939–1945*. Plon.
- Calvocoressi, Peter (2001). *Top Secret Ultra*. M & M Baldwin. pp. 98–103. ISBN 978-0-947712-41-9.
- Grime, James. "Enigma – 158,962,555,217,826,360,000". *Numberphile*. Brady Haran.
- Grime, James. "The Enigma Flaw". *Numberphile*. Brady Haran.
- Heath, Nick, Hacking the Nazis: The secret story of the women who broke Hitler's codes. TechRepublic, 27 March 2015
- Herivel, John (2008). *Herivelismus: And the German Military Enigma*. M & M Baldwin.
- Huttenhain, Orr; Fricke (1945), *OKW/Chi Cryptanalytic Research on Enigma, Hagelin and Cipher Teleprinter Messages*, TICOM
- Keen, John (1 August 2012). *Harold 'Doc' Keen and the Bletchley Park Bombe*. M & M Baldwin. ISBN 978-0-947712-48-8.
- Large, Christine (6 October 2003). *Hijacking Enigma: The Insider's Tale*. 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 Lafont.

- 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
- 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*. *The German Enigma Cipher Machine: Beginnings, Success, and Ultimate Failure*. Artech House. ISBN 978-1-58053-996-8
- Rejewski, Marian. [1] *How Polish Mathematicians Deciphered the Enigma"*. 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
- 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.
- Welchman, Gordon (1982). *The Hut Six Story: Breaking the Enigma Codes*. McGraw-Hill. ISBN 978-0-07-069180-3
- Winterbotham, F. W. (1999). *The Ultra Secret*. Weidenfeld & Nicolson. ISBN 978-0-297-64405-7.

External links

- Gordon Corera, Poland's overlooked Enigma codebreakers, BBC News Magazine, 4 July 2014
- Long-running list of places to visit a unit in the real world
- Bletchley Park National Code Centre Home of the British codebreakers during the Second World War
- Enigma machines on the Crypto Museum website
- Pictures of a four-rotor naval enigma, including Flash (SWF) views of the machine
- Enigma Pictures and Demonstration by NSA Employee at RSA
- Enigma machine at Curlie (based on DMOZ)
- Kenngruppenheft
- Process of building an Enigma M4 replica
- Breaking German Navy Ciphers
- An online Enigma Machine simulator
- Enigma simulation
- Enigma Simulator APK
- Universal Enigma simulator
- Public Enigma Simulator – Java simulator, including 13 Enigma machine variations