

ENIGMA SIM MANUAL

About the Enigma Sim

The program is an exact simulation of the 3-rotor Wehrmacht & Luftwaffe, the 3-rotor Kriegsmarine M3, and the famous 4-rotor Kriegsmarine M4 model of the German Enigma cipher machine, as they were used during World War II from 1939 until 1945. You can select between the three models, choose different rotors or 'Walzen', preset the rotor wiring positions or 'Ringstellung' and switch letters by using plugs or 'Stecker'. The internal wiring of all rotors is identical to those used by the Wehrmacht, Luftwaffe and Kriegsmarine. This simulator is therefore fully compatible with the real Enigma-machine and you can decipher original messages and encipher your own messages.

This manual explains how to use the Enigma simulator, describes the message procedures as used by the German Armed Forces, a complete technical description and a brief history of the Enigma.



For more information, please visit
Cipher Machines & Cryptology
<http://users.telenet.be/d.rijmenants>

Copyright Information

THE ENIGMA SIMULATOR SOFTWARE IS FREWARE AND CAN BE USED AND DISTRIBUTED UNDER THE FOLLOWING RESTRICTIONS: IT IS STRICTLY FORBIDDEN TO USE THIS SOFTWARE OR COPIES OR PARTS OF IT FOR COMMERCIAL PURPOSES, OR TO SELL, LEASE OR MAKE PROFIT FROM THIS PROGRAM BY ANY MEANS. THIS SOFTWARE MAY ONLY BE USED IF YOU AGREE TO THESE CONDITIONS.

Picture Gallery Copyrights:
© Tom Perera, Enigma Museum - <http://w1tp.com/mcpu.htm>
© KMi The Open University

DISCLAIMER OF WARRANTIES

THIS SOFTWARE AND THE ACCOMPANYING FILES ARE SUPPLIED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, WITH RESPECT TO THIS PRODUCT, ITS QUALITY, PERFORMANCE, MERCHANTABILITY, OR FITNESS FOR ANY PARTICULAR PURPOSE. THE ENTIRE RISK AS TO IT'S QUALITY AND PERFORMANCE IS WITH THE USER. IN NO EVENT WILL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES RESULTING OUT OF THE USE OF OR INABILITY TO USE THIS PRODUCT.

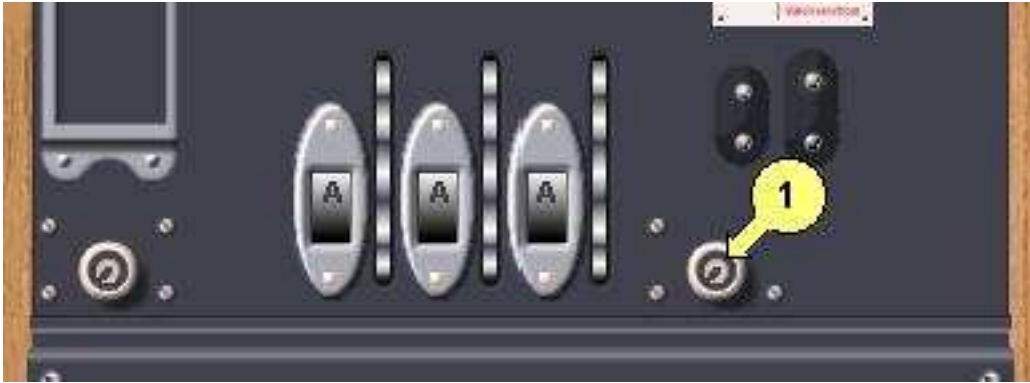
© D. Rijmenants 2008
Cipher Machines & Cryptology
<http://users.telenet.be/d.rijmenants>

How to use the simulator

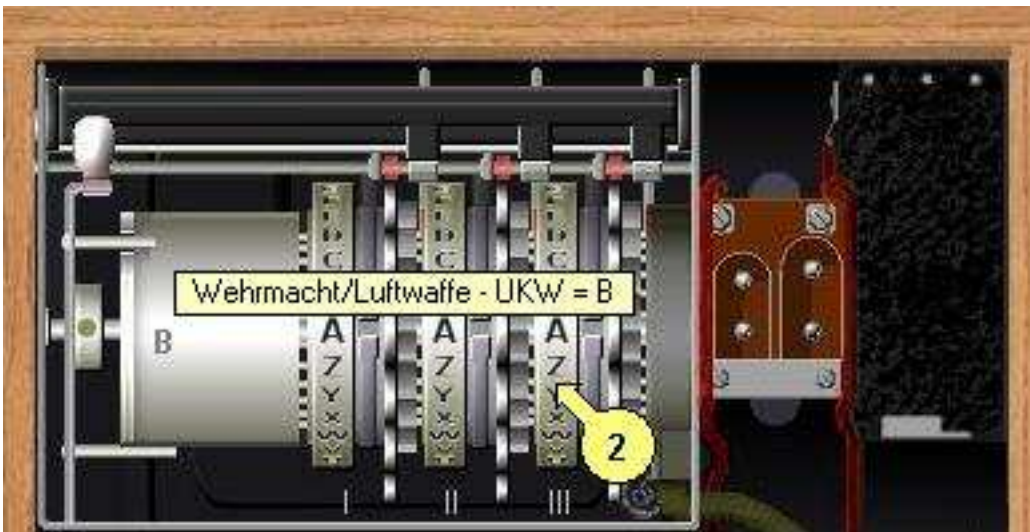
To prepare the Enigma Simulator for use, we need to select the reflector, the rotors and their order, adjust the ring settings, insert the plugs and set the machine in the start position. As you will notice, there will always be a little hand visible when you move the mouse to places where you can select or click something. You can also click or move the mouse over the white power label in the right top corner to call the Simulator Menu.

Setting the rotors in the proper positions

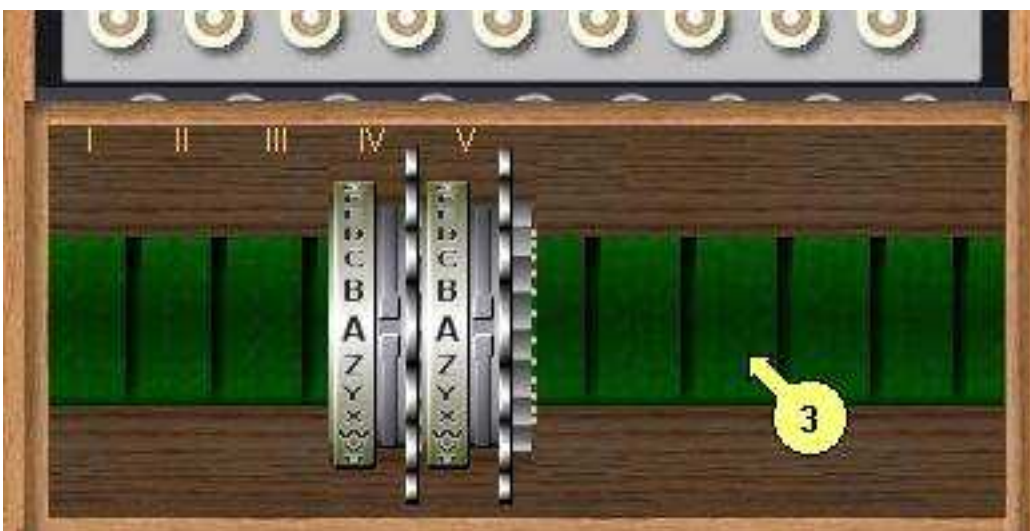
Click on the right lock [1] to open the cover and reveal the Enigma mechanism.



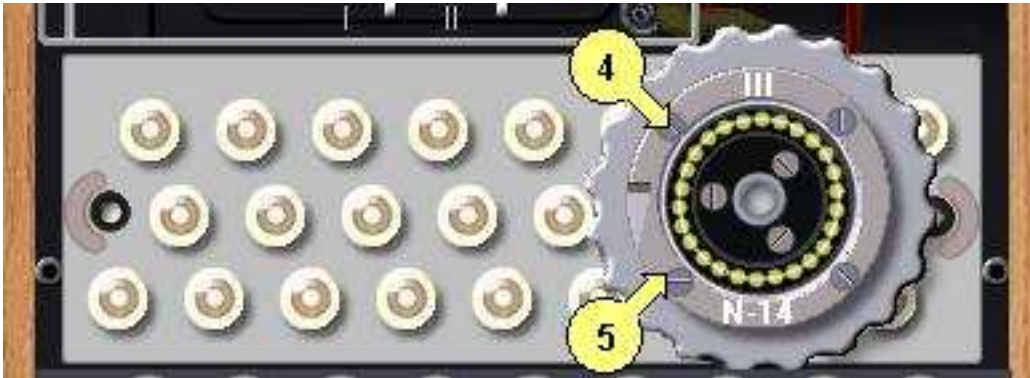
Click on a rotor [2] in the Enigma to lift it out of the machine.



Click on an empty place [3] in the rotor box to put that rotor in the box.



Now you can select another rotor from the box. Once it is out of the box, you can adjust the 'Ringstellung' by clicking on the upper [4] or lower [5] half of the displayed rotor. When the rotor is adjusted, you must click on an empty place in the Enigma to place the rotor in that position. If you find it easier, you can lift out all the rotors and put them into the box first, and then select, adjust and insert them one by one in the machine.



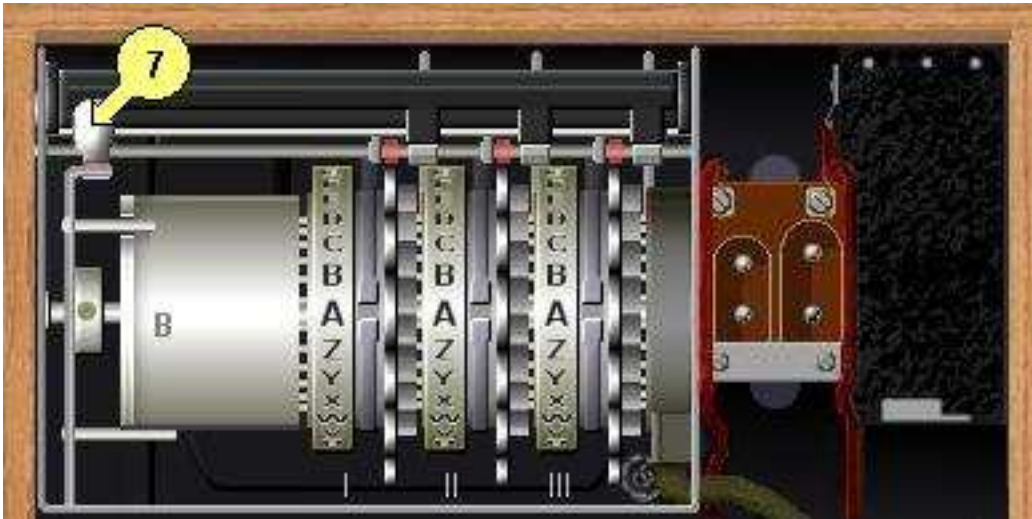
Selecting the reflectors

You can change the reflector [6] by left-or right clicking the letter on the reflector. By changing the reflector, you can select the different Enigma models.



You will go through the wide B and C reflector from the 3-rotor Wehrmacht and Luftwaffe model, the wide B and C reflector from the 3-rotor Kriegsmarine M3, and the thin B and C from the 4-rotor Kriegsmarine M4 model. Notice that on the Wehrmacht-Luftwaffe model, you can select between five rotors and two wide reflectors, on the Kriegsmarine M3 between eight rotors and two wide reflectors, and on the M4 you have the choice between eight rotors, two special 'Zusatzwalzen' or Greek rotors named Beta and Gamma (which cannot advance) that are placed just before the thin reflector, and the two thin reflectors.

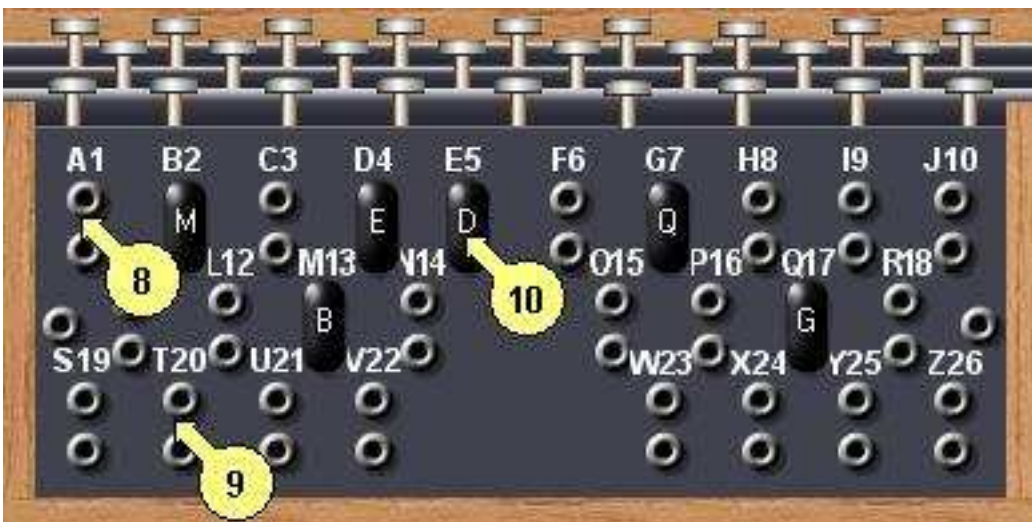
Once all rotors are in place you can close the cover by clicking on the handle [7] at the left, above the reflector.



Special note on the rotors: If you use the M4 model with the thin B reflector and the Beta rotor as 4th rotor in 'zero-position' (rotor and ring set to A), the machine is compatible with its predecessor, the 3-rotor M3 model, and the 3-rotor Army model with wide B reflector (of course, they are compatible only when the other three rotors and the settings are the same). The rotor wirings were designed so that different components of the army could exchange messages, although they had different Enigma models

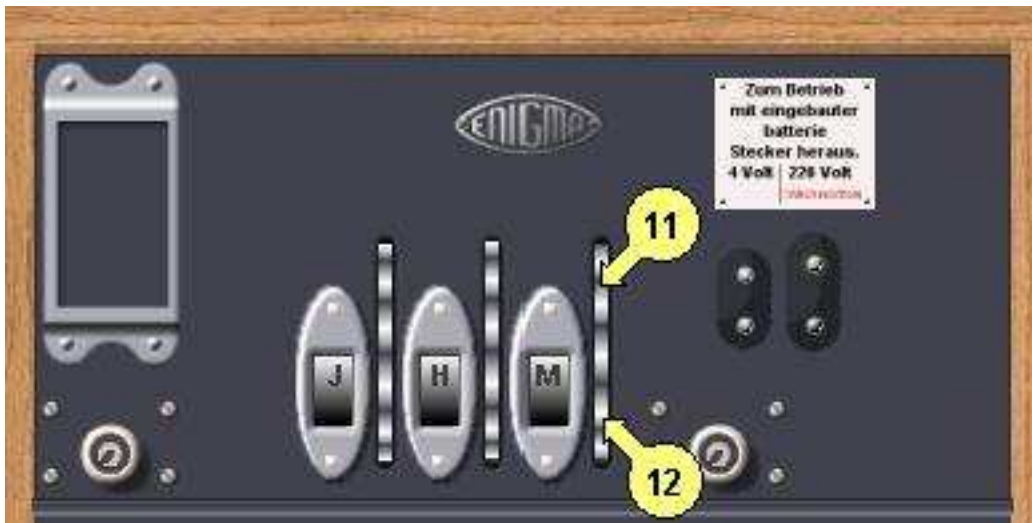
Connecting the plugs

To connect plugs from one socket to another (to switch the letter connections) you must click on the plugs at the bottom of the Enigma. The plugboard or 'Steckerbrett' will appear. Just click the desired socket [8] and the socket that you want to connect it to [9]. To clear a connection, just click one of the plugs [10] and both connected plugs disappear. After finishing the plug settings you can return to the Enigma by clicking the keys on the top.



Setting the Start Position

On the main screen you can change the start position or 'Grundstellung' of the rotors by clicking the upper [11] or lower [12] half of the rotor's wheel. The start position can be saved temporary by pressing INS, and can be retrieved later by pressing HOME.



The Text box and Clipboard

As an extra feature, you can display the encoded and decoded text in a window at the bottom of the Enigma by clicking the lock [13] on the wooden box. Press DEL or Backspace to clear this text box. Click again on the lock to hide the text box. This text box is a handy feature when coding long pieces of text. If you click in this text box or press F5, the Smart Clipboard Window appears. You can select in various ways how to format and transfer text to the clipboard. The text output is arranged in groups of five letters for the Wehrmacht machine and groups of four letters for both Naval M3 and M4 machines.



Using the Auto Typing option

If you have a large amount of plain text or code that needs to be typed, you can use the Auto Typing Window. This window will appear if you press F6. In this window you can type, edit or paste pieces of text, or retrieve the content of the clipboard. You can select four different speeds of typing. Select 'Start' to begin processing the text. During the Auto Typing you can abort by pressing ESC. Make sure that all settings are finished and the rotors are in the start position before starting the Auto Typing.

Note: Auto Typing will only process alphabet characters and ignore all other characters like figures, signs and spaces. When decoding, make sure that there are no 'Kennggruppen' in the code text or delete the 'Kennggruppen' in the text window.

Save and Load Machine Settings

In the Simulator Menu (click the white power label) you can view the current machine setup and the file name, save the current settings or load other settings, or clear and return to default settings. The machine settings are save with the .eni extension. On startup the simulator will be loaded with the last used settings. If no settings file is found the default settings are loaded.

Exiting the simulator

To exit the Enigma simulator, just click on the power plug located in the upper right part of the Enigma. If desired, you can save the current rotor and plug settings (the rotor startpositions are not saved)

Cryptanalysis and test mode

For cryptanalysis and testing purposes, you can disable the rotor advance mechanism by using F10. A warning will be displayed above the rotors. Use F10 again to restore the rotor advance mechanism.

Extra's

Clicking the left lock will bring you to the picture gallery and clicking on the Enigma sign at the top will display the "about" window.

How the machine was used by the German military

Here is an example of how the German Luftwaffe sent messages that were encrypted using Enigma. The operators never used the secret daily key to encrypt the message but used this key only to encrypt a randomly chosen message-key or 'trigram' that was chosen by the operator. This message-key was used to encrypt the rest of the message. With this procedure they avoided excessive use of the secret daily key, and each message on that day was encrypted with another randomly chosen key. During the war, different systems like this were implemented to use the codebooks. In general, a codebook contained all the settings, per day, for a whole month.

The operator's key sheet contained the following information:

| Tag (Day) | Walzenlage (Rotors) | | | Ringstellung (Ringsetting) | | | Steckerverbindungen (Plug Connections) | | | | | | | | | | | |
|--------------|------------------------|----|-----|-------------------------------|----|----|---|----|----|----|----|----|----|----|----|----|--|--|
| 31 | I | II | V | 06 | 22 | 14 | PO | ML | IU | KJ | NH | YT | GB | VF | RE | DC | | |
| 30 | III | IV | II | 17 | 04 | 26 | BN | VC | XS | WQ | AZ | GT | YH | JU | IK | PM | | |
| 29 | V | I | III | 15 | 02 | 09 | ML | KJ | HG | FD | SQ | TR | EZ | IU | BV | XC | | |

On day 31 the following message is transmitted:

U6Z DE C 1510 = 44 = EHZ TBS =
QBLTW LDAHH YEOEF PTWYB LENDP MKOXL DFAMU DWIJD XRJZ=

To decode the message we take the following steps:

1. Select the Walzen (rotors) and adjust the Ringstellung, put the Walzen into the machine and set the plugs or 'Stecker' for day 31
2. Set the start position to EHZ, the first trigram of the message
3. In this position, decode the second trigram TBS to retrieve the message-key. This should result in XWB
4. Set the decoded message-key (XWB) as start position on the machine.
5. Now decode the rest of the message...

This may well be your first decoded message, Good Luck !

A second example

The following original message in two parts is a pre-release of the fruits of an on-going codebreaking project, to break a large number of original German messages, a joint effort by Geoff Sullivan and Frode Weierud, two of the members of the Crypto Simulation Group (CSG). It's a message from the SS-Totenkopf Division and is from the campaign against Russia, operation Barbarossa.

The settings as recovered by the CSG codebreakers

3-rotor model

UKW: B (reflector)

Walzenlage: 245

Ringstellung: BUL

Stecker: AV BS CG DL FU HZ IN KM OW RX

Don't forget to use the first trigram from each part as start position to decode the second trigram in order to retrieve the message-key, that is the start position for the rest of the message.

Important Note: RFUGZ and FNJAU are 'Kenngruppen', groups to identify the key that was used, and must be skipped while decoding!

The Message:

Befordert am: 07.07.1941 1925 Uhr Durch:

Funkspruch Nr.:20 Von/An: f8v/bz2

Absendende Stelle : SS-T Div Kdr An: LVI A.K.

fuer m7g 1840 - 2tl 1t 179 - WXC KCH -

RFUGZ EDPUD NRGYS ZRCXN
UYTPO MRMBO FKTBZ REZKM
LXLVE FGUEY SIOZV EQMIK
UBPMM YLKL TDEIS MDICA
GYKUA CTCDO MOHWX MUUIA
UBSTS LRNBZ SZWNR FXWFX
SSXJZ VIJHI DISHP RKLKA
YUPAD TXQSP INQMA TLPIF
SVKDA SCTAC DPBOP VHJK

2tl 155 - CRS YPJ -

FNJAU SFBWD NJUSE GQOBH
KRTAR EEZMW KPPRB XOHDR
OEQGB BGTQV PGVKB VVGBI
MHUSZ YDAJQ IROAX SSSNR
EHYGG RPISE ZBOVM QIEMM
ZCYSG QDGRE RVBIL EKXYQ
IRGIR QNRDN VRXC YTNJR
SBDPJ BFFKY QWFUS

For those who might have trouble translating the German message from above, here's the English translation (decoding the original is your job!)

Reconnaissance unit from KURTINOWA north-west of SEBEZ
on the flight corridor in direction DUBROWKI, OPOTSCHKA.
Started to move at 18:30. Attack. Infantry Regiment 3 goes
slowly but surely forwards. Time: 17:06. I (Roman number 1).
Infantry Regiment 3 on the flight corridor starting 16 km
east-west of KAMENEC.

Division Commander.

Message copyright by Geoff Sullivan and Frode Weierud

War at sea

The following fragment of a message contains an important piece of naval wartime history. It was intercepted by British codebreakers and made decisive action by the Royal Navy possible.

Settings for the message:

3-rotor model
UKW: B (reflector)
Walzenlage: 314
Stecker: BU CP EI GN HT LZ MX OS
Ringstellung: SXA (19-24-01)
Start position: LBW

The Message:

...
MQLDI BNWQB RITNG UHCQH
YTRNB ZBFXD DSEXG BNGDA
IATLL KJTEC MLKBS ZMJKW
KDUSU JKRQV YLYFT IWSRK
NQSFH FFBLB DLTDQ JTZWB
NEAQZ CMJJG KFHPU IRHFL
BUEDK IJGQU XVAYK JOKMK
GLBSP AIXCN ...

Note: Although this is a marine message, only three rotors are used. As explained, some messages were sent this way for M4 model to be compatible with the M3. Unfortunately for the Germans it gave British cryptanalysts a big hint on the complicated 4-wheel naval codes.

Notes on abbreviations

The Kriegsmarine used the following abbreviations before enciphering their text:

X = Period
Y = Comma
UD = Question Mark
XX = Colon
YY = Dash/Hyphen/Slant
KK*****KK = Parenthesis
J*****J = Stress Mark

Numbers are written out as words.

The Wehrmacht used other abbreviations:

KLAM = Parenthesis
ZZ = Comma
X = Full stop (end of sentence)
YY = Point or dot
X****X = Inverted commas

Question mark (Fragezeichen in German) is usually abbreviated to one of the three following forms: FRAGE, FRAGEZ or FRAQ

Foreign names, places etc. twice delimited by "X", e.g. XPARISXPARISS

The letters CH is written as Q, e.g. ACHT was written as AQT, RICHTUNG as RIQTUNG

It was prohibited to encipher the word "null" several times in succession. For several nulls these abbreviations are used:

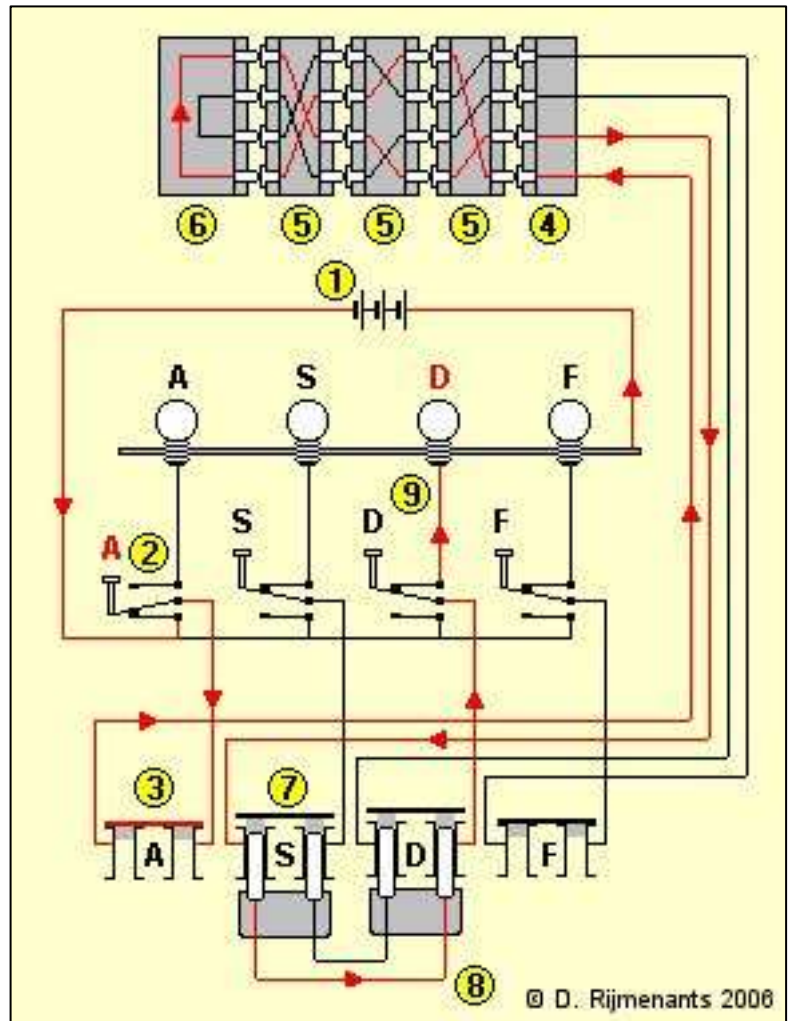
00 = CENTA
000 = MILLE
0000 = MYRIA

Examples: 200 = ZWO CENTA, 00780 = CENTA SIEBEN AQT NULL

Technical details of the Enigma Machine

The Enigma machine is an electro-mechanical device. It consists of a keyboard (German QWERTZ layout), a lamp panel, representing the alphabet, and three or four rotors. These rotors advance each time a key is depressed. Pressing a key is translated, by rotors and plugboard, into a burning lamp, representing the encoded letter. There is a compartment for a 4 volt battery in the machine and a plug to connect the machine to an exterior power supply or transformer type AC power supply.

The picture at the right shows the wiring. To simplify the example, only four of each of the components are shown. In reality, there are 26 lamps, keys, plugboard sockets and wiring connections inside the rotors. The current flows from the battery [1] through the depressed bi-directional letter-switch [2] to the plugboard [3]. The plugboard allows rewiring the connections between keyboard [2] and fixed entry wheel [4]. Next, the current proceeds through the - unused, and therefore closed - plug [3] via the entry wheel [4] through the cross-wirings of the three (Wehrmacht Enigma) or four (Kriegsmarine M4) rotors [5] and enters the reflector [6]. The reflector returns the current, via a different path, back through the rotors [5] and entry wheel [4], and proceeds through the plugboard again and through the plug 'S' connected with a cable [8] to plug 'D', and another bi-directional switch [9] to light-up the lamp. Note that depressing a key will first step the rotors and then the sent the current through the rotors en the light bulb. If the key is released the lamp will no longer light up. Therefore, when no key is depressed, the rotor position of the previous encrypted letter is visible!



The Rotors or Walzen

The rotors (Walzen in German) are the most important elements of the machine. These round disks, approximately 10 cm in diameter, are made from metal or bakelite. A disk consists of a round casing with fixed notch and visible alphabet or number ring. The center of the rotor is a rotatable small disk with 26 spring-loaded contacts on the right side, scramble wired to 26 flat contact on the left side. Changing the position of the internal wiring, relative to the notch and alphabet, is called the ring setting or Ringstellung. The internal wiring is different for each rotor. This wiring represents a substitution encryption. The combination of several rotors, in ever-changing positions relative to each other, is what makes the encryption so complex. Each rotor has on its left a notch, on its right a ratchet. These are used by the stepping mechanism to advance the rotors.

The machine was introduced with three rotors. In 1939 the set was extended to five rotors, marked with Roman numerals I, II, III, IV and V, all with a single notch. The Kriegsmarine extended the set of rotors with another three rotors called VI, VII and VIII, with two notches. In 1942, the Kriegsmarine M4 introduced a fourth rotor. To achieve this, the wide B and C reflectors from the three rotor version was replaced by thin B and C reflectors, leaving room for the special fourth rotor. The fourth rotors were of two configurations, named Beta and Gamma, with spring-loaded contacts on both sides. They were incompatible with the other eight rotors.

Rotor wiring tables

Rotors Kriegsmarine/Wehrmacht/Luftwaffe (3-rotor model)

```
Input = ABCDEFGHIJKLMNOPQRSTUVWXYZ (rotor right side)
      | | | | | | | | | | | | | | | | | | | | | |
I      = EKMFLGDQVZNTOWYHXUSPAIBRCJ
II     = AJDKSIRUXBLHWTMCQGZNPYFVOE
III    = BDFHJLCPRTXVZNYEIWGAKMUSQO
IV     = ESOVPZJAYQUIRHXLNFTGKDCMWB
V      = VZBRGITYUPSDNHLXAWMJQOFECK
```

Rotors used by Kriegsmarine only (3-rotor M3 and 4-rotor M4 model)

```
Input = ABCDEFGHIJKLMNOPQRSTUVWXYZ (rotor right side)
      | | | | | | | | | | | | | | | | | | | | | |
VI     = JPGVOUMFYQBENHZRDKASXLICTW
VII    = NZJHGRCTXMYSWBOUFAIVLPEKQDT
VIII   = FKQHTLXOCBJSPDZRAMWNIUYGW
```

The special fourth rotors, also called Zusatzwalzen or Greek rotors. Used on the Kriegsmarine M4 with thin reflectors only:

```
Input = ABCDEFGHIJKLMNOPQRSTUVWXYZ (rotor right side)
      | | | | | | | | | | | | | | | | | | | | | |
Beta  = LEYJVCNIXWPBQMDRTAKZGFUHS
Gamma = FSOKANUERHMBTIYCWLPZXVJGD
```

In the reflector wiring table we can see that the wide B reflector an 'A' returns as 'Y' and 'Y' returns as 'A'. Notice that the wirings are permanently connected as a loop between two letters. Default wide reflectors Wehrmacht and Luftwaffe:

```
Contacts      = ABCDEFGHIJKLMNOPQRSTUVWXYZ
              | | | | | | | | | | | | | | | | | | | | | |
Reflector B   = YRUHQSLDPXNGOKMIEBFZCWVJAT
Reflector C   = FVPJIAOYEDRZXWGCTKUQSBNMHL
```

Thin reflectors, Kriegsmarine M4 only:

```
Contacts      = ABCDEFGHIJKLMNOPQRSTUVWXYZ
              | | | | | | | | | | | | | | | | | | | | | |
Reflector B Thin = ENKQAUYWJICOPBLMDXZVFTHRGS
Reflector C Thin = RDOBJNTKVEHMLFCWZAXGYIPSUQ
```

Turnover positions

I = Q (if rotor steps from Q to R, the next rotor is advanced)
II = E (if rotor steps from E to F, the next rotor is advanced)
III = V (if rotor steps from V to W, the next rotor is advanced)
IV = J (if rotor steps from J to K, the next rotor is advanced)
V = Z (if rotor steps from Z to A, the next rotor is advanced)
VI, VII & VIII = Z + M (if rotor steps from Z to A, or from M to N the next rotor is advanced)

The Ring Setting or Ringstellung

On the outside of the wiring core there's a movable ring with 26 numbers or letters and a notch. This ring is rotatable and is locked with a springloaded pin (Wehrmacht) or two springloaded arcs (Kriegsmarine) into any of the 26 positions and is called the ring setting or Ringstellung. Changing the position of the ring will therefore change the position of the notch and alphabet, relative to the internal wiring.

As example, let us take rotor type I without any ringsetting offset. You can see that an 'A' is encoded as an 'E', a 'B' encoded as a K, and a 'K' is encoded as an 'N'. Notice that every letter is encoded into any another.

```
Input = ABCDEFGHIJKLMNOPQRSTUVWXYZ (rotor right side)
      | | | | | | | | | | | | | | | | | | | | | | | | | |
I      = EKMFLGDQVZNTOWYHXUSPAIBRCJ
```

When a rotor has stepped, you must take in account the offset to know what the output is, and where it enters the next rotor. If for example rotor I is in the B-position, an 'A' enters at the letter 'B' which is wired to the 'K'. Because of the offset this 'K' enters the next rotor in the 'J' position.

The ringsetting will rotate the wiring. Where rotor I in the A-position normally encodes an 'A' into an 'E', with a ringsetting offset B (02) it will be encoded into 'K'

The Reflector or Umkehrwalze

The reflector, Umkehrwalze or UKW in German, is a unique feature of the Enigma machine. On the internal wiring of all movable rotors, each letter can be wired with any other letter. An 'A' could be wired to 'F', where the 'F' is wired to 'K'. In the reflector, the connections are made in pairs. In the case of the wide B reflector, the 'A' is wired to the 'Y' which means that the 'Y' is also wired to the 'A', resulting in a reciprocal encryption. The advantage for the operator is clear. Encryption and decryption is possible with the same machine setting and wiring. Unfortunately, a letter can never be encrypted into itself, and this feature opened the door to cryptanalysis, making the job easier to the codebreakers.

```
Contacts      = ABCDEFGHIJKLMNOPQRSTUVWXYZ
              | | | | | | | | | | | | | | | | | | | | | | | | | |
Reflector B   = YRUHQSLDPXNGOKMIEBFZCWVJAT
```


The rotor advance mechanism

If we talk about rotor positions, the following notation is commonly used: V, I, III means that the left rotor is type V, the middle type I, and the right is a type III. The rotors appear to work as a normal odometer, but there are some important differences, due to the system of pawls and levers. If the turnover point of rotor type I is Q, this means that the next left rotor will advance one step when the right rotor steps from Q to R. For the first five rotors, you can use the mnemonic "Royal Flags Wave Kings Above", or RFWKA for the letters that are visible after the turnover. In addition, and this is important, the middle rotor will advance on the next step of the first rotor a second time in a row, if the middle rotor is in its own turnover position. This is called the double-step. This results in a sequence as in this example:

KDP, KDQ, KER, LFS (Rotors III,II,I are used in this example)

As you can observe, stepping from Q to R advances the middle rotor, and on the next step it steps again, advancing the third rotor also. The reason for this strange behavior is rather simple.

There are three levers that are all engaged when each letter is pressed. Each lever is half positioned on the index ring (the one that has a notch) of the rotor on its right, and half positioned above the 26 ratchets of the rotor on its left (viewed from the point of the operator). Since the right lever is not above an index ring it will always engage the right rotor.

Once the right rotor has stepped and the middle (spring-loaded) lever can drop down in the right rotor's notch, it will engage the middle rotor's ratchet, advancing the middle rotor one step. The same event will take place when the middle rotor's notch enables the left lever to engage the ratchets of the left (third) rotor.

However, an important event will now take place. A rotor will not only advance if its ratchets are engaged, but also when a lever pushes into its notch. We now have a complete sequence of a middle rotor double-step: The right rotor steps, and takes the middle rotor one step further. If the middle rotor has moved by this step into its own notch-position, on the next step the right lever pushes the ratchet of the right rotor, and it will also push the middle rotor one step further, advancing it a second time in a row. Note that rotors VI, VII & VIII have two notches which means that the rotors to their left will advance twice as fast as with normal one-notch rotors.

The stepping mechanism, as explained above, is used on the Wehrmacht and Kriegsmarine Enigma. The four-rotor Kriegsmarine M4 is derived from the three rotor version without changing the rotor advance mechanism or adding a fourth pawl. Therefore the fourth rotor doesn't move and can only be adjusted manually. The Enigma-G, used by the Abwehr (German Intelligence) has a different mechanism. The Enigma-G has a rotating reflector and three rotors with multiple notches, rotated by a gear box.

The cryptographic strength

The combination of rotor types and order, the ring settings, plugs and start position are what makes Enigma so complicated and provides a stunning 1×10^{23} possible combinations, that's about one hundred thousand billion billion.

About other Enigma models

There are several other Enigma models, civilian as well as military, that were manufactured. German security forces used a variant with rotors containing letters and figures and other versions were produced without plugs, with an exterior alphabet-lightbox, different rotors and different wirings, etc.

The wirings as described here, are for the rotors for Wehrmacht, Luftwaffe and Kriegsmarine Enigma's only. The rotors for other versions of the Enigma machine had other internal wirings.

History of the Enigma Cipher Machine

The story of the famous Enigma cipher machine combines ingenious technology, military history and the mysterious world of espionage, codebreakers and intelligence into a real thriller. Never before has the fate of so many lives been so influenced by one cryptographic machine, as in the Second World War. Enigma is the most famous and appealing example of the battle between codemakers and codebreakers. Enigma showed the importance of cryptography to military and civil intelligence.

Origins of the Enigma

With the rise in the early 1900's of wireless communication the need for secure communications for both military as civilian use became essential. The search to replace the impractical and time-consuming hand ciphers began. In 1917, the American Edward Hugh Hebern developed a cipher machine with rotating disks, each disk performing a substitution cipher. Hebern's idea was the base for many similar machines, developed in several other countries.



In 1918, Engineer Arthur Scherbius patented a cipher machine using rotors. The German Navy and Foreign Offices were approached, but were not interested. In 1923, the rights for the patents went to Chiffriermaschinen-AG, a firm with Scherbius on the board of directors, that commercialized the machine. In 1927, Scherbius bought the 1919 patent from of a similar machine from the Dutchman Koch, in order to secure his own patent, approved in 1925.

The first cipher machine, Enigma A, came onto the market in 1923. It was a large and heavy machine with an integrated typewriter and weighed about 50 Kg. Soon after the Enigma B was introduced, a very similar machine. The weight and size of these machines made them unattractive for military use. The development of the reflector, an idea of Scherbius' colleague Willi Korn, made it possible to design the compact and much lighter Enigma C. Also, the type writer part was replaced by a lamp panel. In 1927, the Enigma D was introduced and commercialized in different versions, and sold across Europe to military and diplomatic services.

The Swiss army used the Enigma K. The Italian Navy bought the commercial Enigma D, as did Spain during the Spanish Civil War. Several intelligence services succeeded in breaking some civil and military versions. The British codebreakers for example cracked the Spanish Enigma that was operated without a plugboard. Japan used the Enigma T, also called Tirpiz Enigma, an adapted version of the Enigma K. Japan also developed their own version, with horizontally placed rotors. The messages of both models T and K were broken as well.

Military versions

In 1926, the commercial Enigma was purchased by the German Navy and adapted for military use. They called it Funkschlüssel C. In 1928, the German Abwehr (Secret Service), Wehrmacht and Luftwaffe bought their own version, the 12 Kg light Enigma G, also called Zählwerk Enigma due to it's counter on the front panel. This model had a gear box to advance the rotors, a rotating reflector, but no plugboard. The Wehrmacht revised this machine, adding the plugboard and a different rotor advancing mechanism. This version, the Enigma I, became known as the Wehrmacht Enigma and was introduced on a large scale to the German Army and public authorities. The Luftwaffe followed the Wehrmacht's lead in 1935. The Wehrmacht Enigma came initially with three rotors. From 1939 on they were equipped with five rotors.

In 1934, the German Navy adopted the Wehrmacht model, with it's securer plugboard, and extended the set of rotors to eight. The Navy machine was called Funkschlüssel M or M3. In 1941, although reassured by the Abwehr that the Enigma M3 was unbreakable, Admiral Karl Dönitz insisted on improvement of the Kriegsmarine Enigma. Early in 1942, the famous four rotor M4 model was introduced in the Kriegsmarine. An estimated total of 100,000 machines were produced.

Breaking the code

In 1932 Poland's Biuro Szyfrow (Cipher Bureau) initiated attempts to analyse and break the Enigma messages. Although the chief of this Bureau received copies of codebooks sold by the German spy Hans-Thilo Schmidt, he did not give them to his codebreakers. He thought that keeping this information from them might stimulate their efforts. Marian Rejewski, Henryk Zygalski and Jerzy Rozicki succeeded in breaking the Enigma codes and developed an electro-mechanical machine called the Bomba, to speed up the codebreaking process. Two major security flaws in the German Enigma procedures were the global groundsetting and the twice encodes message-key, a procedure to exclude errors. These flaws opened the door to cryptanalysis. In 1939 the Bureau was no longer able to break the codes due to increased sophistication in the design, new procedures and lack of funds for the code breakers. When Germany invaded Poland, the Polish knowledge and several replica Enigma machines were passed to French and British intelligence.

Bletchley Park

The Government Code and Cipher School at Bletchley Park initially broke Enigma by hand. In August 1940 they started using their own Bombes, designed by Alan Turing and Gordon Welchman. It was also a rotary electro-mechanical device but it worked on an entirely different principle as Jerewski's Bomba. The Turing Bombe searched for the enigma settings for a given piece of plain and cipher text. When an Enigma message was intercepted, codebreakers had to search for cribs. These cribs were presumed pieces of plain text within the encrypted message. This could be "An den Oberbefehlshaber", "An Gruppe", "Es lebe der Fuhrer" or any other standardized piece of text. Once a crib was located (there were some techniques for that) the associations between the letters of the ciphertext and their plain version were entered in the Bombe. The Bombe, which contains a large number of drums, each replicating the rotors of the Enigma, ran through all possible settings to find the key settings that belong to the given pieces of cipher and plain text. Once these settings were found all messages, encrypted with these setting, could be deciphered.

All information retrieved by cryptanalysis, the breaking of codes, had the codename "Ultra" and played a very important and often decisive role during the war, mainly in the Battle of the Atlantic. All Ultra information was used very carefully, so as to avoid suspicion among the German forces. Special liaison officers, trained to deal with this valuable but delicate knowledge, were placed in Headquarters and other strategic places. Moreover, Ultra was never used unless it could be confirmed by a second source in order to avoid giving the German Command reason to suspect that their communications security might be broken.

The Kriegsmarine

The German Kriegsmarine was very successful in applying their Rudeltaktik or "Wolfpack Tactics" with U-boats. They hunted individually for convoys. If a convoy was spotted, they shadowed it and called other U-boats into battle. Once all U-boats were on the spot, they sank the convoy with a closely co-ordinated attack. This technique was so devastating to the allied supplies that it almost decided the outcome of the war. Communication was the keyword and the U-boats used Enigma to send messages to co-ordinate their attacks. After some initial hard times, Bletchley Park broke the naval codes almost continuously. Decreasing effectiveness of his U-boats made Admiral Donitz suspicious and, although reassured by German intelligence that Enigma was secure, he insisted on improving the Enigma's security. Early in 1942 the famous 4-wheel machine was introduced in the Kriegsmarine and the complicated 'Shark' codes caused a big crisis at Bletchley Park. The Kriegsmarine referred to the spring of 1942 as the "Happy Times" because the Allied forces were unable to decipher the codes and the U-boats were able to continue sinking ships without much interference.

Turning the tide

The codebreakers in Bletchley Park discovered by cryptanalysis that a fourth rotor had entered the battlefield of codes. After ten nerve wrecking months of heavy losses, Bletchley Park succeeded in breaking into Shark. This was due to several different reasons. An important factor were the Wetter-Kurzschlüssel code books, retrieved during attacks on weatherships and U-boats such as the famous attack on the U-559 of Kapitänleutnant Hans Heidtmann by the British HMS Petard. After taking heavy fire from HMS Petard, the sinking U-boat was boarded by three British sailors. They managed to get the Enigma and Kurzsignale codebooks. Two of them returned once more, trying to find the four-rotor Enigma, but went down with the U-boat. This mission proved to be a turning point in breaking Shark.

Sometimes, due to lack of cribs, Bletchley Park used a technique called Gardening. British bombers dropped or planted series of sea mines on well determined places. German U-boats, spotting these mines, transmitted contact messages, thereby providing new cribs to the codebreakers. Also, within the U-boat radio network, weather messages, encoded with the Wetter-Kurzschlüssel, were sent with the four-rotor Enigma in the less complicated M3 mode. This was done to be compatible with the three-rotor Enigma M3, used on weatherships. The Bombes in Bletchley Park, developed to crack the three-rotor Enigma, took more than 20 days to crack the four-rotor Enigma key settings. A three-rotor keysetting could be retrieved in less than 24 hours. Meanwhile, new Bombes were developed to deal with the four-rotor Enigma. By June 1943, the first four-rotor Bombes came into action, and by the end of 1943, another fifty four-rotor Bombes went operational at the American Navy. In the fall of 1943, Shark messages were generally broken within 24 hours.

The tide of the U-boat war had turned. Except for some brief periods, the entire German communication system was intercepted by a large number of listening stations called Y-stations, and the codes were broken in Bletchley Park, where over 7000 workers were employed at its peak. With the positions of the U-boats known, Allied ships could now avoid the enemy and an active hunt for U-boats was started. The elite weapon of the Kriegsmarine got decimated, resulting in heavy losses among the U-boat crews. An estimated 700 U-boats and 30,000 crewman were lost at sea. The German command related these losses to new detection techniques like the ASDIC sonar system, U-boat detection planes, and destroyers, escorting convoys. They did not suspect cryptanalysis of the Enigma.

The Ultra information was kept highly secret during the entire war and played a decisive role, not only in the Atlantic. Breaking the Wehrmacht and Luftwaffe messages also proved to be crucial. The codebreakers exposed the weakness of Field Marshal Rommel's notorious Afrika Korps. The speed and successes of the Afrika Korps created long stretches of poorly defended supply lines. Ultra information provided Field Marshal Montgomery with a vital tactical advantage. In the days before the D-day invasion of Normandie, the Wehrmacht, without realizing it, provided Allied Forces with an enormous quantity of detailed information on the coastal defense, location and strength of all German tank divisions and the movement of troops in France. Experts estimate that breaking Enigma shortened the war by about three years. The number of saved lives cannot be counted. Germany kept on using Enigma during the entire war, without any suspicion.

The heritage of Enigma

After the Second World War, Enigma was the basis for more sophisticated mechanical cipher machines like the Swiss NEMA and the Russian M-125 Fialka. Although Enigma was very well designed and offered, for those days, an unbreakable security, the negligent use in the German Armed Forces and the compromised codebook material enabled the codebreakers to turn the best kept secret of the war into a Trojan horse and give the kick-off for cryptographic intelligence. Today, Signal Intelligence is considered to be a most vital part of the modern battle.

Interesting websites about the Enigma cipher machine

Cipher Machines & Cryptology, the Enigma Sim home page

<http://users.telenet.be/d.rijmenants>

Tom Perera's Enigma Museum:

<http://w1tp.com/enigma>

Frode's Crypto Cellar at CERN:

<http://frode.home.cern.ch/frode/crypto>

David Hamer's cryptology website:

<http://home.comcast.net/~dhhamer>

Bletchley Park official site:

<http://www.bletchleypark.org.uk>

Enigma pages by Tony Sale:

<http://www.codesandciphers.org.uk/enigma>

The use of the naval 'Shark' code on U-boats and how it was broken

<http://www.uboat.net/technical/enigma.htm>

Breaking an original message, the double message key and Kenngruppen

<http://home.earthlink.net/~nbrass1/1enigma.htm>

History of solving the Enigma Cipher:

<http://www.enigmahistory.org/enigma.html>