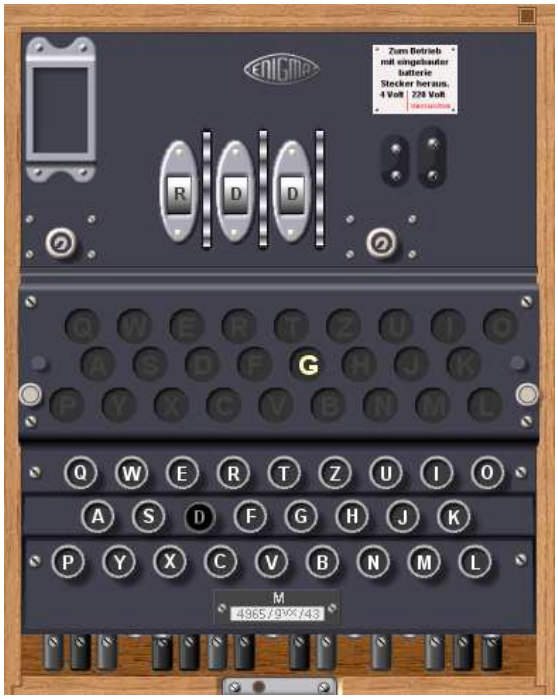
ENIGMA CIPHER MACHINE SIMULATOR 7.0.5

About the Enigma Simulator



The German Enigma machine is the most famous example of the battle between codemakers and codebreakers. Never before has the fate of so many lives been so influenced by one cryptographic machine, as the Enigma did in the Second World War. The story of Enigma combines technology, military history, espionage, codebreaking and intelligence into a real thriller.

This software is an exact simulation of the 3-rotor Heer (Army) and Luftwaffe (Airforce) Wehrmacht Enigma I, the Kriegsmarine (wartime Navy) Enigma M3 and the famous 4-rotor Enigma M4, as they were used during World War II from 1939 until 1945. The internal wiring of all rotors is identical to those used by the Heer, 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.

You can use the Enigma simulator in exactly the same way as a German signal trooper would have done during WW2. The hands-on approach and realistic graphics ensure an authentic feeling. You can open the machine, change the internal settings, select rotors from the spare box, preset their ring settings, insert them into the machine and set the plugboard. The sounds are recorded from an actual Enigma machine.

This manual explains how to use the Enigma simulator, the message procedures as used by the German Armed Forces, including some authentic message examples, a complete technical description and a brief history of the Enigma. More information on the Enigma machine is found at the Cipher Machines & Cryptology website: http://users.telenet.be/d.rijmenants

Content

1. **The Enigma Key Settings**
2. **Message Procedures**
3. **Technical details of the machine**
4. **History of the Enigma**
5. **Websites**
6. **Copyright information and Disclaimer**

Wehrmacht Enigma I

Kriegsmarine Enigma M3

Kriegsmarine Enigma M4

1. The Enigma Key Settings

To prepare the Enigma Simulator for use, we need to adjust the internal settings - the so-called key - as agreed between the sender and recipient. To set the key, we must select the proper reflector, the rotors and their order, adjust the ring setting of the rotors, insert plugs on the plugboard and set the machine in its start position.

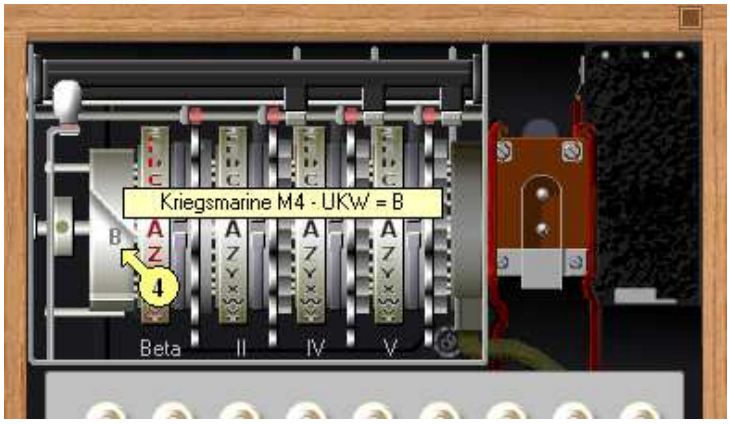
You will notice that the mouse pointer changes into a little hand when you move over places where you can select or click something. To call the Enigma simulator menu, move the mouse to the little icon in the top right corner of the machine [1].

Setting the rotors (Walzen)

Click the power switch [2] (Wehrmacht) or one of the locks [3] (Kriegsmarine M3/M4) to open the Enigma. The interior of the machine will become visible, showing the rotor cradle compartment at the top of the machine and a rotor box, containing the unused spare rotors, at the bottom.

Selecting the Reflector (Umkehrwalze or UKW)

You can choose between the different Enigma models by left-or right clicking the letter on the reflector [4].

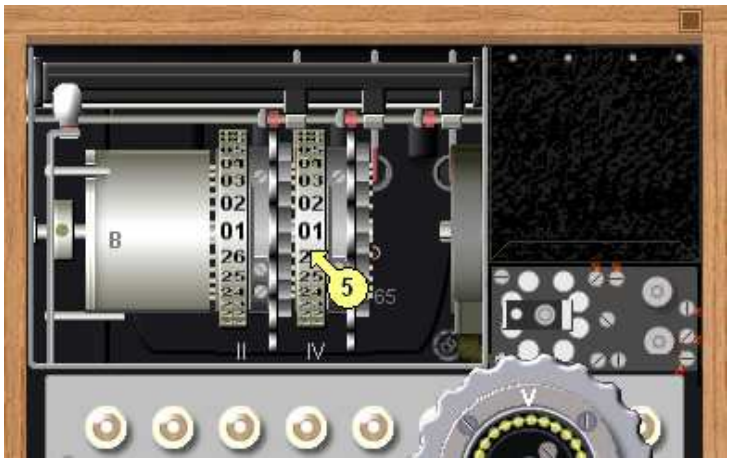


	Model	UKW	Rotors	Choice of rotors
1	Wehrmacht (Heer & Luftwaffe)	B	3	5 normal
2	Wehrmacht (Heer & Luftwaffe)	C	3	5 normal
3	Kriegsmarine M3	B	3	5 normal + 3 double notched
4	Kriegsmarine M3	C	3	5 normal + 3 double notched
5	Kriegsmarine M4	B	4	5 normal + 3 double notched + Beta + Gamma
6	Kriegsmarine M4	C	4	5 normal + 3 double notched + Beta + Gamma

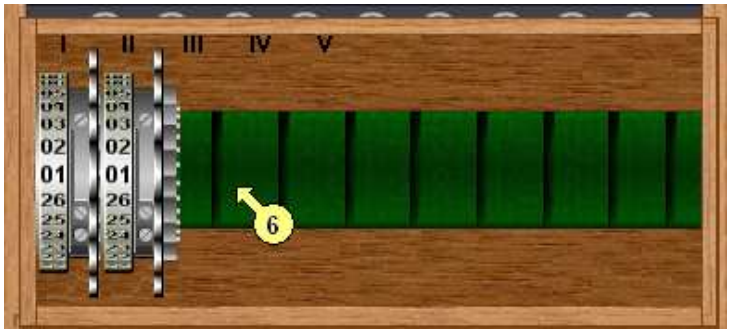
Note: the 4-rotor Kriegsmarine M4 with thin B reflector and Beta rotor with its ring and rotor in A position is compatible with both the 3-rotor Kriegsmarine M3 and Wehrmacht Enigma with wide B reflector. Of course, this is only true when the 3 normal rotors, their order, rings setting and the plugboard are identical.

Changing the Rotors (Walzen)

To change one or more rotors, click on a rotor [5] in the rotor cradle to lift it out of the Enigma machine. The rotor will be placed on top of the machine. Below a Werhmacht model with one extracted rotor.



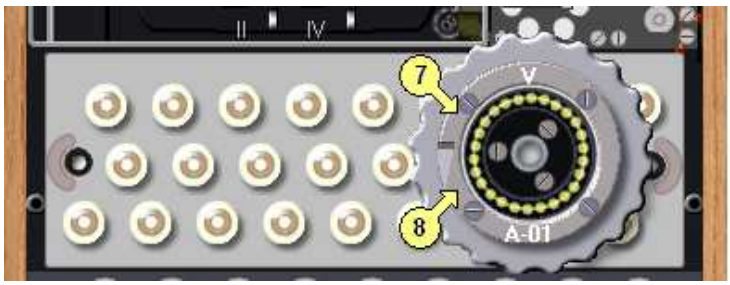
Click on an empty place [6] in the box with spare rotors, at the bottom of the machine, to put the extracted rotor in the spare rotors box.

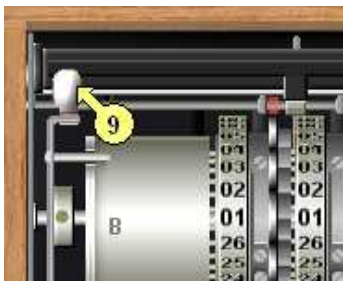


To insert another rotor in the rotor cradle, select the desired rotor from the rotor box (it will be placed on top of the machine) and click on an empty place in the rotor cradle.

Adjusting the Ring Setting (Ringstellung)

You can adjust the ring setting (Ringstellung) of a rotor when it is extracted from the machine. Once it is placed on top of the machine, you can adjust the ring setting by clicking the upper [7] or lower [8] half of the displayed rotor. When the ring is adjusted, click on an empty place at the desired location in the rotor cradle to place that rotor in the machine.





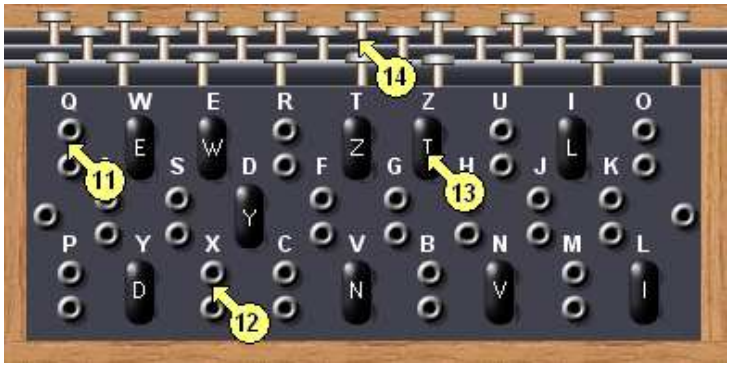
You might find it easier to lift out all rotors from the rotor cradle and put them all into the box with spare rotors first, and then select, adjust and insert them one by one in the machine.

Once all rotors are placed in the rotor cradle, you can close the lid by clicking the little handle [9] at the top left, above the reflector. It will be impossible to close the lid if not all required rotors are placed inside the machine. Once all settings are finished and the machine is closed, the proper machine (Enigma I, M3 or M4) will appear.

Connecting the Plugs (Stecker) on the Plugboard (Steckerbrett)

To connect plugs from one socket to another (to switch the letter connections) you must click in the area of the plugs [10], at the bottom of the Enigma.

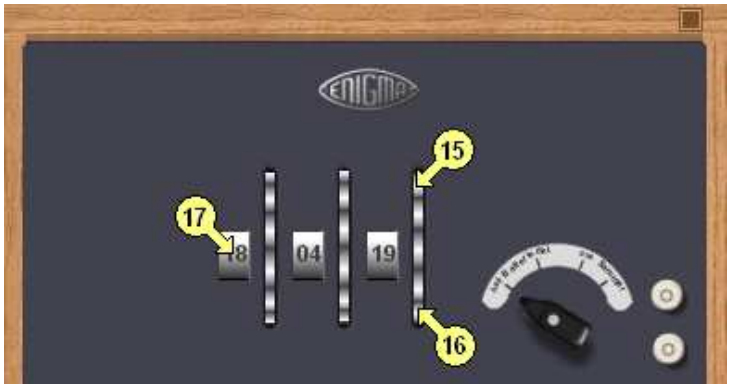
The plugboard or 'Steckerbrett' will appear. Simply click the desired socket [11] and then click the socket that you want to connect it to [12]. To clear a connection, just click one of the plugs [13] of a pair and both plugs will disappear. After finishing the plug settings you can return to the Enigma top view by clicking the keys [14] above the plugboard.



The Wehrmacht machine has a plugboard with QWERTZ layout, identical to its keyboard. The Kriegsmarine machine has a sequentially numbered layout. For ease of setting, you can change this layout by clicking one of the single test sockets on the left and right (QWERTZ to ABCDEF for Wehrmacht and 1 2 3 4 5 to ABCDEF for Kriegsmarine)

Setting the Rotor Start Position (Spruchschlussel)

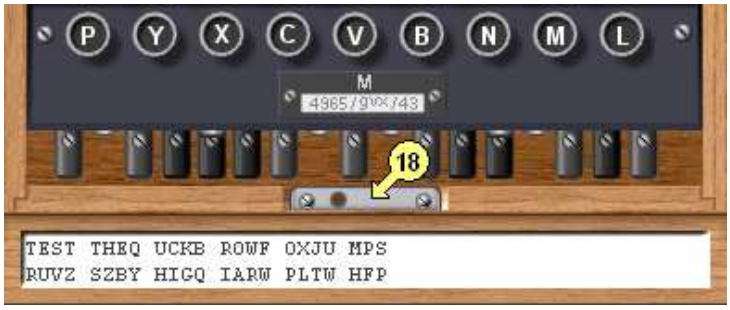
On the main screen you can change the start position of the rotors by clicking the upper [15] or lower [16] half of the rotor thumb wheels. You can save the start position temporarily by pressing the INS key, and retrieved these rotor positions later by pressing the HOME key.



The Wehrmacht Enigma has rotors with numbers. Therefore, to set a message key (see procedure later on), the simulator has a help sheet to convert letters to numbers. This sheet appears when you click on the number inside the little rotor window [17]. The real Enigma has this table fixed inside the wooden cover of the machine.

The Text Box

You can display the plaintext and ciphertext together in a little text box at the bottom of the Enigma by clicking the lock [18] on the wooden box. Use the DEL or Backspace keys to clear this text box. Click again on the lock to hide the text box. This text box is useful when processing large pieces of text.



The Auto Typing Function

If you have a large amount of plaintext or ciphertex that needs to be typed, you can use the Auto Typing function. This function is called from the Enigma menu. In the Auto Typing 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' when your text is ready for processing. Auto Typing is aborted by pressing the ESC key. Make sure that all setting are finished and the rotors are in the proper start position before starting the Auto Typing.

Note: Auto Typing will only process alphabet characters and ignore all other characters (figures, punctuations and spaces). When decrypting a message, make sure that there are no Kenngruppen included (see procedure later on) or delete the Kenngruppen from the text window.

The Smart Clipboard

You can call the Smart Clipboard from the Enigma menu or by clicking inside the text box at the bottom of the Enigma. You can select various ways to format and transfer text to the clipboard. When formatted for ciphertext, the output is arranged in groups of five letters for the Wehrmacht machine and groups of four letters for both Naval M3 and M4 machines.

Save and Load Machine Settings

Loading, saving, deleting and viewing the key settings is available from the simulator menu. The machine settings can be saved with the .eni extension. On start-up the simulator will be loaded with the last used settings. If no settings file was found on start-up, the default settings are loaded and a message is displayed.

Enabling or Disabling the Sounds

The sound effects can be disabled through the simulator menu. The sound is automatically muted when the "Very Fast option" is chosen during Auto Typing.

Exiting the Simulator

To exit the Enigma simulator, select Exit in the simulator menu. If the key settings are changed, you will be prompted to save the current rotor and plug settings (the rotor start positions are never saved)

Photo Gallery

Select the Gallery in the simulator menu to view a series of photos of Enigma machines.

Cryptanalysis and Test Mode

For cryptanalysis and testing purposes there are two special features:

You can hold down an Enigma letter key, by means of the PC keyboard, and at the same time move a rotor manually by clicking the rotor thumb wheel with your mouse. This way, for a given key, you can observe the ciphering output lamps change while turning the rotors by hand.

You can disable the rotor advance mechanism by using the F10 key. A warning will be displayed above the rotors. Use F10 again to restore the rotor advance mechanism.

2. Message Procedures

Wehrmacht Procedure

Each day, the Heer (Army) and Luftwaffe (Airforce) operators set up the machine according to the secret daily key sheet. This sheet contained the day (Tag), rotor selection and order (Walzenlage), ring setting (Ringstellung), plug connections (Steckerverbindungen) and identification groups (Kenngruppen). The days were printed in reversed order so that the operator could cut off each expired setting at the bottom.

```
-------------------------------------------------------------------------
Tag  Walzenlage  Ringstellung     Steckerverbindungen           Kenngruppen
-------------------------------------------------------------------------
31   I   II   V    06 22 14   PO ML IU KJ NH YT GB VF RE DC   EXS TGY IKJ LOP
30   III IV  II    17 04 26   BN VC XS WQ AZ GT YH JU IK PM   KIJ TFR BVC ZAE
29   V   I  III    15 02 09   ML KJ HG FD SQ TR EZ IU BV XC   QZE TRF IOU TGB
```

To identify the key, used for a particular message, the operator had to insert a five-letter identification group, usually as first group of the message. This so-called Buchstabenkenngruppe is composed of two randomly selected letters and one of the four possible three-letter Kenngruppen on the key sheet for that day. In our case, some examples of a correct Buchstabenkenngruppe for day 31 are TVEXS TGYZA or LOPXY. This five letter group, usually at the start of the message, had to be skipped during encryption and decryption.

If a message was divided into several parts, the operator had to insert a new Buchstabenkenngruppe for each part of the message. This key identification group was included in the letters count for the message header. By looking at this first group, the recipient immediately recognized which key was used for that particular message, which was important when messages arrived from previous days. To encrypt a message, the operator had to select a random start position for the rotors, the so-called message key, which had to be unique for each message. This procedure avoided excessive use of the same secret settings for a given day. Since the message key must be kept secret, they used the following procedure:

The operator selected a random basic position (Grundstellung) and a random message key (Spruchschlussel). In our example, the operator selects EHZ and XWB. He sets the rotors in the basic position EHZ and keys in the random message key XWB. The resulting TBS is the encrypted message key. Next, he encrypts the message with the random message key XWB as start position of the rotors. Finally, he sends the start position EHZ and encrypted message key TBS along with the encrypted message to the recipient.

On day 31 the following message is transmitted, from C to U6Z, sent at 1500 hrs and containing 49 letters.

```
U6Z DE C 1510 = 49 = EHZ TBS =

TVEXS QBLTW LDAHH YEOEF
PTWYB LENDP MKOXL DFAMU
DWIJD XRJZ=
```

To decrypt the message we proceed as follows:

- Select the Wehrmacht Enigma I with B reflector.
- Select the rotors, adjust their ring setting and set the plugs according to key sheet day 31
- Set the rotor start positions to EHZ, the first trigram of the message
- Type in the second trigram TBS to retrieve the original message key. The result should be XWB
- Set the decrypted message key XWB as start position for the three rotors.
- Now decrypt the actual message, but make sure to skip the key identification group TVEXS.

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

Note: in the pre-war Wehrmacht procedure, each message key was encrypted twice (to exclude errors) by a fixed secret basic position, valid for the whole day. For instance, with basic setting ABC, the message key XYZ was keyed in twice, resulting in JKL MNO. Only the double encrypted message key JKL MNO was sent along with the message. However, this created a mathematical relation between J and M, K and N, and L and O, a flaw that was exploited by the Polish codebreakers. German cryptologists understood this flaw and dropped the double encrypted message key in 1939, replacing it with a random basic position, sent along with a once encrypted message key.

Kriegsmarine Procedure

The Kriegsmarine (German Wartime Navy) procedures on sending messages with the Enigma cipher machine were far more complex and elaborate than the Heer and Luftwaffe procedures. The Kriegsmarine Enigma key sheets consisted of two parts.

- Schlusseltafel M Algemein - Innere Einstellung (internal settings), contained the three rotors and their ring settings, the thin beta or gamma rotor and the reflector, and this only for the odd days of a month.
- Schlusseltafel M Algemein - Aussere Einstellung (external settings), contained the plugs and Grundstellung (basic start position) for each day of the month.

An additional key existed for the officers and a special Schlussel M NIXE was used for private communication between the captain and U-boat Command, without other U-boats being able to read the message.

The Kriegsmarine system of Kenngruppen was completely different to the Heer and Luftwaffe Kenngruppen system. In addition to the key sheets, the Kriegsmarine used a Kenngruppenbuch on their main cipher nets to determine the message key. The Kenngruppenbuch contained the following parts:

- Zuteilungsliste (an allotment list) that told the operator which table (Spalte) he should use for a particular cipher net. This list consisted of two parts. The first part showed the Spalte number, given the name of the cipher nets, and the second part showed the different cipher nets, given the Spalte number.
- Tauschtafelplan (table pointer) told the operator which column of a given Spalte was used to select the required trigrams.
- Kenngruppen (identification groups), the tables (Spalte) with Kenngruppen.

The operator had to select two three-letter kenngruppen or trigrams from the Kenngruppenbuch:

- Schlüsselkenngruppe (key indicator group) to identify which key was used
- Verfahrenkenngruppe (encryption indicator group) to obtain the message key

Both Schlüsselkenngruppe and Verfahrenkenngruppe had their own tables as determined in the Zuteilungsliste.

With the Enigma in the Grundstellung (the basic position for that day) the operator typed in the Verfahrenkenngruppe. The result would be the message key, used as start position to encipher the message. The two trigrams together (Schlüsselkenngruppe and Verfahrenkenngruppe) were the message indicator.

This message indicator underwent an additional substitution encryption with a bigram table called Doppelbuchstabentauschtafel (double-letter conversion table). A set of bigram tables consisted of nine different tables. A calendar determined which of the substitution tables was used on a particular day. The bigram table was reciprocal, meaning that if a bigram AB was encoded in KW, the bigram KW would also decode to AB.

The operator wrote the two trigrams from the message indicator underneath each other, but added one random dummy letter at the beginning of the first trigram and one dummy letter at the end of the second trigram. To encode, the bigrams were taken vertically from the message indicator and encoded according to the bigram table. The resulting two four-letter groups (the encoded message indicator) were added at the start of the message and were repeated at the end.

The Kriegsmarine Enigma messages were formatted in four-letter groups. Some messages were encoded with the Kurzsignalheft code book or the Wetterkurzschlussel, prior to encryption with the Enigma. The Kurzsignalheft (short-signal book) converted words, numbers and all kinds of operational and technical expressions and phrases into four-letter codes. The Wetterkurzschlussel (weather-short signal key) converted a complete weather report into a 23 or 24 letters code.

Formatting Rules and Commonly used Abbreviations

The Heer and Luftwaffe transmitted their messages always in five-letter group. To make cryptanalysis harder, it was forbidden to use more than 250 characters in a single message. Longer messages were divided into several parts, each part using its own message key.

The Enigma machine could process letters only. Therefore, numbers were written out and punctuations were replaced by rare letter combinations.

The Wehrmacht used the following abbreviations:

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

Question mark (Fragezeichen in German) was usually abbreviated to FRAGE, FRAGEZ or FRAQ.

Foreign names, places, etc. are delimited twice by "X" as in XPARISXPARISX or XFEUERSTEINX

The letters CH were written as Q. ACHT became AQT, RICHTUNG became RIQTUNG

Numbers were written out as NULL EINZ ZWO DREI VIER FUNF SEQS SIEBEN AQT NEUN

It was prohibited to encipher the word "NULL" several times in succession, so they used CENTA (00), MILLE (000) and MYRIA (0000). Some examples: 200 = ZWO CENTA, 00780 = CENTA SIEBEN AQT NULL.

To make cryptanalysis even harder, some complications were introduced in the Wehrmacht message procedures during the war. Since the third, left-most rotor, only advanced every 676 keystrokes, this rotor didn't have much effect during enciphering (such long messages were forbidden for security reasons). However, the operator could encipher a certain four letter code into the message, for instance CYOP, and change the left rotor position. When the receiving operator encountered these letters during deciphering, he also turned the left-most rotor to another position (in the case CYOP to position O).

Another complication, added at the end of the war, was placing the rotors 'with rotation'. Every 8 hours, a given rotor placing was rotated clockwise. If the rotors for that day were 241, this changed during the day to 124 and 412. The ring setting for the individual rotors did not change, and moved along with the rotors.

The Kriegsmarine formatted their messages in four-letter groups. They used the following abbreviations:

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

On the following pages, you will find two authentic messages, one Wehrmacht and one Kriegsmarine message, to put your knowledge on Enigma procedures into practice.

Authentic Wartime Message from the Russian Front

The following authentic 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 wartime messages. The project is a joint effort by Frode Weierud and Geoff Sullivan, two members of the Crypto Simulation Group (CSG).

The message was sent by the commander of the SS-Totenkopf Division (SS-T), also known as 3 SS-Panzergrenadier-Division Totenkopf, a division of the Waffen-SS. The message was destined to the LVI (56) Armee Korps. In April 1941, SS-T was ordered east to join Heeresgruppe Nord, which formed the northern wing of operation Barbarossa, the campaign against Russia. SS-T saw action in Lithuania and Latvia, and breached the Stalin Line in July 1941. The message from July 7 contains a situation report on SS Panzer Regiment 3 and its 1st Battalion.

The settings as recovered by the CSG codebreakers:

Maschine:	Wehrmacht Enigma I
UKW:	B
Walzenlage:	2 4 5
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 decrypt the second trigram in order to retrieve the message key (start position for decrypting). RFUGZ and FNJAU are Kenngruppen to identify the key, and must be skipped while decrypting!

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 YLKLT TDEIS MDICA
GYKUA CTCDO MOHWX MUUIA
UBSTS LRNBZ SZWNR FXWFY
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 VRXCY YTNJR
```

Decrypting the message is your job. Good luck!

The next page contains a spoiler with the raw decrypt, the rearranged plaintext and the translation in English. Don’t read any further before you decrypted the message.

This is a spoiler!

The raw plaintext, without Kenngruppen:

```
PART 1

AUFKL XABTE ILUNG XVONX
KURTI NOWAX KURTI NOWAX
NORDW ESTLX SEBEZ XSEBE
ZXUAF FLIEG ERSTR ASZER
IQTUN GXDUB ROWKI XDUBR
OWKIX OPOTS CHKAX OPOTS
CHKAX UMXEI NSAQT DREIN
ULLXU HRANG ETRET ENXAN
GRIFF XINFX RGTX

PART 2

DREIG EHTLA NGSAM ABERS
IQERV ORWAE RTSXE INSSI
EBENN ULLSE QSXUH RXROE
MXEIN SXINF RGTXD REIXA
UFFLI EGERS TRASZ EMITA
NFANG XEINS SEQSX KMXKM
XOSTW XKAME NECXK
```

The plaintext, rearranged and with converted abbreviations:

```
AUFKL[AERUNG] X ABTEILUNG X VON X KURTINOWA X KURTINOWA X
NORDWESTL[ICH] X SEBEZ X SEBEZ X UAF FLIEGERSTRASZE
RIQTUNG X DUBROWKI X DUBROWKI X OPOTSCHKA X OPOTSCHKA X UM X
EINS AQT DREI NULL X UHR ANGETRETEN X ANGRIFF X INF X RGT X
DREI GEHT LANGSAM ABER SIQER VORWAERTS X EINS SIEBEN NULL
SEQS X UHR X ROEM[ISCHEN ZIFFER] X EINS X INF RGT X DREI X
AUF FLIEGERSTRASZE MIT ANFANG X EINS SEQS X KM X KM X
OSTW[EST] X KAMENEC X K
```

Translation into English:

```
RECONNAISSANCE UNIT FROM KURTINOWA NORTH-WEST OF SEBEZ ON THE
FLIGHT CORRIDOR IN DIRECTION DUBROWKI, OPOTSCHKA. STARTED TO
MOVE AT 18:30 HOUR. ATTACK INFANTRY REGIMENT 3 GOES SLOWLY BUT
SURELY FORWARDS. 17:06 HOUR, I (BATTALION) INFANTRY REGIMENT 3
ON THE FLIGHT CORRIDOR STARTING 16 KM EAST-WEST OF KAMENEC.
```


More examples of broken messages are found on Frode Weierud's Cryptocellar web pages:
http://cryptocellar.org

Authentic wartime U-Boat Message from the North Atlantic

The following message was intercepted by the British destroyer HMS Hurricane in the North Atlantic on November, 25, 1942. This was during the ten months black-out which occurred after the introduction of the notorious four-rotor Enigma. During that period, the codebreakers in Bletchley Park were unable to decrypt the Kriegsmarine radio traffic, encrypted with the Triton keys on the new Enigma M4. This message is one of three, believed to be unbroken until today, and published by Ralph Erskine in a letter to Cryptologia.

U-264 Insignia

With the contents of the message unveiled, we were able to find the story of the U-boat in the Archives. It is a story that brings the message and its reader closer than ever to the dramatic events of naval warfare during the Second World War. The message was written by Kapitänleutnant Hartwig Looks, commander of U-264, a type VIIC U-boat. Between November 1942 and February 1944, U-264 sailed out on six patrols. On its first patrol, U-264 sank the Greek 'Mount Taurus' in convoy ONS-144. On the third patrol, U-264 sank the British 'Harperley' and American 'West Maximus', both in convoy ONS-5. On February 5, 1944, U-264 left St-Nazaire for its seventh and fatal patrol. The message, presented here, was sent on their first patrol.

In 2006, Stefan Krah started the M4 Project, an effort by to break these three authentic messages, enciphered on four-rotor Enigma M4. Stefan has already succeeded in breaking 2 of the 3 messages, with the help of distributed computing (a large number of computers, working together in a network).

The settings as recovered by Stefan Krah:

Maschine:	Kriegsmarine M4
UKW:	B
Walzenlage:	Beta 2 4 1
Ringstellung:	A-A-A-V
Stecker:	AT BL DF GJ HM NW OP QY RZ VX
	(1/20, 2/12, 4/6, 7/10, 8/13, 14/23, 15/16, 17/25, 18/26, 22/24)
Start position:	V-J-N-A

Note: the M4 software returned the plug settings as letters. In reality, Kriegsmarine key sheets contained plug combinations with numbers (the M4 carried a sequentially numbered plugboard layout).

The message, as received by HMS Hurricane (a few small errors included, probably during reception):

```
     T.O.R.1152/19/221 (53 GROUPS).

FCLC QRKN NCZW VUSX PNYM INHZ XMQX SFWX WLKJ AHSH NMCO CCAK UQPM KCSM
HKSE INJU SBLK IOSX CKUB HMLL XCSJ USRR DVKO HULX WCCB GVLI YXEO AHXR
HKKF VDRE WEZL XOBA FGYU JQUK GRTV UKAM EURB VEKS UHHV OYHA BCJW MAKL
FKLM YFVN RIZR VVRT KOFD ANJM OLBG FFLE OPRG TFLV RHOW OPBE KVWM UQFM
PWPA RMFH AGKX IIBG FCLC QRKM VA
```

The first two and the last two groups (FCLC QRKN) are the message indicator and must be skipped during decryption. Set your Enigma to the provided settings, with rotor start position VJNA, and decrypt the message, starting from group NCZW.

The message indicator told the operator which settings he had to use for a particular message. This message indicator was composed with the complex Kriegsmarine Kenngruppen system and remains unknown. However, Krah's software provided the actual message settings without help of the message indicator details.

The next page again contains the spoiler. Don't read any further before you decrypted the message.

Thanks go to Stefan Krah for the permission to use this message as an example. More information on the M4 message breaking project and the original messages can be found on Stefan Krah's website:

http://www.bytereef.org/m4_project.html

This is a spoiler!

The raw plaintext, without kenngruppen.

```
VONV ONJL OOKS JHFF TTTE
INSE INSD REIZ WOYY QNNS
NEUN INHA LTXX BEIA NGRI
FFUN TERW ASSE RGED RUEC
KTYW ABOS XLET ZTER GEGN
ERST ANDN ULAC HTDR EINU
LUHR MARQ UANT ONJO TANE
UNAC HTSE YHSD REIY ZWOZ
WONU LGRA DYAC HTSM YSTO
SSEN ACHX EKNS VIER MBFA
ELLT YNNN NNNO OOVI ERYS
ICHT EINS NULL
```

The plaintext, rearranged and with converted abbreviations:

```
VON VON J LOOKS J HFFTTT [HF FUNKTELEGRAMM] EINS EINS DREI ZWO YY QNNS NEUN
INHALT XX BEI ANGRIFF UNTER WASSER GEDRUECKT Y WABOS [WASSERBOMBEN] X
LETZTER GEGNERSTAND[ORT] NUL ACHT DREI NUL UHR
MAR[INE]QU[ADRANT] ANTON JOTA NEUN ACHT SEYHS DREI Y ZWO ZWO NUL GRAD Y
ACHT S[EE]M[EILEN] Y STOSSE NACH X
EKNS VIER M[ILLI]B[BAR] FAELLT Y [WIND] NNN NNN OOO VIER Y SICHT EINS NULL
```

Translation into English:

```
FROM LOOKS: RADIO SIGNAL 1132/9
CONTENTS: FORCED TO SUBMERGE DURING ATTACK, DEPTH CHARGES.
LAST ENEMY LOCATION 08:30 HOUR NAVAL GRID AJ 9863, 220 DEGREES,
8 NAUTICAL MILES, [I am] FOLLOWING [THE ENEMY]. [BAROMETER] 1014 MILLIBAR
[TENDENCY] FALLING, [WIND] NORTH NORTH EAST 4, VISIBILITY 10
```

On February 19, 1944, in search of a convoy in the North Atlantic, U-264 was detected by destroyers, protecting convoy ON-224. HMS Woodpecker, HMS Starling, HMS Kite, HMS Wren and HMS Wild Goose tightened the rope around U-264 and dropped more than 250 depth charges near the U-boat, causing fatal damage. Out of control, U-264 sank to a depth of 230 meter and Kapitänleutnant Looks gave the order to blow the air tanks and surface.

As they surfaced, the five sloops encircled the U-boat and immediately opened fire. Looks ordered his crew to leave the boat. U-264 sank in the early evening of February 19, at position 48°31'N-22°05'W. Looks and all crew members, 52 men in total, were picked up by HMS Woodpecker. The crew of U-264 survived their incredible nightmare and spent the rest of the war as prisoners, unlike many other U-boats crews who where less fortunate.

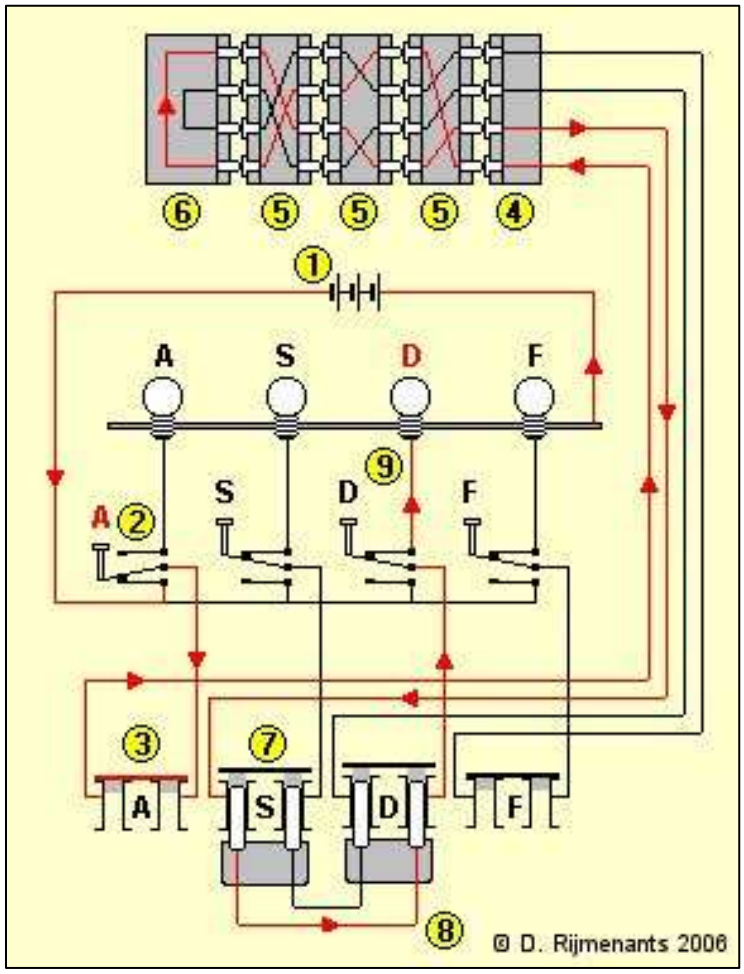
Note: the decrypted message was sent on the first patrol of U-264 and therefore is not related to the final days of Kapitänleutnant Hartwig Looks' U-boat.

A detailed account of the final hours of U-264 is found on the Enigma Simulator website:

http://users.telenet.be/d.rijmenants/en/m4project.htm

3. 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. One or more rotors move on each key stroke. The rotors and plugboard translate the depressed key into a burning lamp, representing the encrypted letter. The machine has a compartment for a 4 volt battery. Some versions have a switch to select between internal battery and external power supply. Other versions have an transformer to connect the machine to the AC mains.



The picture on the left 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 plate [4]. Next, the current proceeds through the - unused, and therefore closed - socket [3] via the entry plate [4] through the cross-wirings of the three (Wehrmacht Enigma) or four (Kriegmarine M4) rotors [5] and enters the reflector [6]. The reflector returns the current, via a different path, back through the rotors [5] and entry plate [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 (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 rotatable round casing with the letters A through Z or the numbers 01 through 26, and a notch. The center of the rotor, which is fixed to the thumb wheel, contains 26 spring-loaded contacts on the right side, scramble wired to 26 flat contacts on the left side. Changing the alphabet ring with its notch, relative to the position of the internal wiring, is called the ring setting (Ringstellung). The wiring represents a substitution encryption and is different for each rotor. 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 (fixed to the ring) and on its right 26 teeth. 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 Kriegmarine extended this set of rotors with another three rotors called VI, VII and VIII, each 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 were 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, making them incompatible with the other eight rotors.

Rotor Wiring Table

The internal wiring of the rotors performs the actual encryption. In the table below, the letter-columns for each rotor represent the 26 left side contacts and 26 right side pins. The signal first travels from right to left through the rotors towards the reflector and then returns from left to right through the rotors. If we look at rotor type I, we see that, from right to left, 'A' is encrypted into 'E', 'B' into “K”, and 'C' into 'M'.

Rotor wiring Enigma I – M3 – M4									
I	**II**	**III**	**IV**	**V**	**VI**	**VII**	**VIII**	**Beta**	**Gamma**
E-A	A-A	B-A	E-A	V-A	J-A	N-A	F-A	L-A	F-A
K-B	J-B	D-B	S-B	Z-B	P-B	Z-B	K-B	E-B	S-B
M-C	D-C	F-C	O-C	B-C	G-C	J-C	Q-C	Y-C	O-C
F-D	K-D	H-D	V-D	R-D	V-D	H-D	H-D	J-D	K-D
L-E	S-E	J-E	P-E	G-E	O-E	G-E	T-E	V-E	A-E
G-F	I-F	L-F	Z-F	I-F	U-F	R-F	L-F	C-F	N-F
D-G	R-G	C-G	J-G	T-G	M-G	C-G	X-G	N-G	U-G
Q-H	U-H	P-H	A-H	Y-H	F-H	X-H	O-H	I-H	E-H
V-I	X-I	R-I	Y-I	U-I	Y-I	M-I	C-I	X-I	R-I
Z-J	B-J	T-J	Q-J	P-J	Q-J	Y-J	B-J	W-J	H-J
N-K	L-K	X-K	U-K	S-K	B-K	S-K	J-K	P-K	M-K
T-L	H-L	V-L	I-L	D-L	E-L	W-L	S-L	B-L	B-L
O-M	W-M	Z-M	R-M	N-M	N-M	B-M	P-M	Q-M	T-M
W-N	T-N	N-N	H-N	H-N	H-N	O-N	D-N	M-N	I-N
Y-O	M-O	Y-O	X-O	L-O	Z-O	U-O	Z-O	D-O	Y-O
H-P	C-P	E-P	L-P	X-P	R-P	F-P	R-P	R-P	C-P
X-Q	Q-Q	I-Q	N-Q	A-Q	D-Q	A-Q	A-Q	T-Q	W-Q
U-R	G-R	W-R	F-R	W-R	K-R	I-R	M-R	A-R	L-R
S-S	Z-S	G-S	T-S	M-S	A-S	V-S	E-S	K-S	Q-S
P-T	N-T	A-T	G-T	J-T	S-T	L-T	W-T	Z-T	P-T
A-U	P-U	K-U	K-U	Q-U	X-U	P-U	N-U	G-U	Z-U
I-V	Y-V	M-V	D-V	O-V	L-V	E-V	I-V	F-V	X-V
B-W	F-W	U-W	C-W	F-W	I-W	K-W	U-W	U-W	V-W
R-X	V-X	S-X	M-X	E-X	C-X	Q-X	Y-X	H-X	G-X
C-Y	O-Y	Q-Y	W-Y	C-Y	T-Y	D-Y	G-Y	O-Y	J-Y
J-Z	E-Z	O-Z	B-Z	K-Z	W-Z	T-Z	V-Z	S-Z	D-Z

Important note:

The letters in the table are absolutely not related to the actual signal path of letters in the machine. The signal, coming from the entry plate ‘A’ contact, can enter the right side rotor at any of its 26 right side pins, depending on that rotor’s current position and ring setting (see next section).

Reflector (Umkehrwalze) Wiring Table

Reflectors			
B	**C**	**B thin**	**C thin**
Y-A	F-A	E-A	R-A
R-B	V-B	N-B	D-B
U-C	P-C	K-C	O-C
H-D	J-D	Q-D	B-D
Q-E	I-E	A-E	J-E
S-F	A-F	U-F	N-F
L-G	O-G	Y-G	T-G
D-H	Y-H	W-H	K-H
P-I	E-I	J-I	V-I
X-J	D-J	I-J	E-J
N-K	R-K	C-K	H-K
G-L	Z-L	O-L	M-L
O-M	X-M	P-M	L-M
K-N	W-N	B-N	F-N
M-O	G-O	L-O	C-O
I-P	C-P	M-P	W-P
E-Q	T-Q	D-Q	Z-Q
B-R	K-R	X-R	A-R
F-S	U-S	Z-S	X-S
Z-T	Q-T	V-T	G-T
C-U	S-U	F-U	Y-U
W-V	B-V	T-V	I-V
V-W	N-W	H-W	P-W
J-X	M-X	R-X	S-X
A-Y	H-Y	G-Y	U-Y
T-Z	L-Z	S-Z	Q-Z

The reflector (Umkehrwalze or UKW in German) is a unique feature of the Enigma machine. The reflector has 26 pins on the right side only and the wiring is made in loop pairs (see [6] on circuit diagram previous page).

In the table, the right side letters represent the pins on the right side of the refelctor, and the left side letters represent the pin to which it is wired.

In the case of the wide B reflector, the right side 'A' contact is wired to the 'Y' and ‘Y’ is wired to ‘A’, performing a loop. Physically, both ‘A’ and ‘Y’ pin are on the right side of the reflector. The result is a reciprocal encryption.

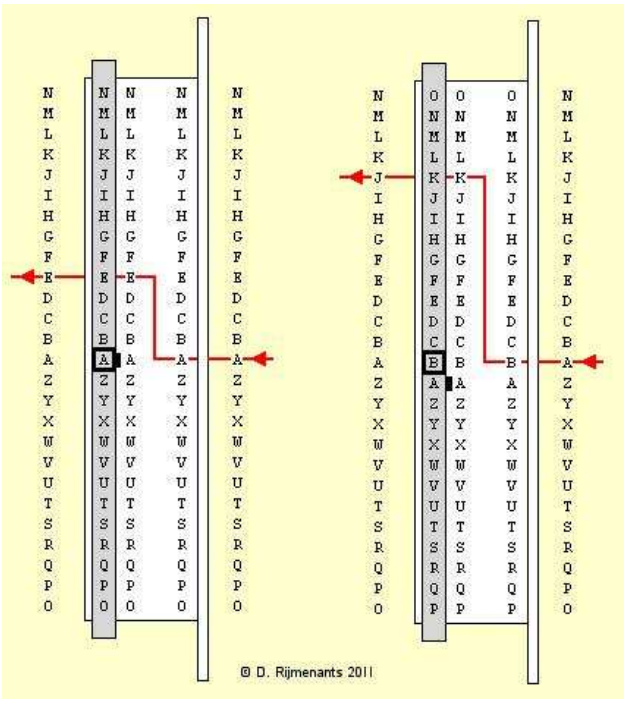
The advantage of such reciprocal design is that encryption and decryption are performed with the same electromechanical process and settings. Unfortunately, a letter can never be encrypted into itself, a property that opened the door to cryptanalysis, making the job easier to the codebreakers.

The Ring Setting (Ringstellung)

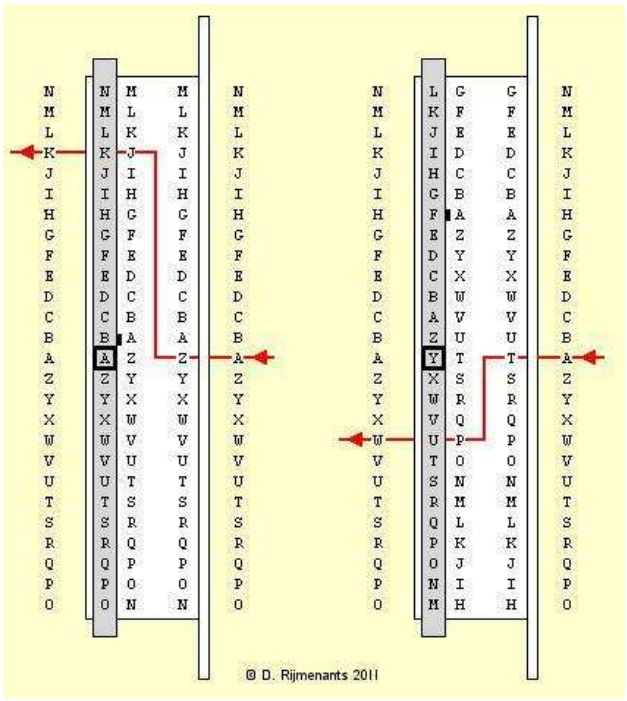
On the outside of the wiring core there's a movable ring with 26 numbers or letters and a notch. This ring is rotatable and is locked with a spring-loaded pin (Wehrmacht) or two spring-loaded arcs (Kriegmarine) into any of the 26 positions. The position of the ring is called the ring setting (Ringstellung).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

Example 1 shows how rotor I, with ring setting A-01, encrypted two consecutive depressed 'A' keys. On the left you see rotor I in the 'A' position (visible in the little window). The signal, coming from the depressed 'A' key, arrives at the 'A' position, enters at the 'A' contact and exits at the 'E' contact on the 'E' position (see wiring table for type I rotor above)

Next to it, we see that the rotor has stepped to the 'B' position. The signal again arrives at the 'A' position, but enters now at the 'B' contact and exits at the 'K' contact. Since the complete rotor has stepped one position, the K contact is now in the 'J' position and the signal therefore exits at the 'J' position towards the next rotor.



Example 1 - Rotor I with ring setting A



Example 2 - Rotor I with ring setting B and ring setting F

Example 2 explains the ring setting. On the left, rotor I has a ring setting B-02 (pin or dot at B) and the rotor is in the 'A' position ('A' visible in little window). The signal arrives at the 'A' position, enters at the 'Z' contact and exits at the 'J' contact. Due to the ring setting, the wiring core is shifted one position and so do the exit contacts. Therefore, exit contact 'J' is now in the 'K' position and the signal exits at the 'K' position towards the next rotor.

Next to it, we have another example with the same rotor I with, setting F-06 and the rotor in the 'Y' position. The signal arrives at the 'A' position, enters at the 'T' contact and exits at the 'P' contact. However, the combination of the rotor position and its ring settings causes a shift of seven positions of the exit contacts. With exit contact 'P' in the 'W' position; the signal exits the rotor at the 'W' position towards the next rotor.

The flow of the signal, described above, is from right to left: the signal, coming from the plugboard arrives at the rotor entry plate (located on the right side of the rotor cradle) and proceeds, from right to left, through the right-most, middle and left-most rotor. Once the signal has passed all three or four rotors, the reflector returns this signal back trough the left, middle and right rotor via another path, causing a second completely different scramble of the signal. It is obvious that the combination of rotor wiring, rotor position and ring offset created a complex encryption. A single step of one rotor will produce a completely different path trough all three rotors.

The Rotor Stepping Mechanism

If we talk about rotor positions, the following notation is commonly used: V, I, III means that the left-most rotor is type V, the middle type I, and the right-most is a type III. If the turnover point of rotor type I is 'Q', this means that the next-left rotor will perform 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. The rotors VI, VII & VIII have two notches and therefore will advance the rotors to their left will twice as fast as single notch rotors.

Rotor	Turnover	Action
I	Q	When rotor steps from Q to R, the next-left rotor steps
II	E	When rotor steps from E to F, the next- left rotor steps
III	V	When rotor steps from V to W, the next- left rotor steps
IV	J	When rotor steps from J to K, the next- left rotor steps
V	Z	When rotor steps from Z to A, the next- left rotor steps
VI + VII + VIII	Z + M	When rotor steps from Z to A or from M to N, the next- left rotor steps

The rotors appear to work as a normal odometer, with the right-most rotor always stepping on each key stroke and the other rotors stepping after a complete cycle of the previous rotor, but there is an important difference due to the system of pawls and teeth. 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. Below and example of such a sequence when the rotors III – II - I are used:

KDO KDP, KDQ, KER, LFS, LFT, LFU…

As you can observe, stepping from Q to R advances the middle rotor, and on the next step that middle rotor steps again, advancing the third rotor also. This is caused by the mechanical design of pawls and teeth.

There are three pawls that are all three activated on every key stroke. Each pawl is half positioned on the index ring (carrying a notch) of the rotor on its right, and half positioned above the 26 teeth of the rotor on its left (viewed from the point of the operator). A rotor's ring prevents the pawl from pushing into the teeth of the next-left rotor. When a notch occurs in a ring, the pawl can drop into that notch and push into the teeth of the next-left rotor. Since the right-most pawl is not above an index ring it will continuously advance the right-most rotor.

Once the right-most rotor has stepped and the middle (spring-loaded) pawl can drop down in the right rotor's notch, it will engage the middle rotor's teeth, pushing the middle rotor one step. An identical event will take place when the middle rotor's notch enables the third pawl to drive the teeth of the left-most rotor.

A rotor will not only advance if its teeth are catched, but also when a pawl pushes into its notch. This situation creates a double-step of the middle rotor: the right rotor steps and the middle pawl takes the middle rotor one step further. If the middle rotor has moved by this step into its own notch position, then, on the next step, the right-most pawl catches the teeth of the right-most rotor, but the same pawl also pushes the middle rotor one step further, moving it a second time in a row. Note that a double notched rotor in the middle position will also have two double steps.

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 adapting the stepping mechanism or adding a fourth pawl. Therefore, the fourth rotor never moves and can only be adjusted manually.

Other Enigma Models

Several other Enigma models, civilian as well as military, were manufactured. The popular civilian Enigma D and Swiss K model had three rotors and a rotatable reflector (which looked very similar to a regular rotor). The reflector could be set in one of 26 positions but didn't step during enciphering. The commercial machines had other rotor wirings than the military versions and did not carry a plugboard.

The Abwehr (German Intelligence Service) used a variant where the rotor pins were not placed circular but in a zigzag pattern. The rotors, each carrying multiple notches, were driven by a system of gears instead of pawls. This machine neither had a plugboard. These machines also had their own rotor wiring.

The commercial enigma was sold to many counties and each country used its own rotor and reflector wiring, for obvious security reasons. However, since all machines were produced in Germany, it is unlikely that those wirings were unknown to German intelligence. Most of the machines that survived the war were seized by the Allies, who rewired the rotors and sold them to other countries, of course not mentioning their ability to crack the Enigma.

The cryptographic strength

To calculate the mathematical security we have to find all possible different settings of the machine. Therefore, we need to look at the following properties of the machine: the selection and order of the rotors, their wiring, the ring setting on each of the rotors, the start position of these rotors at the beginning of the message, the reflector and the plugboard settings.

Now, there are different ways to calculate a grand total of this. If all possible variations of wiring in each of the rotors and the reflector are included, this results in an astronomical 3×10^{114} possible different combinations. However, this figure represents all theoretically possible variations of the machine.

Unfortunately for the Germans, the Allied codebreakers knew the machine, the rotors and the internal wiring of these rotors. Therefore, they only had to take in account the actual different ways you could set the machine, the actual key settings or key space. This is what we call the practical security, which is far less than the theoretical security in the case of Enigma. For the German cryptologists, a single rotor could be wired in 4×10^{26} different ways. Combining three rotors and a reflector quickly gives you astronomical figures.

For the Allied codebreakers, who knew the wring of the rotors, there were only 26 different variations for a single rotor, that is, the 26 positions it could have in the machine. They didn't have to search through the immense number of possible wirings. The German cryptologists made a critical mistake by ignoring Auguste Kerckhoff's law that the security of a device may never depend on the secrecy of the system (i.e. rotor wiring, design), which will be compromised sooner or later anyhow, but only on the secrecy of the key (i.e. rotor selection and plugboard.

Let us look at all the things we can actually set on the machine which are unknown to the codebreaker. In our example, we take the three-rotor Wehrmacht Enigma with default B reflector and selection out of 5 rotors. We use 10 plug cables on the plugboard, the default number of cables, issued with the machine (don't ask me why they didn't provide 11 cables, which gave far more possible combinations)

To select 3 rotors out of a possible 5, there are 60 combinations (5 x 4 x 3). Each rotor, in other words, its internal wiring, can be set in any of 26 positions. Therefore, with 3 rotors there are 17,576 different rotor positions (26 x 26 x 26). The ring on each rotor holds the rotor labeling (which doesn't matter here) and a notch that affects the stepping of the next-left rotor. Each ring can be set in any of 26 positions. As there is no rotor to the left of the third (most-left) rotor, only the rings of the most-right and middle rotor affect the calculation. This gives 676 ring combinations (26 x 26). With 10 plug cables you can wire the plugboard in 150,738,274,937,250 different ways.

In total, this gives:

60 x 17,576 x 676 x 150,738,274,937,250 = **107,458,687,327,250,619,360,000** or **1.07×10^{23}**

Thus, the Wehrmacht Enigma machine could be set in **1.07×10^{23}** different ways, comparable with a **77 bit key**.

There are some comments we should add to this number. In reality, the maximum period of the rotors - the number of steps before the machine repeats itself - is slightly less than 17,576. This is caused by the double-step feature of the stepping mechanism. The actual period depends on the type of rotor. The three double-notched Kriegsmarine rotors will have an even smaller period than the Wehrmacht rotors as they produce more double steps of the middle rotor. The maximum period however is no part of the variables that can be set and therefore do not influence the key space.

The Wehrmacht machine could be equipped with either the B or C reflector. In general, radio nets always used the same reflector, as the use of different reflectors created logistical, procedural and practical problems. If nonetheless taken in account, the choice between B and C reflector would only double the key space.

The adding of a fourth rotor for the Naval Enigma M4 to improve its security was a missed opportunity. The non-moving fourth rotor complicated the machine only by a factor 26 and, together with the thin reflector, could be considered as a settable reflector with 26 positions, of which the Allies quickly found the wiring (after 10 months of panic).

The introduction of 8 naval rotors on the Kriegsmarine M3 and later on the four-rotor M4 was a far better approach. They increased the rotor combinations from 60 to 336, and brought in additional complexity with 3 multiple notched naval rotors VI VII and VIII.

Let us now calculate the practical key size of the four-rotor Kriegsmarine Enigma M4. This machine uses 3 normal rotors, selected from a set of 8 (of which three with double notches). This gives 336 rotor combinations (8 x 7 x 6). The M4 also has a special fourth rotor called Beta or Gamma (without a ring), which gives us 2 choices. These are not compatible with the other rotors and are only suitable as fourth (most left) rotor. The 4 rotors can be set in any of 456,976 positions (26 x 26 x 26 x 26). The M4 had a smaller B or C reflector, to enable the placement of the fourth rotor. We don't include the choice of reflector as it was generally never changed. Again, only two rings were involved, as the third rotor didn't step the never moving fourth rotor. The M4 was also issued with 10 plug cables.

In total, this gives:

336 x 2 x 456,976 x 676 x 150,738,274,937,250 = **31,291,969,749,695,380,357,632,000** or **3.1×10^{25}**

Thus, the Kriegsmarine M4 Enigma could be set in **3.1×10^{25}** different ways, comparable with a **84 bit key**.

This is about 291 times stronger than the Wehrmacht machine. This is due to the increased choice of rotors (already available on the M3 before the war) and the possible initial positions for 4 rotors instead of 3. However, although the fourth rotor did increase the key size, it failed to add to the complexity of the encryption itself, since it couldn't move during the enciphering process.

A better solution would have been to completely re-wire some of the rotors on a regular basis. A single variable rotor wiring would multiply the key space with no less than 4×10^{26}, which is far more than a settable reflector with its 7.8×10^{12} possible variations. A single practical, daily changed, re-wireable rotor, which has 4×10^{26} possible settings, would have been much more effective than the overestimated daily non-moving plugboard setting with only 2×10^{14} variations (the plugboard was always in pairs). The use of such rotor, for instance in conjunction with a thin M4-like reflector and two out of four normal rotors, would be a true disaster for the codebreakers. However, introducing re-wireable rotors during wartime would have been cumbersome and a logistical and financial nightmare, just as the re-wireable D reflector proved to be. The D reflector did scare the codebreakers initially, until they realized that the D reflector was used simultaneously with the default reflectors in the same radio nets, due to practical considerations. This dual use made it possible to break it even by hand.

Any crypto-expert would also discard the 17,576 ring combinations. Even with completely wrong ring settings, you will initially start with a correct plain text. As soon as you get garbled text, you adjust the ring of the most-right rotor (a 1/26 chance you're right) and if you're lucky you have no more trouble for the next 676 characters. If less lucky, you had to adjust the ring of the middle rotor after 26 letters.

Unfortunately for the Germans, the ingenious Turing Bombe design, with mirrored identical rotor packs, avoided the need to search through the immense number of plugboard settings, taking a factor 2×10^{14} shortcut when linking of their cribs (known piece of plain and ciphertext) to a given rotor setting.

Nonetheless, the breaking of Enigma still was an enormous challenge with a key setting that was extraordinary in the electro-mechanical era of the 1940's. With a practical key space of 1.07×10^{23}, an exhaustive search was impossible in the 1940's, and its comparable 77 bit key is even huge for today's computer standards. To give you an idea of the size of that number, with 1.07×10^{23} sheets of paper (0.0039 inch each) you can build roughly 70,000,000 stacks of paper, each of them reaching from the Earth to the Sun. Also, 1.07×10^{23} inches equals 288,500 light-year. A pretty big number! The Germans were correct in assuming that the Enigma was theoretically unbreakable…theoretically!

Theoretical versus Practical Security

How secure was the Enigma machine actually and why ended it up being the Achilles heel of the superior German war machine? During a top secret Allied operation in the final days of the war, special TICOM teams round up German cryptologists and Signals Intelligence personnel. The answer to our question is found in their only recently declassified TICOM reports, vol 2, "Notes on German High Level Cryptography and Cryptanalysis".

Summarized, it comes to this: to create a secure crypto device you need both excellent codemakers and codebreaker. You cannot effectively assess the security of a crypto machine unless you test it by trying to break it. According to TICOM, Germany had very capable cryptologists and developed some excellent crypto machines. Unfortunately, their codebreaking skills, although excellent, were not on par with their brilliant Polish, British and American counterparts. It was this little difference in codebreaking skills that convinced the Germans that Enigma was secure. Their studies only revealed theoretical weaknesses. It was the same little difference in skills that enabled the Allies to find a practical solution to the theoretical weaknesses of the Enigma machine. German cryptologists did continue to develop various improvements to Enigma and other crypto machines during the war, some of which, according to TICOM reports, would prove impossible to break by the Allies at that time. Fortunately, logistical problems, shortage of raw materials and lack of time and money kept these new machines from entering service.

4. 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.

Kriegsmarine M4

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, which 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 on 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, a very similar machine, was introduced,. 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 several versions with different rotor wirings, and sold across Europe to military and diplomatic services. The Enigma D had three normal rotors and one reflector that could be set in one of the 26 positions.

Several intelligence services succeeded in breaking the civil and military Enigma versions which were all based on the commercial D. The Enigma D had no plugboard, a military feature that would increase security considerably from 1935 onwards. The Italian Navy bought the commercial Enigma D, as did Spain during the Spanish Civil War. The Swiss army used the Enigma K, a slightly modified version of the Enigma D. Japan used the Enigma T, also called Tirpiz Enigma, an adapted Enigma D with modified entry rotor connections. Japan also developed their own version of the T, with horizontally placed rotors. The messages of both models T and K were broken as well. The Railway Enigma, another D clone which was used by the German Reichsbahn in Eastern Europe, was partially broken from 1941 onwards..

Military versions

In 1926, the commercial Enigma was purchased by the German Navy and adapted for military use. They called it Funkschlüssel C. Meanwhile, Chiffriermaschinen-AG developed a special Enigma with rotors that have the same contact alignment as the D rotors, but with teeth, multiple notches and advanced by gears instead of pawls and teeth. It also had a rotating reflector and a counter on its left. Only one is know to exist today. This probably experimental model, presented in 1928 but exceptionally only patented in 1931, lead to the Enigma G. The Enigma G had different rotors with a zigzag pin placement and the counter on its right. Its rotors, which also had multiple notches, were moved by a system of gears, similar to the 1928 special predecessor. Already in 1928, the German Abwehr (secret intelligence service) bought the 12 Kg light Enigma G, also called Zahlwerk (clock-work) Enigma due to it's counter on the front panel. The Enigma G was exclusively used by the Abwehr.

The Wehrmacht revised the commercial Enigma D In 1932 and added the plugboard at the front of the machine. This version, designated Enigma I (later known as the Wehrmacht Enigma), was introduced on a large scale in the Heer (Army). The Luftwaffe (Airforce) followed the Heer'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 its 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.

During the war, different types of reflectors were introduced. The B and C reflector were used on both the Wehrmacht and Kriegsmarine M3 machines. The Kriegsmarine M4 used a thin B and C version, to fit in the 4 rotor machine, with other wirings, albeit compatible with the Wehrmacht M3 version in combination with its fourth rotor 'zeroized'. By the End of the war German Command tried to introduce a new type D rewirable reflector. Early use of this reflector posed a significant problem to Allied codebreakers, but problems in distribution of this reflector and its key sheets prevented a widespread use of the D reflector. Another military add-on, introduced in 1944 by the Luftwaffe, was an extra plugboard switch, called the Uhr (clock), a switch with 40 positions, each position resulting in a different combination of plug wiring.

An estimated total of 100,000 Enigma machines were produced. Although generally know as Enigma, there were only a few machines that actually carried the name Enigma and the logo. Most machines only had a serial number and fabrication code. The machines were produced in different factories on various locations such as Ertel-Werk für Feinmechanik in München, Olympia Büromaschinenwerke in Erfurt, Chiffriermaschinengesellschaft Heimsoeth & Rinke in Berlin, Atlas-Werke Maschinenfabrik in Bremen and Konski & Krüger in Berlin. The machines that survived the war were confiscated by the Allies and mostly sold to other countries. The rotors of these machines were often rewired. Of course, they forgot to mention that they were able to break them.

Breaking the code

When the Wehrmacht introduced the plugboard on the military Enigma, this added an astronomical number of possible key settings. The general idea was that this military Enigma, unlike the commercial types, would be impossible to break. No one even tried to break it. However, 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 were convinced that mathematics could solve the problem and succeeded in breaking the Enigma messages. They also 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 basic setting and the twice encrypted 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 rotor choice of the Enigma, new procedures and a lack of funds for the Polish codebreakers. Just before Germany invaded Poland, the Biuro Szyfrow passed its knowledge and several replica Enigma machines to the baffled French and British intelligence. The work of the Biuro Szyfrow was vital, not only because their pioneering work, but also because it convinced other cryptologic bureaus that it was possible to break Enigma.

Bletchley Park

The Government Code and Cipher School (GC&CS) 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 so-called cribs. These cribs were presumed pieces of plain text within the encrypted message. This could be "An Der Oberbefehlshaber", "An Gruppe", "Es Lebe Den Fuhrer" or any other standardized code (from code books) or piece of text. Once a crib was located (special techniques existed to do this) 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 - was codenamed 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, to avoid any suspicion with German command. 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 Germans a reason to suspect that their communications security might be breached.

The Kriegsmarine

The German Kriegsmarine was very successful in applying their Rudeltaktik or "Wolfpack" tactics with U-boats. They hunted individually for convoys and when 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 and the complicated 'Shark' codes caused a big crisis at Bletchley Park. The Kriegmarine 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 Blechtley Park discovered by cryptanalysis that a fourth rotor had entered the battlefield of codes. After ten nerve-wracking months of heavy losses, Bletchley Park succeeded in breaking the 'Shark' codes. The major reason for this success was the capture of Kurzsignal codebooks by British Navy on German weather ships and the attacks on U-boats like Kapitanleutenant Heidtmann's U-559 by HMS Petard. These boarding were not to steal Enigma machines or key sheets, as often wrongly portrayed in movies and books (they already had replicas of the Enigma from the Biuro Szyfrow). Enigma key sheets only gave access to a particular radio net and area for a single month. However, only two editions of the Kurzsignal codebook, issued to all U-boats, were ever printed during the war. These codebooks encoded weather and operational reports in four-letter codes, prior to encryption with Enigma. By seizing them, Bletchley Park could use these four-letter codes as new cribs to attack all future Enigma setting. Moreover, new Bombes were developed to deal with the four-rotor Enigma, and by the end of 1943, another fifty of these Bombes became operational in the US Navy.

The tide of the U-boat war had turned. Except for some brief periods, the entire communication system was intercepted by a large number of listening stations, and the message were broken in Bletchley Park, which employed over 7000 workers at its peak. With the positions of the U-boats unveiled, Allied ships could now evade the U-boats and the Allies actively hunted for U-boats. The elite weapon of the Kriegsmarine got decimated, with heavy losses among the U-boat crews. An estimated 700 U-boats and 30,000 crewmen were lost at sea. U-boat command never suspected cryptanalysis of the Enigma and related these losses to new Allied submarine detection techniques like ASDIC sonar, surface radar, HF direction finding and anti-submarine airplanes.

All improvements, introduced by the German Forces, were tackled successfully by the codebreakers. The introduction of the rewireable D reflector, with its key changes every ten days, proved to be a big problem to the codebreakers. A widespread use of the D reflector would require five to ten days to break a particular key (without D reflector only 24 hours), which would render tactical information useless. Fortunately, logistical problems prevented general use of the D reflector in the German forces. German operators were also reluctant to use the D reflector and found it too elaborate to program in tactical situations. Instead, the B reflector remained the default reflector and the D reflector was used for important messages only, on the same machines with the same basic machine settings for rotors and plugboard. With the key already broken for these machines with the B reflector, the codebreaker only had to retrieve the unknown wiring of the D reflector, used on that same machines. A work that was performed by hand. The fatal mixed use of B and D reflectors enabled the codebreakers to continue reading the once feared D reflector messages. The Enigma Uhr (clock), used by the Luftwaffe, was another useless effort by the Germans to increase the security of the Enigma. The Uhr was a switch that replaced the plugs of the Enigma and provided 40 different plug wirings. However, the unique design of the Allied Bombes, used to retrieve the key settings of the Enigma, excluded the plugboard wiring. The Enigma Uhr therefore had only little effect on the codebreaking results.

The ULTRA information was kept highly secret during the entire war and played a decisive role. Breaking the Heer and Luftwaffe messages also provided crucial tactical information. The codebreakers exposed the weakness of Field Marshal Rommel's notorious Afrika Korps. The speed and success of the Afrika Korps created long stretches of poorly defended supply lines. ULTRA information revealed their logistical problems and provided Field Marshal Montgomery with a vital tactical advantage. In the days before the D-day invasion of Normandy, the Wehrmacht, without realizing it, provided the Allies with an enormous quantity of detailed information on the coastal defences, location and strength of all German tank divisions and the movement of troops in France. Experts estimate that the breaking of Enigma shortened the war by about three years. The number of saved lives is innumerable. The large scale breaking of German communications was one of the best kept secret of the Second World War. German armed forces kept on using Enigma during the entire war without any suspicion.

5. Websites about the Enigma cipher machine

Cipher Machines & Cryptology (Enigma simulator website)
http://users.telenet.be/d.rijmenants

Paul Reuvers' and Marc Simoens' Cryptomuseum
www.cryptomuseum.com

Bletchley Park official site:
www.bletchleypark.org.uk

Tom Perera's Enigma Museum:
http://w1tp.com/enigma

Frode Weierud's Crypto Cellar
http://cryptocellar.org

David Hamer's cryptology website:
http://home.comcast.net/~dhhamer

Tony Sale's Enigma pages:
www.codesandciphers.org.uk/enigma

TICOM report on Axis SIGINT, vol 2, "Notes on German High Level Cryptography and Cryptanalysis" (pdf)
http://www.nsa.gov/public_info/_files/european_axis_sigint/volume_2_notes_on_german.pdf

6. Copyright Information & Disclaimer

Copyright Information

This software is provided as freeware and can be used and distributed under the following conditions: it is strictly forbidden to use this software or copies or parts of it for commercial purposes or to sell or lease this software, or to make profit from this program by any means. You are allowed to use this software only if you agree to these conditions.

This manual is copyrighted and reproduction of its content is allowed only after explicit permission of the author.

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, or fitness for any particular purpose. The entire risk as to its quality and performance is with the user. In no event will the author of this software be liable for any direct, indirect or consequential damages, resulting out of the use or inability to use this software.

Cipher Machines & Cryptology
http://users.telenet.be/d.rijmenants
dr.defcom@telenet.be