ENIGMA - E

A fully operational - Real - Electronic Enigma

USER MANUAL

by Paul Reuvers & Marc Simons

with contributions by
Frode Weierud and Geoff Sullivan

including never-before released original German Army Enigma Messages

ENIGMA - E

A fully operational - Real - Electronic Enigma

Electronic DIY kit - All components included

USER MANUAL

Step by step guide to build your own electronic Enigma
Version 1.32 9 August 2004

by Paul Reuvers & Marc Simons

with contributions by Geoff Sullivan & Frode Weierud
including never-before released original German Army Enigma Messages

First printed September 2003

Acknowledgments

The authors wish to thank the following people and organisations:

- Geoff Sullivan & Frode Weierud, *Secrets From The Past: Breaking German Army Ciphers* (Chapter 8)
- Dr. David Hamer, photographs, advice and support
- Arthur O. Bauer, calculations in chapter 6
- Karl de Leeuw, *Invention of the Rotor Machine* 1915-1923
- Jerry Proc, photographs
- Bureau voor de Industriële Eigendom, Rijswijk, Netherlands
- British Patent Council, UK
- Reichspatentamt, Germany

Disclaimer

Although every effort has been made to ensure that the information presented in this document is correct, this cannot be guaranteed. Neither the producers of this Building Kit, nor the reseller can be held responsible for any loss or damage, financially or otherwise, direct or indirect, resulting from the use or misuse of this product. The **Enigma-E** is intended for educational purposes. The suitability of this product for any purpose whatsoever, cannot be guaranteed. Please note that encrypting messages may be subject to local law.

Trademarks

© Copyright 2001 - 2004

September 2003,

Paul Reuvers (PE1BXL) & *Marc Simons* (PE1RRT)
enigma-e@xat.nl

website: http://www.xat.nl/enigma-e/

Contents

Continued on the next page...

1. Introduction

Thank you for purchasing the **Enigma-E** DIY kit. You are about to start building your own Enigma machine and we can image the excitement you must be feeling at this very moment. Please read this manual carefully before you start building your machine; this will help to avoid problems, questions and dissapointment later.

You don't have to be an experienced electronics engineer to build this kit. However, some basic knowlegde and practice, especially with soldering of electronic components, is most welcome. If you lack this experience, or if you don't feel confident to build this kit, please ask someone with the required skills. There are many electronics enthousiasts around and in particular radio HAMs may be willing to help you out.

The next chapter explains in great detail how the **Enigma-E** is best built up. Before you start, you should check if all components have been delivered. If any item is missing, please contact us immediately on our e-mail address **enigma-e@xat.nl** and tell us which item you can't find and where you purchased your kit. The best way to check whether all components are present is to use the next chapter as a guide. Each component is separately listed and two check boxes are available: one should be ticked if the item has been located, the other one should be ticked when the item has been mounted on the PCB (Printed Circuit Board). Please note that we've checked and re-checked every kit prior to packing, so please look twice before reporting a component as missing.

Once your **Enigma-E** is built, you need to test it. Chapter 3 describes how to do this. Please follow the procedure carefully, to ensure that your device is working properly. If it passes the test, you may want to decode your first message. Chapter 3 describes a real message with a simplified setup procedure, so if you really can't wait...

By buying this **Enigma-E** DIY kit you are actually contributing to restoration and conservation of old WWII equipment. In the UK the project will support the Bletchley Park Museum, which is *the* place for all Enigma enthusiasts. In The Netherlands, we will be supporting the Museum Jan Corver, named after one of the first radio HAMs in that country. Other projects may be supported in different countries.

We wish you good luck and a lot of fun when building your own **Enigma-E**.

September 2003,
Paul Reuvers & Marc Simons

1.1 How it all started

You may wonder how the idea was born to create an electronic variant of the famous Enigma coding machine. Well, it all started in the summer of 2001. After having read the book Enigma, by Robert Harris, we got intrigued by the mysteries of this secret little machine. Shortly after, we attended a lecture on WWII radio equipment and the presenter briefly touched the subject of the Enigma and... Bletchley Park.

After searching the Internet, we found that Bletchley Park actually existed and had just opened as a museum. A destination for our summer holidays was found. In our busy schedules, we both managed to allocate a week in August. At Bletchley Park we found the answers to most of our questions and we were overwhelmed by the quantity and quality of the information presented there. Not only can you see the Enigma behind glass, there is actually a device available for you to touch and type your own message!

Once you've seen the Enigma in action, you are likely to be contaminated with the Enigma Virus. It seems that there is no cure to this disease. The more we read about the Enigma, the more we wanted to possess such a machine. The only problem is that they are rare these days and the few machines around really cost a fortune. We then decided to build our own machine. Since we are both electronic engineers, the decision was made to create an electronic equivalent, using modern components and built around a small micro processor.

1.2 The RISC OS Simulator

Many problems had to be overcome before we could start building our Enigma. First of all we needed to understand exactly how the mechanics and the electronic circuits inside the Enigma work. How do the wheels move when a key is pressed? What is the effect of the Ringstellung? What happens if you accidently press a wrong key? What does the Steckerbrett do? How many wheels are available? What is the wiring of each wheel? Questions, questions, questions...

Programming a small micro processor is a tedious task. As the memory in such devices is rather limited, they are best programmed in machine code (also known as Assembly Language). The problem with machine code however, is that experimenting and debugging is not very easy, to say the least. So we had to find a way to test the Enigma algorithm before actually starting to program the micro controller. Time to build a simulator.

For our regular jobs, we have some RISC OS computers available. You may remember these machines as they were at one time very populair in British schools. The BBC Computer, followed by the Archimedes and later the Acorn Risc PC. Recently these machines have been superceeded by the all new IYONIX pc, which runs the latest release of the RISC OS operating system. RISC OS is believed to be very powerful and comes with an advanced BASIC language (BBC BASIC V), which is excellent for our experiments.

Simple BASIC programs were created to test the permutations of the wheels and to check the wheel wiring. In the end the BASIC program turned out to be a real simulator, capable of decoding every message we could find and suitable to simulate every Enigma variant we had found. As we were already suffering from the Enigma Virus, we thought it would be 'neat' to finish off the simulator and make it available via the Internet to other users of the RISC OS operating system. Finally, it became the most advanced and realistic Enigma simulator yet available. It features high quality graphics, sound, smooth animation and much more. Details of our findings can be found in chapter 6, where we explain the working principle of the Enigma machine.

Here's a screen shot of the Enigma Simulator for RISC OS, running an M4 emulation. If you're interested, the full software is available from the website at

http://www.xat.nl/enigma/

The website also contains links to Enigma Simulators on other platforms, such as Windows, Palm, Psion, Java, etc.

1.3 The Electronic Enigma

Now that we had a reliable simulator, we could actually start working on our initial goal: the electronic Enigma variant. As we were already playing with the thought to make it available as a DIY kit later, we wanted to keep the cost at an absolute minimum. A circuit diagram was designed and every effort was made to keep the circuit as simple as possible. We decided to keep the look and feel of the original Enigma: our device would need to have 26 keys and 26 lamps, otherwise it wouldn't be a real Enigma.

Next, we needed to find a replacement for the -mechanical- wheels. Alpha-numerical LED displays where found and the latest generation of these, produces much more light at much lower power consumption, which was very welcome as we wanted the device to be battery powered. At the heart of the unit came a low-cost micro controller from the well known manufacturer Microchip. A range of processors with built-in memory is available from this brand, and we picked a model that would be large enough to simulate both the M3 and M4 Enigma machines.

Once the circuit diagram was complete, a professional PCB (Printed Circuit Board) had to be designed. We decided to create the PCB in two parts: the main Enigma PCB and a separate Steckerbrett. This would greatly enhance the possibilities when building the PCB in a case. Some people may want to use the Enigma 'as is', whilst others may want to build it in, say, a wooden box.

When the first prototype boards arrived from the PCB manufacturer, we were very nervous. First we had to check if all components would fit -mechanically- on the PCB, which they did. We then built the first board and tested it electrically and, believe it or not, it passed the initial test. But that was only part of the story as the real pain had yet to come: programming the Microchip controller. To cut a long story short, after weeks of programming, testing and modifying, we finally managed to decode our first real message. The many hours that went into the project had payed off and we were finally looking at a more or less finished product.

If you are interested in electronics and circuit diagrams, you'll find the complete story in chapter 4. The full circuit diagram is printed in Appendix A (separate sheet).

1.4 What's in a name?

We now needed a name for our new Enigma variant, especially if we were going to sell it. Many names were invented and scrapped and we finally adopted the simplest of them all. Most real Enigma machines have a serial number starting with a letter. 'A' for the Heeres Enigma (Armee) and 'M' for the naval machines (Marine). Other letters were used for special Enigma variants, such as 'G', 'K', 'D', 'C', etc. As our machine is completely driven by electronics, we will be using the letter 'E' which is not used for any other Enigma variant. Thus, the **Enigma-E** was born.

1.5 Terminology used in this manual

Many articles on the Enigma subject have been written over the years. Depending on the country of origin, different expressions are used for the same thing. Take for example the wheels of the Enigma: in UK English they are often called **Wheels** or **Drums**, whilst in American literature they are commonly called **Rotors**. And to make it even more complex, the original German expression for a wheel is **Walze**. In this manual, we will be using the German expressions wherever possible. After all, it is a German device.

1.6 Registering your device

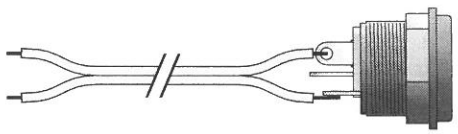
Each **Enigma-E** comes with a unique serial number and a certificate to prove that it's a genuine item. The serial number is printed on the box, the PCB and on the certificate. We would like you to register yourself and your serial number through the on-line registration form on the website. This way, we can keep you informed of future developments. To register, visit:

http://www.xat.nl/enigma-e/

Mount these wires to the oval pads **1...7** at the back of the PCB. Insert the wires from the back and solder them. The oval pad is large enough to do this. Mounting the cables from the back of the PCB may prove useful if you want to build both PCBs in a case mounted at an angle of 90° between them. If you want, you may now break off the Steckerbrett, but be careful not to damage the rest of the PCB and the components.

2.5.2 Connecting a battery and/or adapter

Take the piece of dual wire that you've found in the kit and cut it in half. Strip the wires at both ends. Solder the two wires at one end to the outer contacts of the power socket. The other end goes to the two pads, marked a ~ on the top left of the Enigma PCB. The word **Adapter** is printed between these two pads. Insert the wires from the back of the PCB and solder them at the back.



Prepare 3 pieces of the single black wire of 20 cm each (approx. 8 inches) and strip them at both ends. Solder one end of these wires to the (optional) power switch. The other ends should go to the pads marked **B**, **C** and **N** at the top of the PCB (to the right of the Voltage Regulator). The centre contact of the switch should go to the pad marked as **C**.
If you don't have a switch available at this point: don't worry. You may use a short piece of wire to connect the **C** terminal to the **B** terminal if you're going to use a battery, or between **C** and **N** if you're going to use an external power adapter.

You may connect a battery to the (**plus**) and (**minus**) terminals at the top left of the board. These terminals have the word **Battery** printed in between them and they are located to the right of the of the *Adapter* terminals we've discussed before. Put the switch in the 'N' position to turn the **Enigma-E** off, or in the 'B' position to turn it on. The **Enigma-E** consumes about 20mA. A standard 9V block battery will last for about 6 hours!

2.5.3 Wiring the serial port

Connecting the serial port is not necessary for a correct operation of your **Enigma-E**, so you may want to do this at a later stage. However, it may be nice to be able to send and receive encrypted messages to and from another **Enigma-E** or a PC. If you want to use the port, you need to connect an (optional) 9-pin sub-D female connector to the pads marked **TxD**, **RxD** and **GND**. These pads are located at the top right of the PCB.

- Pin 3 on the serial port of a PC always carries the TxD signal. This signal comes from the PC and should go into the RxD line of the **Enigma-E**.
- Pin 2 on the serial port of a PC always carries the RxD signal. This line should be connected to the TxD line of the Enigma-E. This is the data that flows from the **Enigma-E** to the PC.
- Pin 5 on the serial port of a PC is always connected to ground (GND) and should be connected to the GND terminal of the **Enigma-E**.

The serial port of the **Enigma-E** runs at 9600 baud, 8 data bits, no parity and 1 stop-bit (often referred to as 9600, 8N1). At the PC-end you may use any piece of terminal emulation software (e.g. VT110, VT220, TeraTerm, HyperTerminal, PCCom, HearSay, etc.). Please note that you should turn handshaking off.

Users of a RISC OS computer are in an even better position: they may use the *Enigma Simulator for* RISC OS, described in paragraph 1.2 to connect their RISC OS computer directly to the **Enigma-E**.

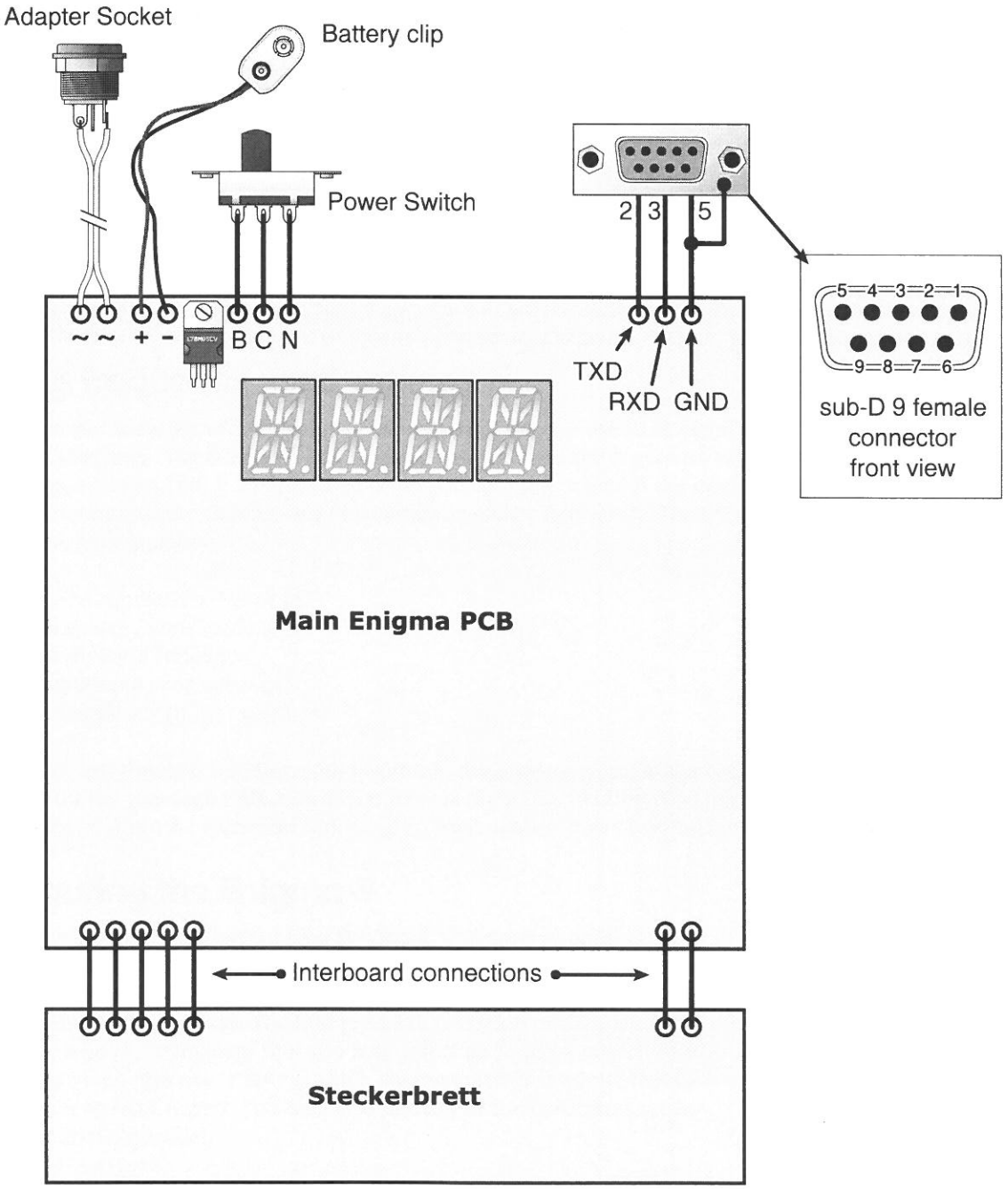
2.5.4 Fitting the jumpers

For now it's best to leave the jumpers off, until we've tested the **Enigma-E**. The jumpers may be used at a later stage, to turn certain special features on or off. If you don't want to lose the jumpers, you may fit each of them to a single pin of the header (J1).

2.6 Wiring Diagram

The drawing below shows how the boards are connected together and how the external components should be connected to the main PCB. The polarity of the external adapter is not important (i.e. the leads may be swapped). The polarity of the battery however, **is** important. The **red** wire should go to the **leftmost** terminal (marked +) and the **black** wire should go to the **rightmost** terminal (marked with a minus sign). The power switch is used to switch between the battery and the external power supply. Only three contacts of the power switch are used.

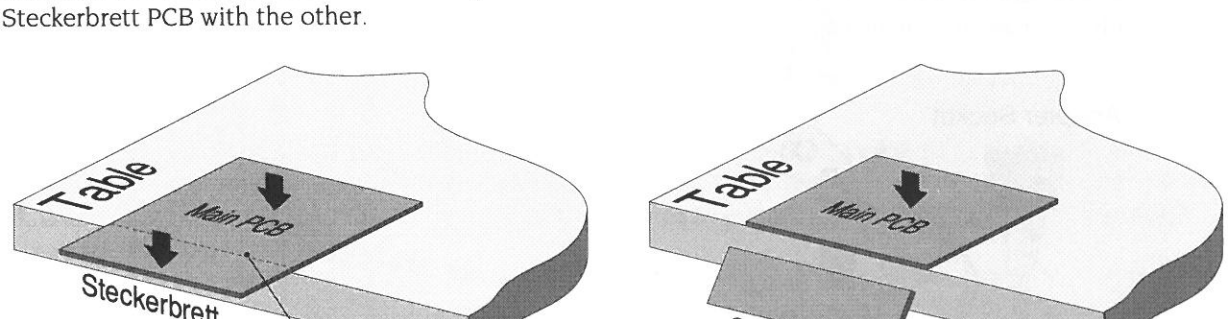
If you want to use the serial port, please use a sub-D 9-pin female connector or socket and connect it in the way described below. The TXD line should go to pin 2, RXD is connected to pin 3 and GND is connected to pin 5. To avoid damage to your PC, it is advised to connect pin 5 to the metal house of the sub-D connector.



2.7 Separating the PCBs

As it will have become clear by now, the **Enigma-E** PCB consists of two parts: the main PCB and the Steckerbrett PCB. It's up to you to decide how you want to use your kit: either as one contiguous PCB or as two separate boards. Which ever way you use it, you'll always have to establish the connections between the two boards as described in paragraph 2.6.

On a genuine Enigma machine the Steckerbrett is fitted to the front of the machine, so you might want to separate the Steckerbrett of your **Enigma-E** from the main PCB. The PCB has already been prepaired for this and if you look closely, you'll see a **V-cut** line on both sides of the PCB. Place the PCB at the edge of a table and align the V-cut line with the table edge. Now hold the main PCB with one hand and break-off the Steckerbrett PCB with the other.



Don't be afraid to apply some force whilst doing this. The V-cut line was added to the PCB especially for this purpose and breaking the PCB shouldn't cause any damage to the PCB or the components.

3. Using your Enigma-E

In the previous chapters we've described how to build the **Enigma-E** PCB and how to connect it to the outside world. It's now about time to turn it on for the very first time. Before you do that, please check all wires and solder junctions once more to ensure that everything is connected in the right place.

3.1 Testing the Enigma-E

Ensure that only jumper ⑤ is fitted to the header (**J1**) and connect the battery or power adapter to the unit. If you are using a power switch, turn it on now. The first thing you should see, is a rotating line on each of the LED displays followed by some initialisation messages.

If this doesn't happen, something is wrong. Check the state of the power switch. Also check the amount of current taken up by the unit. If it's using much more than 20mA, something really is wrong (e.g. a component fitted the wrong way around)! If you don't have access to a current meter, check the multifuse (**FUSE1**) by touching it with your hand. If it's hot, turn the **Enigma-E** off immediately! Now check the PCB for short circuits and also check if any of the components is fitted the wrong way around.

If you can't work it out, use a volt meter to check the power between the rightmost pin of the Voltage Regulator and its case (the bolt). This should be 5V. If the 5V is present, you should at least see something on the displays. You may also try to disconnect the Steckerbrett. Next try the **Enigma-E** again. If it works, you know for certain that the problem is in the Steckerbrett. You may also check the section on *Trouble Shooting* on our website at: **http://www.xat.nl/enigma-e/**.

Left of the PIC (**IC5**) is a green LED, which can be regarded as the heartbeat of the unit. If the software is running OK, it should flash once every second.

3.2 Storing frequently used settings

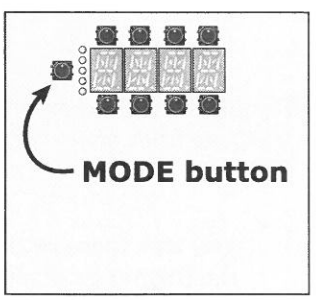
When experimenting with enciphered messages, it may be useful to store a number of commonly used Enigma settings. The **Enigma-E** can store up to 8 of these settings in its non-volatile memory. These settings, called **A** thru **F**, are retained when you turn the power of the unit off! This can be very useful if you want to return to the *Grundstelling* of a certain message frequently. The following settings will be stored in the on-board memory:

- Enigma Emulation: M3 or M4,
- Walzenlage (wheel order),
- Umkehrwalze (reflector),
- Ringstellung (ring settings),
- Grundstellung (initial settings).

If you've just finished building your **Enigma-E**, the 8 memory positions are, of course, empty and the display will show the message **FAIL** on startup. This is not a malfunction. You need to store a valid setting in memory position **A** before you can recall it. We'll explain how to do this in a few moments.

3.3 Configuring the Enigma-E

To alter the basic settings of your **Enigma-E**, you need to enter the **Configuration Mode**. Press the **MODE** button (to the left of the displays) briefly. The Enigma will now show the message 'SELECT AN ENIGMA' in the displays. The first red LED to the left of the displays will now be lit, to indicate that you may select an Enigma model. In the display you'll now see '***M4***', which means that it is currently set to emulate an M4 Enigma. You may now use any of the up/down keys to select another model.



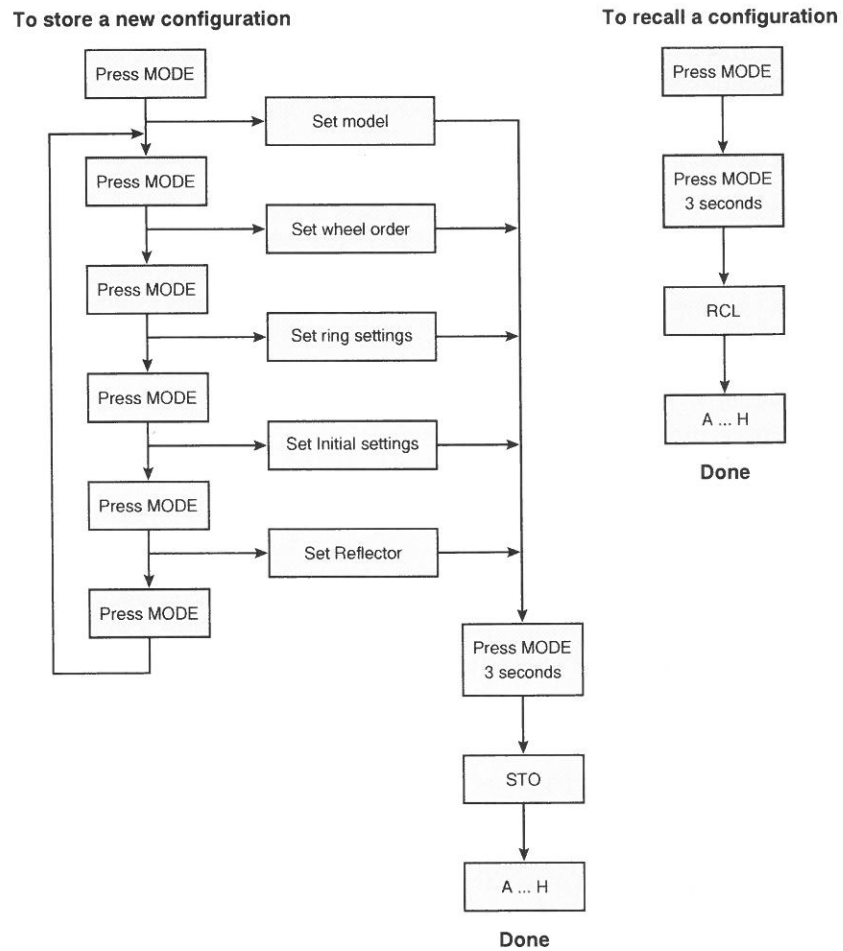
Press the MODE key again to change the next item. A different red LED will be lit each time you press the MODE key. You may now change the following settings respectively:

•	SELECT AN ENIGMA	***M4***	Use up/down to select a model.
•	SET WHEEL ORDER	**c215**	Walzenlage ('c' means 'gamma')
•	RING SETTINGS	**ASOD**	Ringstellung
•	INITIAL SETTINGS	**AMZI**	Grundstellung
•	UKWC	**UKWC**	Umkehrwalze C

You may use the MODE key to step through these settings as often as you like. Each display has its own up and down key. Press any of these keys to alter the contents of the display. Whenever you've changed any of the settings, the red LED will start flashing to show you that the software has detected your change.

Once you are statisfied with the new settings, press and hold down the **MODE** key for about three seconds. The message '**CHOOSE FOR STORE**' will now be shown in the displays, followed by a blinking messge '**STO**'. You should now tell the **Enigma-E** in which of its 8 memory positions you want these settings to be stored. You should do this by pressing one of the letters **A** thru **H** on the normal keyboard. 'A' means the settings will be stored at memory position 1, 'B' means 2, etc. Press for example the letter 'H'. The machine will now show that it has accepted this. Please note that you must store a setting at memory position **A** to prevent the message **FAIL** on start-up.

The flow chart below clearly shows how to save and recall any of the 8 preferred settings.



Play with these settings for a while to get a good feeling of what's happening. The scrolling messages on the **Enigma-E**'s displays are used to guide you through. Messages can be supressed by inserting *jumper* 4.

3.4 Setting the jumpers

The jumpers are only used to turn off certain features of your **Enigma-E**. The table below shows the meaning of each of the jumpers. They are numbered ① to ⑤, just like it is printed on the PCB. The topmost one is ⑤.

⑤	**Hide Permutations**	If the jumper is out, the **Enigma-E** will slowly show the entire translation process (permutations) in the displays.
④	**No Scrolling messages**	If the jumper is in, no scrolling messages will be used in the Configuration Mode.
③	**No Startup text**	If the jumper is in, the **Enigma-E** will not show the lengthy startup message.
②	**Morse OFF** **Serial port ON**	If the jumper is out, the serial port will be turned off and the terminals of the serial port may be used to connect an extra (optional) buzzer. Each time you press a key, the corresponding enciphered letter will be sounded in morse code. Check the website for more information.
①	**Buzzer inhibit**	If the jumper is in, the buzzer will be turned off.

Jumper ⑤ needs a little extra attention. If you press a key, with the jumper removed, the **Enigma-E** will show all permutations as and when they happen. It'll show the encoding by each of the wheels. Try some messages and see if it works correctly. This feature has been implemented in case you want to learn more about the internal algorithm used by the Enigma. For normal use, jumper ⑤ should be in place. Please refer to paragraph 3.8 for more information.

3.5 Factory Default settings

At some stage you may end-up in a situation whereby you've messed up all of the settings. If that's the case, you might want to return your **Enigma-E** to the default settings. The factory default settings of the **Enigma-E** are:

Emulation:	M4
Walzenlage:	gamma-215
Ringstellung:	ASOD
Grundstellung:	AMZI
Umkehrwalze:	C

Here's how to return to the factory default settings:

- Turn the **Enigma-E** off by removing the power.
- Press and hold down the MODE key.
- Turn the **Enigma-E** on, whilst keeping the MODE key depressed.
- Wait until the **Enigma-E** has fully started and release the MODE key.

The factory defaults have now been restored and you may save the new situation:

- Press **MODE** again,
- Toggle between **M4 -> M3 -> M4** emulation (the software needs this to notice a change).
- Press the **MODE** key for 3 seconds.
- Press any of the keys **A...H** on the keyboard.

Note:
Please note that, after the factory defaults have been restored, the display will read **FAIL** on startup. This is not a malfunction of your **Enigma-E**, but an indication that it has failed to load any user settings. Once you've stored a setting, as described above, this message will no longer appear.

3.6 Decoding your first message

Now that we've established the correct operation of your **Enigma-E**, it's time to decode our first message. For this we use a real message with a simplified setup procedure, which is reprinted here with kind permission from Dr. David Hamer.

IMPORTANT NOTICE

When typing the message, you need to PRESS and HOLD DOWN a key, in order to see the enciphered letter. Try this a few times to get familiar with it. Here is an example. Press and hold the **A** key. The translated letter, say **H**, will now be lit on the lamp panel. As soon as you release the key, the lamp panel will be cleared again, just like on a real Enigma.

You are the radioman on the U-516 that departed Kristiansand, Norway on 16 April 1945.
The date is now 30 April 1945 and the Radio Officer has set your Enigma to the daily settings, which are:

Umkehrwalze	**C**
Walzenlage	Gamma, II, I, V (shown on the display as: **c215**)
Ringstellung	**ASOD**
Grundstellung	**AMZI**
Steckerbrett	**AD LR ZJ XI BU KV SW FH EN MY**

The following encrypted message has been received:

HRQN SMAD LVIO DMMW JLKN GSRJ VNLC IKGT
MDRB IDAW YLIK IFIF CMCG HRQN SMAD

Select the **M4** emulation and setup the *Walzenlage*, *Ringstellung* and *Steckerbrett* to the settings given above. Setup the *Grundstelling* so that it reads **AMZI** in the display and type the first two four-letter groups. This will reveal the message key in duplicate. Set the four *wheels* of your Enigma to this key and decrypt the remainder of the message. Just to give you a hint: the first word **LVI** should translate as **DER**, so if you don't get this, think again! The final pair of four-letter groups is a repeat of the enciphered message key and may be ignored.

If you accidently press the wrong key when typing the above message, ignore it and proceed to the next character. Do not re-enter the character that was wrongly keyed or the rest of the message will become meaningless...

Note:
As stated at the beginning of the paragraph, we've taken certain liberties with history here, by using the simpler message key employed by the German army in 1939. The naval key system is far too complex at this stage...

3.7 Sending messages

By now you should know how to decode a message, but what about encoding a message? Well, due to the way in which the Enigma works, the cipher process is reversable. In other words: encoding works exactly the same as decoding. Exchanging Enigma messages, requires both the sender and the receiver to setup their Enigma in exactly the same way.

3.8 Showing all permutations

Every time a key is pressed on the Enigma, a complex poly-alphabet substitution process is started. Each part of the Enigma may translate the keycode into something different until the result is shown on the lamp panel. If you are interested to know exactly how the translation process works, you should remove jumper ⑤ from **J1**. With this jumper removed, the **Enigma-E** will slow down and show you each permutation as and when it happens.

Here's an example. Turn on the **Enigma-E**. It is assumed that you still have the Enigma setup for the message of paragraph 3.6. Once the startup procedure has completed, the display should show **AMZI**. Now press and hold down the letter **Q**. The following sequence will now be shown:

<--Q	You have pressed the letter Q on the keyboard,
STCR	this is passed through the Steckerbrett...
<--Q	...and translated into a Q (as there is no stecker in place for the letter Q).
<--Z	The first wheel translates the Q into a Z.
<--C	The second wheel translates the Z into a C.
<--L	The third wheel translates the C into an L
<--B	The greek wheel translates the L into a B.
UKWC	The B now enters the Umkehrwalze...
D-->	...which translates the B into a D.
Z-->	The greek wheel translates the D into a Z.
T-->	The third wheel translates the Z into a T.
P-->	The second wheel translates the T into a P.
U-->	The first wheel translates the P into a U.
STCR	The U is now passed through the Steckerbrett again...
B-->	...and translated into a B

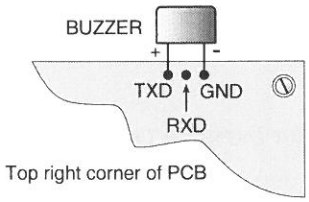
Finally, **B** will be lit on the lamp panel and the display shows **AMZJ**

As the ETW (Eintrittswalze) is connected in a linear fashion (A, B, C, D...Z) it is left out of the equasion. The arrows show the direction of the electric current. When a key is pressed, the current flows from right to left, until it hits the UKW (Umkehrwalze) where it is *reflected* back into the wheels. Next the current flows from left to right until it turns on a lamp on the lamp panel. Refer to chapter 6 for a detailed description of the working principle of the Enigma.

3.9 Using morse code

During WWII the German army used morse code to transmit messages across the world. If you want to know how this sounds, you might want to explore the built-in morse generator of your **Enigma-E**. Please note that you cannot use the buzzer on the main PCB for this. If you want to hear the morse code, you need to connect another (optional) buzzer to the terminals of the serial port (in the top right corner of the board). Also, note that jumper ② should be removed.

The extra buzzer should be connected to the serial port as follows:



The plus terminal of the buzzer (the longest leg) should be connected to the leftmost terminal of the serial port (TXD). The other leg of the buzzer (minus) should be connect to the rightmost terminal of the serial port (marked GND). Once morse is enabled (i.e. jumper ② is removed) the serial port cannot be used for communication with a PC.

As the TXD line is an open-collector output, you may drive e.g. a Short Wave SSB transceiver directly and transmit your morse code.

If you want to find a suitable buzzer for the morse code, look for a model similar to the one supplied with your **Enigma-E** building kit (i.e. the one mounted next to the keyboard). This should be a buzzer with some built-in electronics, so that it generates a sound when a 5 Volt DC voltage is applied to it.

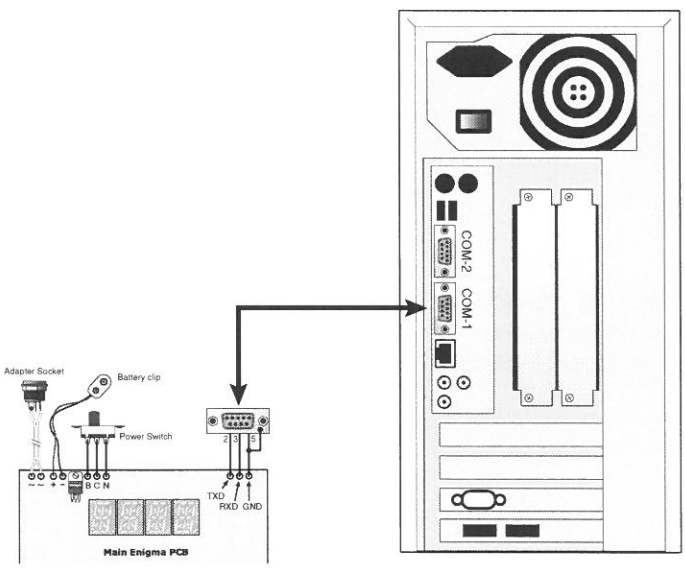
3.10 Using the serial port

Your **Enigma-E** is equiped with a serial port which greatly enhances the possibilities of your kit. First of all, the serial port can be configured to drive a buzzer, as described in the previous paragraph. Secondly, you may use it as a true RS232 serial port, by putting Jumper 2 in place. Please note that the morse capability is now disabled.

Once jumper ② is fitted, the serial port is activated, using the following specifications:

Baudrate	**9600 baud**
Data format	**8N1**
Handshaking	**none**

You may now connect a serial cable to the PCB, as described in the wiring diagram in paragraph 2.6
The other end of the serial cable may be connected to a another **Enigma-E** or directly to a PC.



At the PC end, any standard terminal emulation program can be used, such as HyperTerminal for Windows. Any text typed on your **Enigma-E**, will appear enciphered on the PC and vice versa.

Users of a RISC OS computer, may use the software Enigma Simulator, available from our website, which has built-in serial port capability. Users of other platforms are advised to check our website for suitable software.

4. Circuit Description

This chapter explains how the **Enigma-E** circuitry works. Each part of the hardware is described below and you may want to fold out the circuit diagram that came with the kit (Appendix A).

4.1 Power Supply

All electronic parts inside the **Enigma-E** are powered at 5V. This has to be a rather stable power source. There are two possible ways to provide this power:

Using a battery

If you want to use your **Enigma-E** in a portable environment, you may want to connect a battery to the unit. A battery can be connected directly to the PCB at terminals **TWP1** and **TWP2**. Please ensure that power is higher than 8V. Although it's possible to use a standard 9V battery, a small dry rechargable 12V battery is preferred as it will last longer and can be recharged too.

Using a power adapter

If you're using the **Enigma-E** at home, an external power supply is recommended. This is probably the only thing that is not contained in the DIY kit. The reason for this is that safetly regulations and mains voltage are different for each country. Please source a power adapter locally or use one of the power adapters you are likely to have at home. The voltage of the adapter is not critical; any DC adapter between 9V and 12V can be used. If you want to use an AC adapter, please note that the voltage needs to be between 12V and 15V. The power consumption of the **Enigma-E** is below 100mA, so even the smallest adapter will do.

You may also want to connect an on/off switch between the power source and the **Enigma-E** PCB. This way you can turn the unit off when you're not using it. Alternatively, you can use a two way switch, so that you can choose between the battery and the power supply. The power switch should be connected to terminals **TWP5**, **TWP6** and **TWP7**. A suitable switch is supplied with the kit.

As the PCB contains a bridge rectifier, you may connect the AC or DC power source either way, which means that if you accidently swap the (+) and (-) terminals, you won't damage your **Enigma-E**. The PCB also contains a **7805** power stabiliser, which converts the external power source to a stable 5V level. All circuitry of the **Enigma-E** is connected to this 5V rail.

4.2 Micro controller

At the heart of the **Enigma-E** is a small RISC micro controller. This little beast controls just about everything that your **Enigma-E** is capable of. The micro controller we've used for this design is a PIC16F873; a well known member of the famous Microchip PIC family. From now on, we'll refer to this chip as the 'PIC'. For it's operation, the PIC needs a 4MHz high frequency signal, which is provided by the ceramic resonator **RES1**. The PIC can execute instructions at a quarter of this speed, which means it can do 1 million instructions per second! All software is held in the non-volatile memory inside the PIC. It contains the mathematical algorithms for the encryption, the permutation tables for all wheels, the wheel wiring, setup procedure, selection of wheels, etc. But that's not all. The PIC also scans the keyboard, the Stecker board and the alpha-numerical displays.

4.3 Serial port

You may connect your **Enigma-E** to the outside world by using the on-board serial port. This is a standard RS232 interface, build around two transistors **T5** and **T6**. When a PC or laptop is connected, a negative voltage will be present at the RX line (**TWP9**). As soon as information is sent by the PC, positive pulses will be received on this line. Transistor **TR6**, converts these positive pulses into negative ones. These pulses are then fed to pin 18 of the PIC. The **Enigma-E** can also send data to the PC. In this case, the serial port will 'steal' the required negative voltage, from **TWP9** through diode **D41**. Resistor **R25** is used to charge capacitor **C29**. This way we have buffered the negative voltage in order to send data from the **Enigma-E**.

When the **Enigma-E** is tranmitting, the PIC will produce negative pulses which will cause **T5** to open, raising the voltage at **TWP8**. For this, it uses -via **R23**- the charge stored in **C29**.

For the technically minded: the serial port operates at a speed of 9600 baud, the data protocol is 8N1 (8-bits, no parity and 1 stop-bit) and no handshaking is used. If you want to use the serial port, an optional 9-pin sub-D female socket should be connected to terminals **TWP8**, **TWP9** and **TWP10**. Alternatively you may use these terminals to connect a buzzer, so that the encrypted text is converted into morse code as you type. For this you need an extra buzzer (not supplied in the kit). Additional information can be found in the following paragraphs: 2.6 (Wiring Diagram), 3.8 (Using morse code) and 3.9 (Using the Serial Port).

4.4 Buzzer

T7 also drives the buzzer, which is used to 'simulate' the key-click sound of the Enigma. Of course, the buzzer is far too small to generate the real key-clunck as can be experienced on a real Enigma. The buzzer may be turned off temporarily by placing jumper ① on header **J1**.

4.5 Steckerbrett

The Stecker board can be explained best as a matrix. HEF4094 ICs are used to convert a serial signal from the PIC into a series of outputs. A HEF4021 is used to do the opposite: it converts inputs into a serial signal that can be read by the PIC. The software inside the PIC plays a crucial role here. Pins 12, 23 and 24 of the PIC carry the signals to drive the HEF4094s. The PIC will now drive the HEF4094s in such a way, that only a single output will be active at any one time. All other outputs of the four ICs will stay low. Next, the PIC reads, via pin 23, 13 and 7, the inputs of the HEF4021 ICs, one by one.

If only a single match is found, the letter is not 'Steckered'. However, if another match is found, the letter is assumed to be swapped with the letter corresponding to that input. In its memory, the PIC builds a table of all known connections. This technique is called 'scanning' and has the advantage that only single wires are needed to create the patch cables. Scanning the Steckerbrett is done in the background and is so fast, that any changes are spotted by the software immediately.

The Steckerbrett is a separate part of the PCB and can be removed. Without the Steckerbrett, the **Enigma-E** can be used as normal. However, the extra permutations introduced by the Steckerbrett will be lost, and you won't be able to use the jumpers.

4.6 Displays

The **Enigma-E** caries four large alpha-numerical LED displays. These displays replace the mechanical wheels (Walze) of a real Enigma. **IC1** and **IC2** are two HEF4094s. Each output of these ICs is connected to a single segment of these displays. The PIC scans **T1**, **T2**, **T3** and **T4** and drives the LED displays one-by-one. This technique is called 'multiplexing' and it happens so fast, that the human eye can't see it.

4.7 Lamp panel

At the centre of the PCB are the 26 LEDs that simulate the 26 lamps of a real Enigma. All LEDs are connected in a matrix, just like on the Steckerbrett. Again HEF4094 ICs are used to muliplex the LEDs. Transistors **T1**, **T2**, **T3** and **T4** (also used for multiplexing the displays) allow the LEDs to be 'scanned' one group at a time. The configuration LEDs (mounted left of the displays) are also driven by these transistors.

4.8 Keyboard

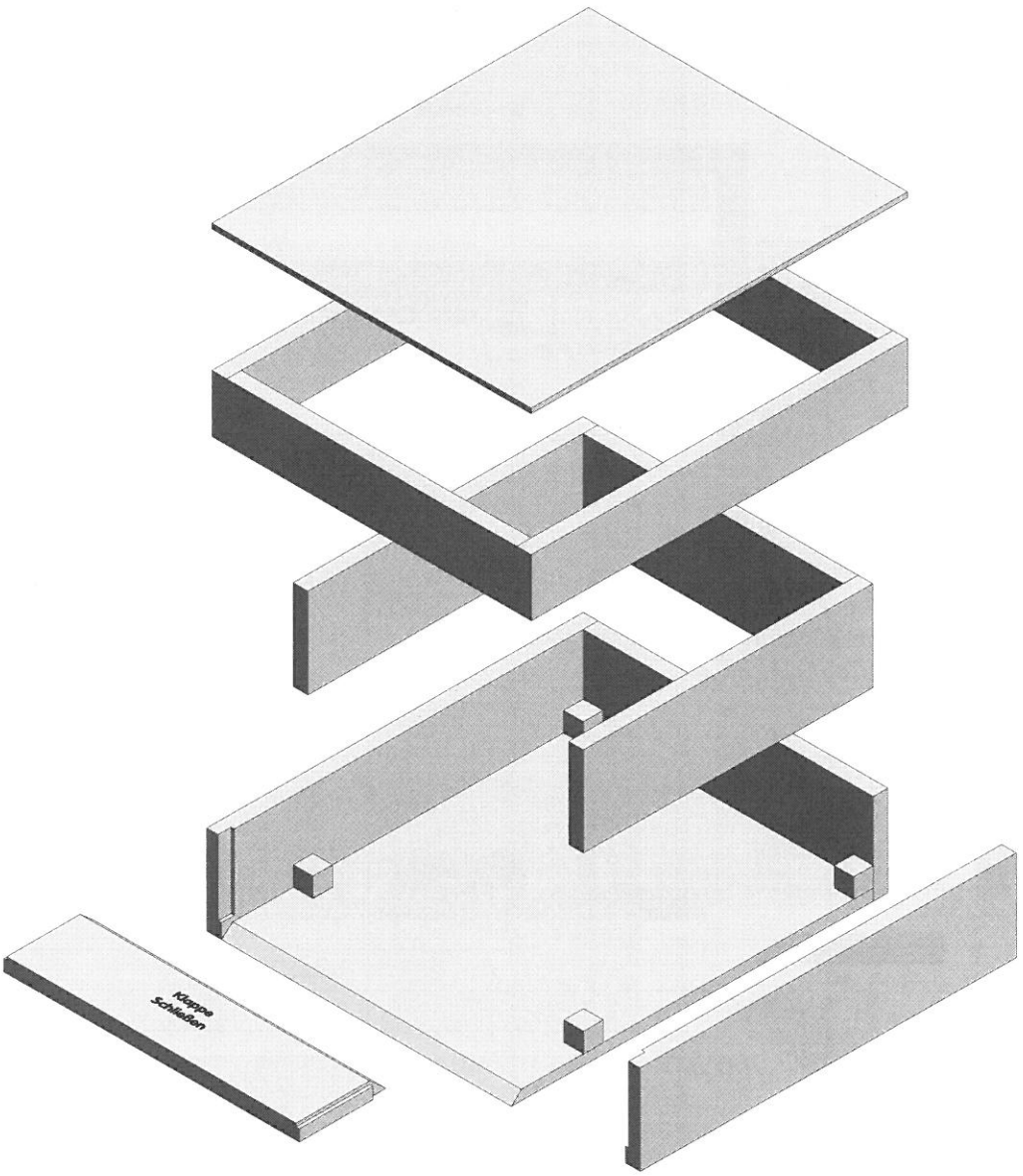
Like the lamp panel, the keyboard is divided into groups. The PIC drives a single HEF4094 (**IC4**), which in turn selects a group of four keys on the keyboard. The four signals **CharInt1...CharInt4** are directly read by the PIC. The up/down keys of the displays, are scanned at the same time. The input '**WheelInt**' of the PIC is used to read the state of these keys.

5. Design ideas

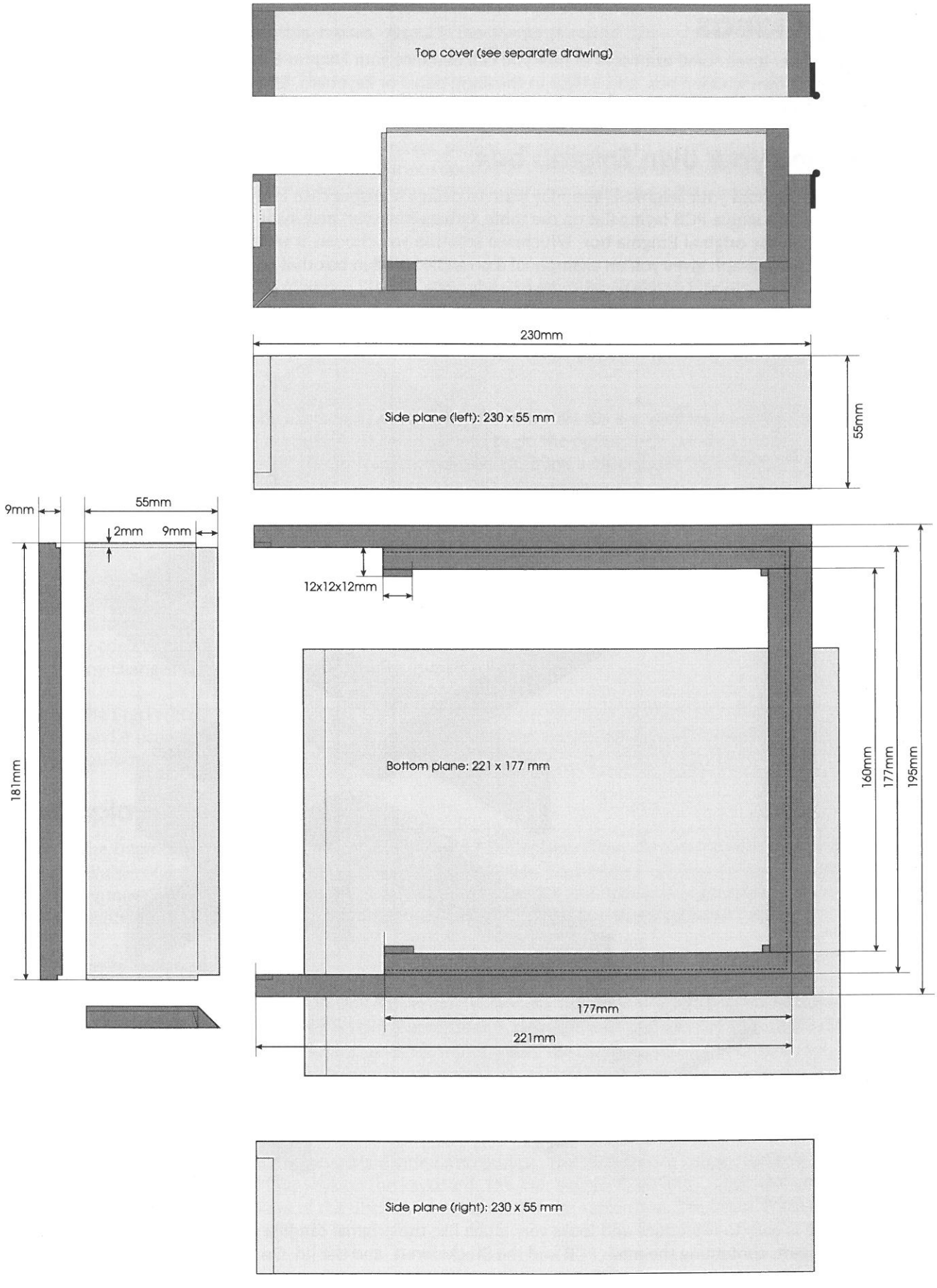
This chapter gives some examples of how you can enhance your **Enigma-E** building kit. You may want to build your own wooden box, add letters to the lamp panel or keyboard, add a serial port, etc. The latest overview of design ideas can always be found on the website.

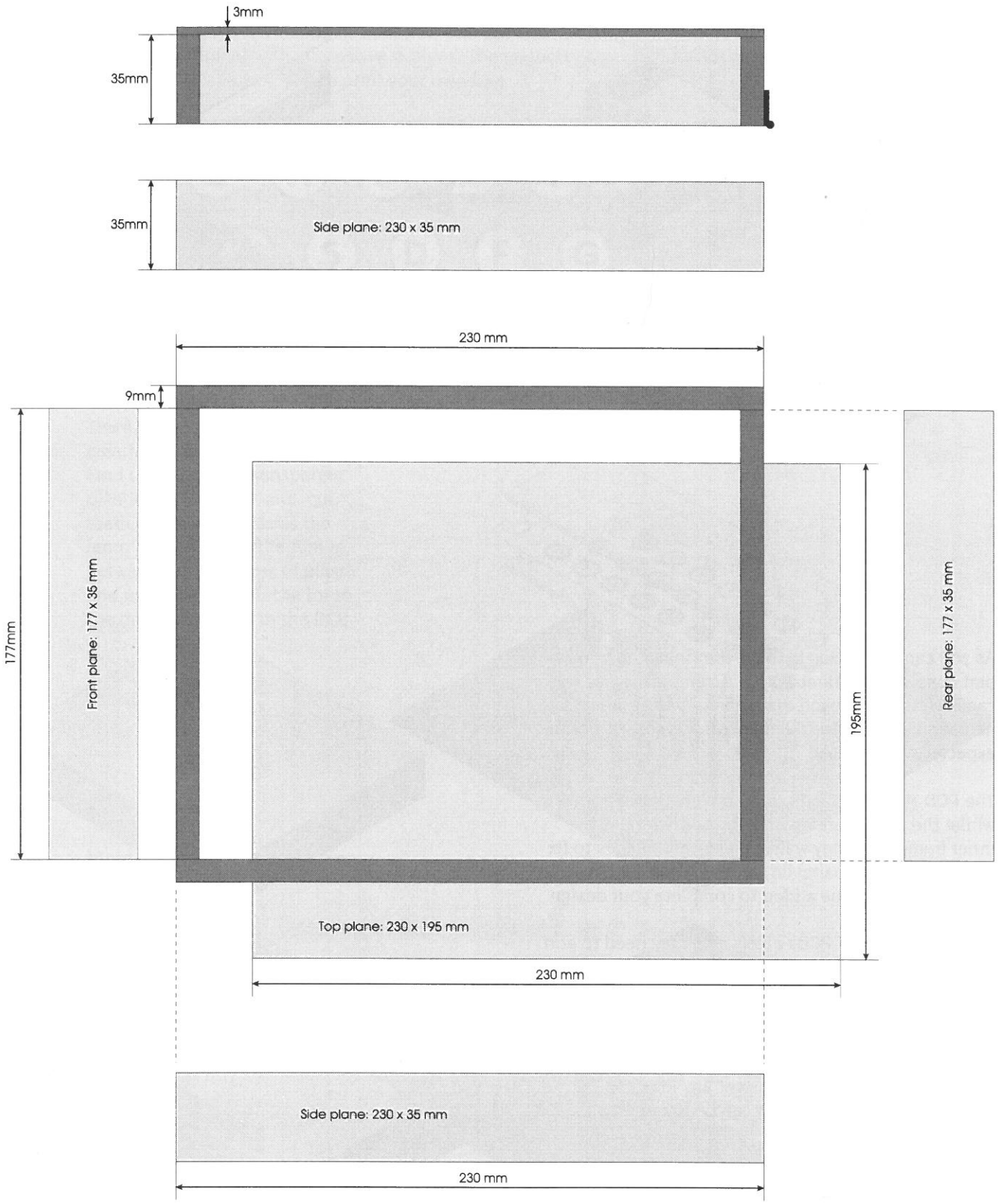
5.1 Designing your own Enigma box

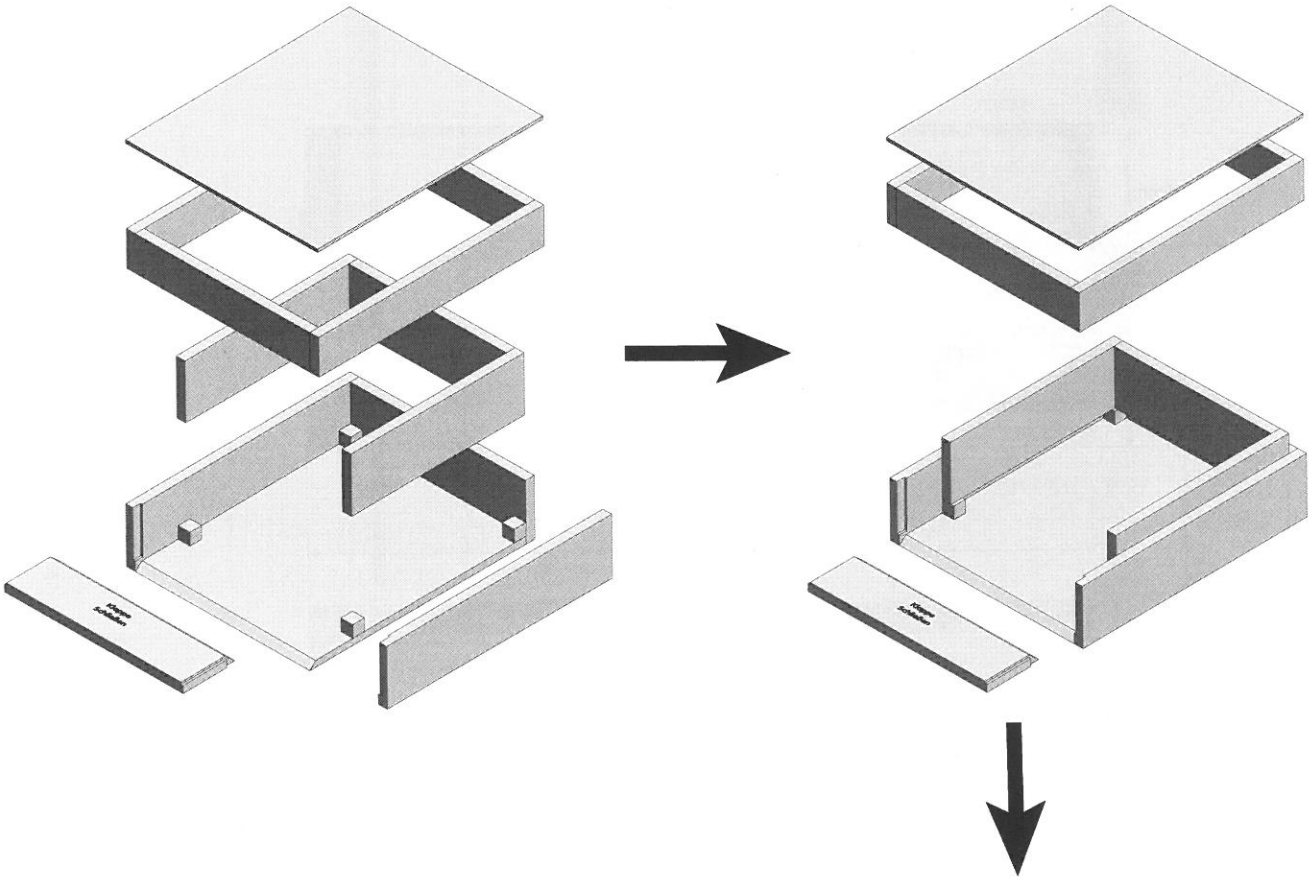
Once you've built your **Enigma-E**, you may want to design a proper case for it. Some people will prefer it the way it is: as a single PCB laying flat on the table. Others however, may want to create, say, a wooden case, resembling the original Enigma box. Whichever solution you choose, it will be your design. Just as a rough idea, this paragraph gives you an example of a possible wooden box that you could build. Any other ideas are most welcome and if they prove to be reproducable, we will certainly put them on our website.



This one is easy to reproduce and looks very much like the original Enigma case. It consists of two parts: a bottom part, containing the main PCB and the Steckerbrett, and the lid. On the next pages you'll find the dimensions, in case you want to give it a go.


Top cover (see separate drawing)
230mm
Side plane (left): 230 x 55 mm
55mm
9mm
55mm
2mm
9mm
181mm
12x12x12mm
Bottom plane: 221 x 177 mm
160mm
177mm
195mm
177mm
221mm
Side plane (right): 230 x 55 mm


3mm
35mm
35mm
Side plane: 230 x 35 mm
230 mm
9mm
177mm
Front plane: 177 x 35 mm
195mm
Rear plane: 177 x 35 mm
Top plane: 230 x 195 mm
230 mm
Side plane: 230 x 35 mm
230 mm

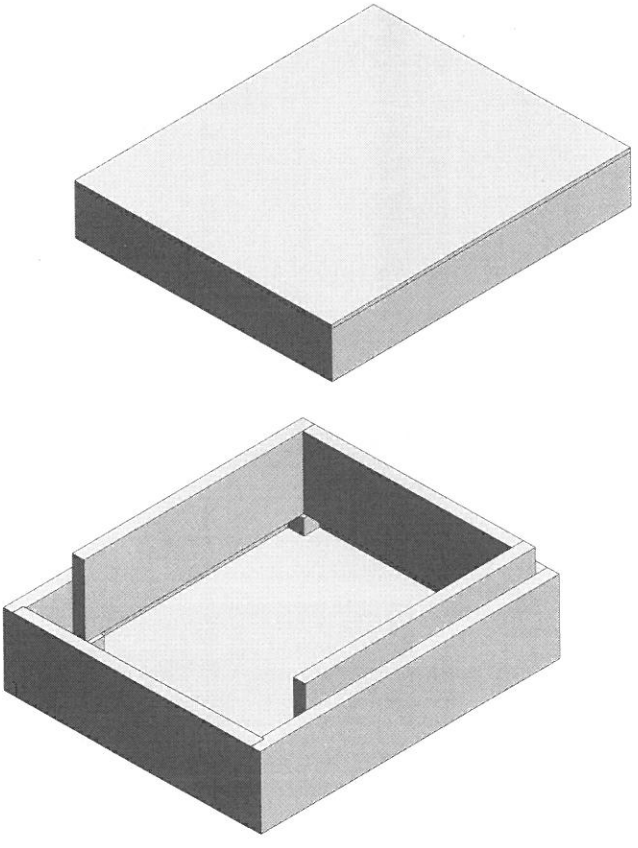


As you can clearly see in these drawings, the bottom part consists of a frame within a frame. This way we can use standard wood dimensions, whilst it also helps to keep the overall height of the box within the expected aspect ratio.

The PCB should be fitted on top of the inner frame, whilst the Steckerbrett will go on the front of the inner frame. You may want to use small hinges to fix the Klappe (front panel lid) and the top cover. A suitable lock may be added to complete your design.

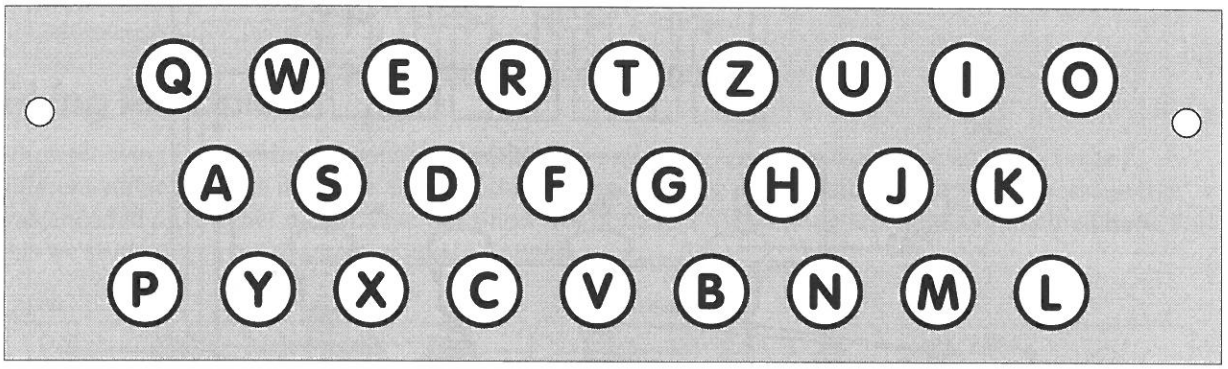
In order to fit both PCBs nicely, you may need to add extra supporting wooden strips and wedges. Please refer to the website for some detailed images.

If you've managed to design and build your own case, please let us know. We would very much like to learn about other designs and present any ideas on our website. Our e-mail address can be found on page 2.

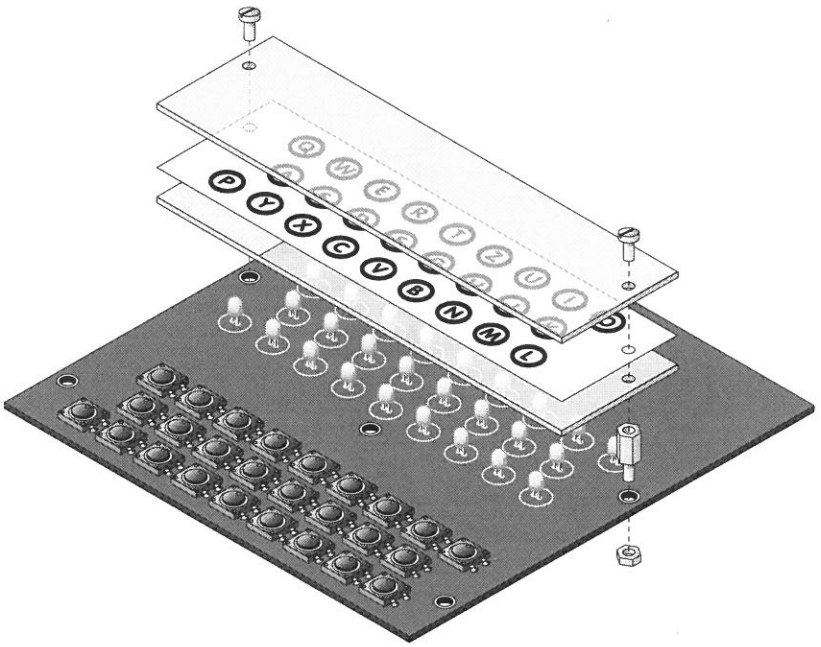


5.2 Improving the lamp panel

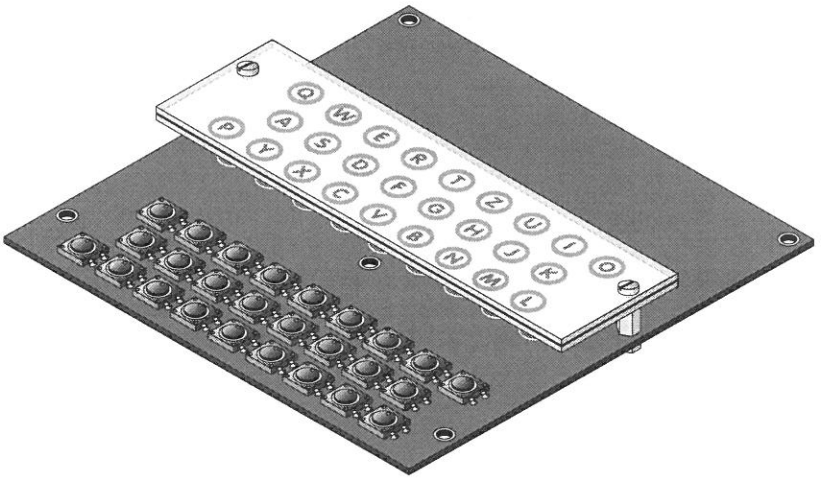
The LEDs on the lamp panel are rather small and it may be difficult to read the letters printed on the PCB next to the LEDs. You may improve the readability by fitting a film, containg the 26 letter of the alphabet, over the LEDs. A suitable film is supplied with your kit (inside the back cover of the manual), but you may want to experiment with alternative designs. The support page on our website contains some letter designs for download, allowing you to print your own film.

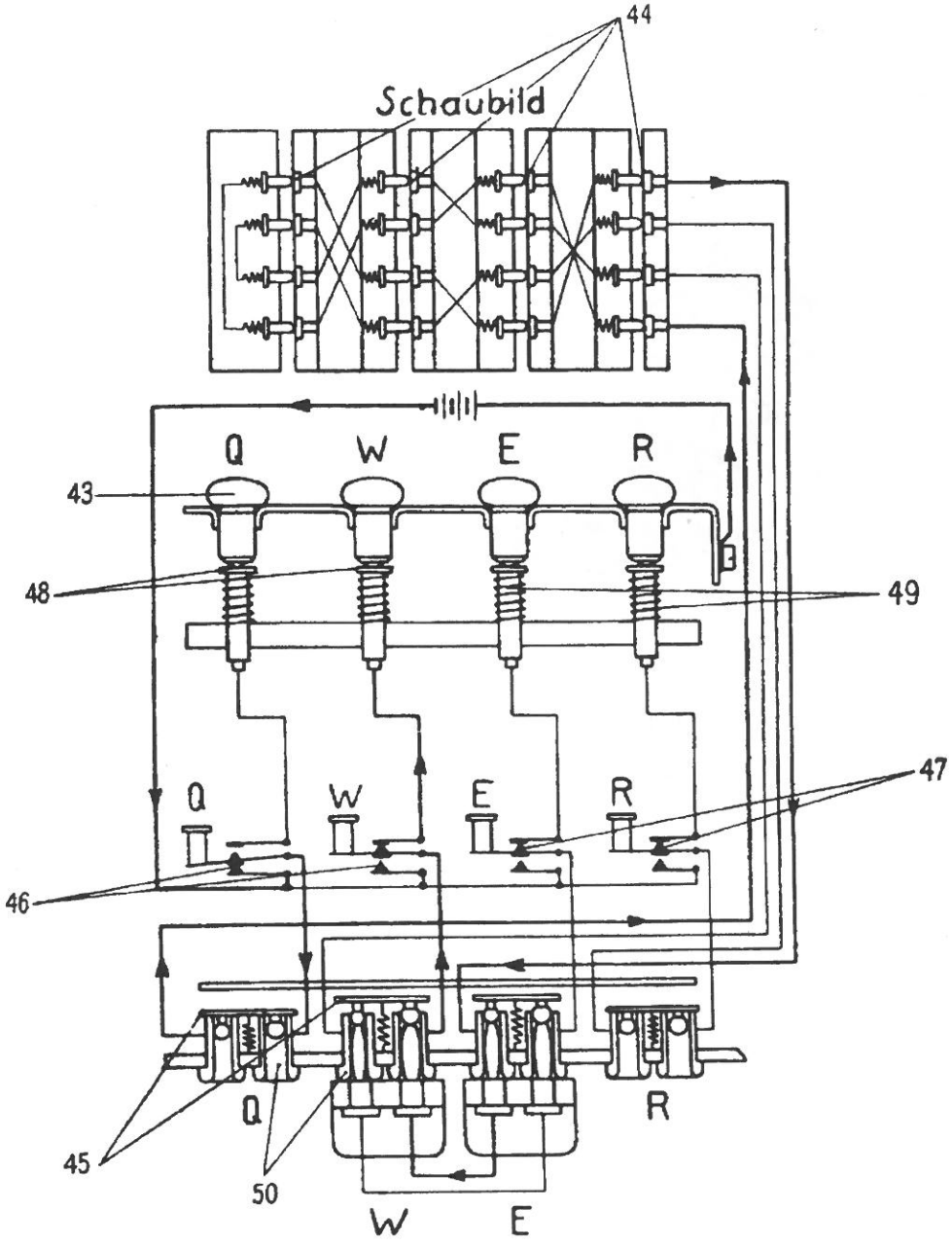


The film can be held in place, by creating a sandwich construction. Find two pieces of transparent plastic or plexiglass, and cut them to the same size as the lamp panel film. Fit the film in between the two pices of plastic and use spacers to fit the lot to the mounting holes in the PCB.



More examples are available on the **Enigma-E** website.





43 Glühlampen
44 Chiffr. Walzen-Kontakte
45 Kurzschlußbleche
46 Taſtkontakte (Arbeitskontakte)
47 Taſtkontakte (Ruhekontakte)
48 Lampenkontakte
49 Federnde Lampengegenkontakte
50 Buchſen im Steckerbrett

The above image was taken from the original Enigma manual and shows a simplified circuit diagram of the machine. The legend is given in the original German as well as in a suitable English translation.

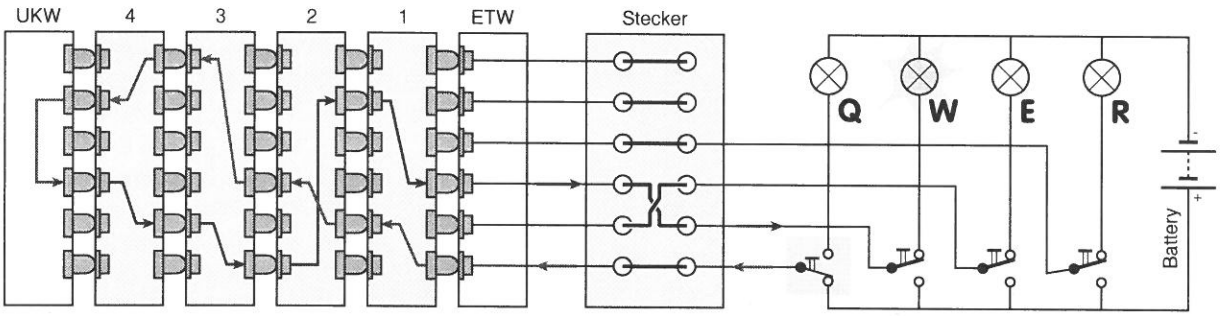
43	Glühlampen	*Lamps*
44	Chiffrier Walzen-Kontakte	*Coding wheel contacts*
45	Kurzschlußbleche	*Contact strip*
46	Tastkontakte (Arbeidskontakte)	*Key contact (closed)*
47	Tastkontakte (Ruhekontakte)	*Key contact (open)*
48	Lampenkontakte	*Lamp contact*
49	Federnde Lampengegenkontakte	*Spring loaded contacts*
50	Buchsen im Steckerbrett	*Sockets on the patch panel*

6. Working Principle of the Enigma

This is an attempt to describe the working principle of the Enigma. When developing our Enigma Simulator for RISC OS, we've searched the Internet and read many articles and books. Most articles give a rough description of the machine, but many important details, necessary to deduce the algorithm, are missing. This chapter describes the working principle of the Enigma machine in an easy to read manner. Any suggestions, that may help to clarify this matter further are most welcome. Please contact the authors at the address given on page 2.

6.1 Working Principle

When studying the working principle of the Enigma, we have to consider that there are in fact many different variants of this machine. Some of the differences make it impossible to decrypt a message that was encoded on another model. That does however not affect the working principle as explained here. For this we study the circuit diagram of an M4 Enigma.



Letters are 'scrambled' by a set of rotatable wheels each with 26 contacts on either side. Each contact on one side is connected (wired) to a contact on the other side in some random fashion. Some models, like the M3 have 3 such rotating wheels, but the M4 model, used later in the war during the U-boat war, has 4 wheels. Each time a key is pressed, the right most wheel is rotated by one step, resulting in a different mapping of the internal wires. A wheel has one or more notches that may cause the next wheel to be moved by one position too. This will result in a different encoding for each letter entered on the keyboard!

The keyboard consists of 26 keys, marked A-Z. Whenever a key, say '**Q**', is pressed the wheels will be moved into a new position and a contact is closed. As a result a current will flow. The wires from the 26 keys are connected to the Steckerbrett. The Steckerbrett may cause the letter to be swapped with another letter. The wires from the Steckerbrett are connected to a static wheel called the Stator or Eintrittswalze (ETW). The order in which the keys are connected to the 26 contacts on the ETW varies between the different Enigma models. In the diagram they are mapped in a linear fashion (i.e. A, B, C, etc.).

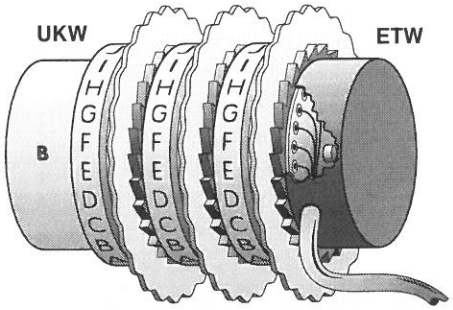
Leaving the ETW, the current enters the right most wheel (1) at the right hand side. The internal wiring of that wheel 'translates' this to one of the contacts of its left hand side, where it enters the next wheel, etc. Left of the rotating wheels is the Reflector, or Umkehrwalze (UKW). This wheel sends the current back into the rotating wheels, but this time the current flows from left to right, until it reaches the ETW again. From the ETW the current goes to the lamp board where the corresponding letter ('**W**' in the example) will be lit. It is inherent to this design, that a letter can never be encoded into itself.

Before starting the ciphering process, the Enigma needs to be setup in a way known by both sides. This means the wheel order (Walzenlage) needs to be known as well as the starting position of each wheel (Grundstellung). In order to further complicate things, each wheel has a settable index ring that moves the contacts independant of the wheel's alphabet. This is called the ring setting (Ringstellung).

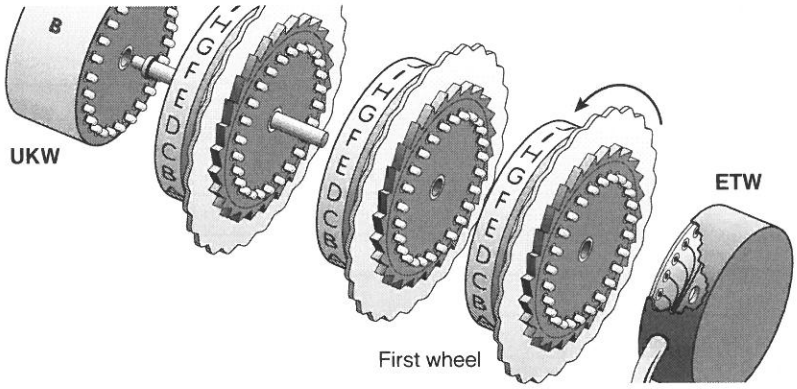
Due to the fact that the current flows through the wheels twice (once from right to left, then from left to right), the cipher process is reversable. This means that encoding a letter is exacly the same as decoding. In other words: if '**Q**' becomes '**W**', then '**W**' would become '**Q**' (with the same Enigma settings).

6.2 Wheel rotation in more detail

The mechanical part of the Enigma consists of the ETW (Eintrittswalze), 3 or 4 Walze (wheels) and the UKW (Umkehrwalze). The wheels are held in position by a rod, which also allows the wheels to rotate. The ETW contains 26 circular contacts, one for each letter of the alphabet. Each wheel contains 26 flat circular contacts on one side, and 26 spring-loaded contacts on the other side. The UKW contains only 26 spring-loaded contacts. When the wheels are in place and the UKW is engaged, it will look like this:



The UKW can be disengaged by pulling a lever. The rod, containing the 3 (or 4) wheels, can now be removed. Removing the wheels from the rod, clearly shows the spring-loaded contact. The ETW is shown here with part of its body 'removed' so that you can see how the internal wires are connected to the pads.



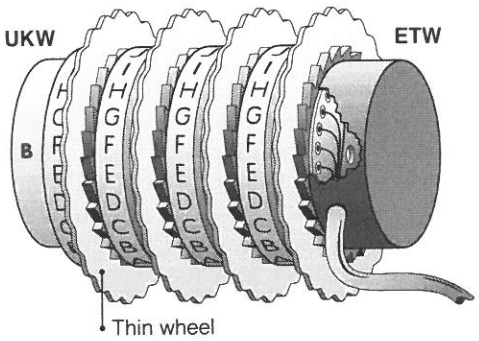
When a key is pressed, the wheels are moved into a new position, **before** the electrical contact is closed.

Pressing a key engages the transport mechanism, causing the first wheel to step by one position in counter clockwise direction (looking from the ETW).

A wheel contains one or more notches that may cause the next wheel to be stepped as well, etc. This is done to ensure a unique coding for each letter pressed, without generating a repeating pattern. The last wheel, just before the UKW, makes the fewest steps and is therefore often called the 'slow wheel'.

Each wheel has 26 positions that we will call A-Z. The index on the wheels is engraved (either as A-Z or 1-26) along the side of the wheel. The wheels are rotated counter clockwise, when viewed from the ETW. If **A** was visible in the window, the letter **B** will be visible next time the wheel is moved. Each wheel has a ring that can be used to rotate the wiring independant from the index. This can be regarded as creating an offset in the opposite direction. The notches are fixed to the index. Therefore the turnover of the next wheel, will always happen at the same letter in the window.

In Janury 1942, the German Navy introduced the Enigma M4 featuring an extra wheel. The design of the M4 was based on a 'modified' M3, so that existing parts could be used. As the same case was used, the 4 wheels had to be fitted in the space previously used for 3 wheels. This was done by replacing the existing UKW by a much smaller one, which provided space for an extra coding wheel. As the remaining space wasn't sufficient for a standard coding wheel, a **thin** wheel was designed to sit next to the UKW. For this reason the 4th wheel cannot be swapped with the other three wheels. When mounted together, all four wheels and the UKW would fit in the same space as before.



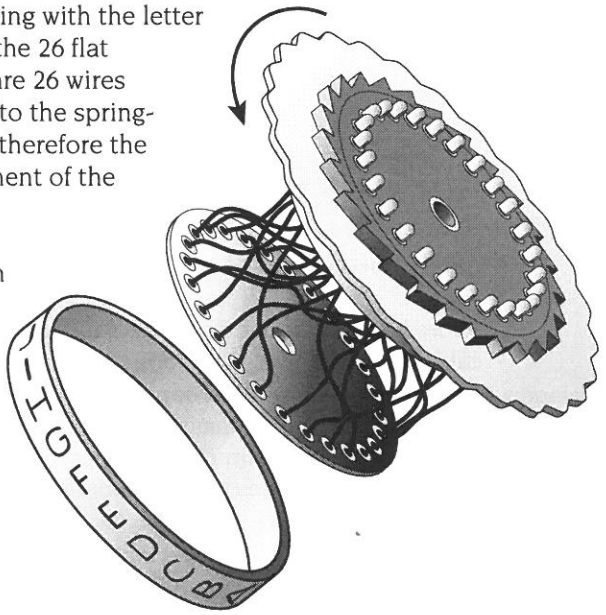
Two variants of the 4th wheel were available, called **Beta** and **Gamma**, one for each UKW (**B** and **C**). The 4th wheel is never moved by any of the other wheels and will stay in place for the duration of the cipher session. It can be set up in 26 positions which, in combination with the UKW, effectively creates 26 different UKWs.

The four wheel Enigma M4, was used exclusively by the U-boat section of the German Navy. In order to be able to exchange messages with other parts of the navy (or indeed other parts of the army), some level of compatibility had to be achieved. The UKW and 4th wheel were therefore wired in such a way that, when set to **A**, the machine would behave as an M3. So an **M4 UKB-B + Beta (set to A) = M3 UKW-B**. Of course the same is true for UKW C and the Gamma wheel. Extra complexity could be added to the M4 by using UKW-B in combination with the Gamma wheel and UKW-C in combination with Beta.

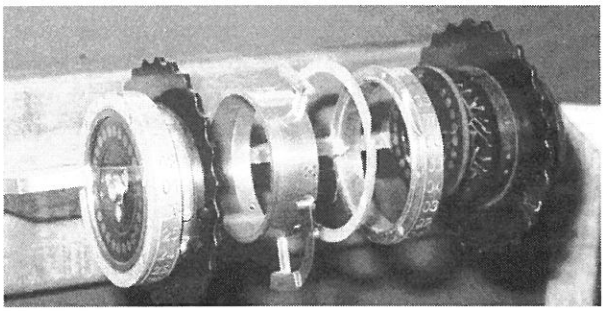
There are various names for the **4th wheel**. We've already called it the **thin wheel**, but it's also called the **Zusatzwalze** or, more commonly, the **Griechenwalze** (as the Greek symbols Beta and Gamma are used).

Most Enigma models are equipped with stepping levers and notches which, under certain circumstances, may cause the middle wheel to step twice on two sucessive key presses. The Enigma G series however, uses a transport mechanism similar to a gear box and does not suffer from the double stepping behaviour.

This drawing shows the interior of a coding wheel. The ring with the letter index has been removed and the circular plate holding the 26 flat contacts has been disassembled. As you can see there are 26 wires connecting the flat contacts from one side of the wheel to the spring-loaded contacts at the other side. The letter-index, and therefore the contact numbering, goes clockwise, whereas the movement of the wheel during encipherment is counter clockwise.



The image below shows two Enigma wheels. The one on the left is a fully assembled wheel. You can see the 26 flat circular contacts on the left hand side. The wheel on the right is shown in 'exploded view', which means you can see the interior. On the right hand side you can see the inner wiring of the wheel.



Exploded view of an Enigma wheel
Photo by Jerry Proc

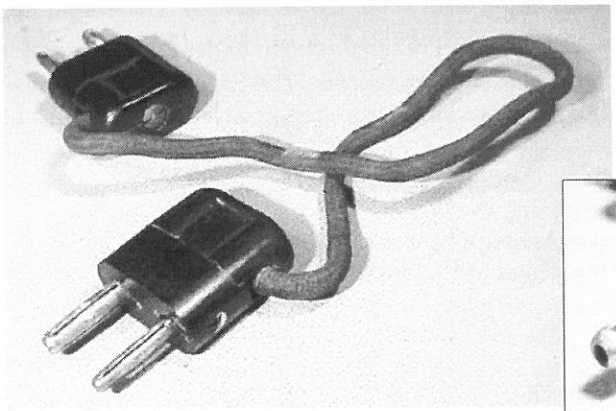
The Heeres Enigma (A models) were supplied with a set of 5 wheels, 3 of which could be used in any particular order. This would give 60 possible combinations (5 x 4 x 3). There are 17576 possible settings for the Grundstellung (26 x 26 x 26) and another 17576 settings for the Ringstellung.

The M3 had 3 extra wheels to pick from, so this would give 336 possible combinations (8 x 7 x 6).
The M4 was supplied with two 4th wheels: Beta and Gamma, which would double the number of wheel combinations to 672. In additions to the combinations for Grundstellung and Ringstellung, the 4th wheel can be set to 26 different positions.

On top of that, the Steckerbrett was added, which has even more combinations...

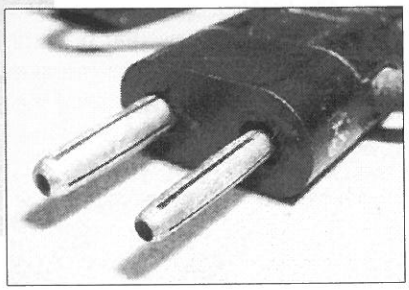
6.3 The Steckerbrett

The army variants of the Enigma (A, M3 and M4) were enhanced with a Steckerbrett (*plug board* or *patch panel*) that would allow any pair of letters to be swapped. If a patch cable was used between **G** and **P**, those two letters would be swapped. In other words: **G** would become **P** and **P** would become **G**. As the Steckerbrett is connected between the keyboard and the ETW, the encoded letter will go through stecker mappings twice. This would prevent a letter from being encoded into itself, which can be regarded as one of the weaknesses of the system. Nevertheless, the addition of the Steckerbrett greatly increased the number of possible permutations of the Enigma machine, making it much more secure than the commercial models.



A *real Enigma cable in close-up*

These pictures show a single patch cable of a real Enigma machine. To prevent a plug from being inserted the wrong way around, a thick and a thin pin were used. Two wires were used to cross-connect the pins of both plugs.



If no cable was used, the letter was known to be *Self-Steckered*. The diagram on page 38 shows how a contact in the socket is closed when the plug is removed.

As we have 26 characters, a theoretical maximum of 13 cables could be used. Note that any number of cables can be used, from none to 13, giving a much increased number of possible permutations. Most machines however, were supplied with only 11 cables. The reason for this is probably that the maximum number of permutations is reached when using 11 cables. Using more than 11 cables reduces, strangely enough, the maximum number of combinations. In order to understand this, we'll take a look at the mathematics behind the Steckerbrett. When using **n** cables, the maximum number of combinations is:

$$26! / (n! \cdot (26-2n)! \cdot 2^n)$$

The results are given in the table below.

Number of cables (n)	Combinations
0	1
1	325
2	44,850
3	3,453,450
4	164,038,875
5	5,019,589,575
6	100,391,791,500
7	1,305,093,290,000
8	10,767,019,640,000
9	53,835,098,190,000
10	150,738,274,900,000
11	205,552,193,100,000
12	102,776,096,500,000
13	7,905,853,580,550
0-13 cables	532,985,208,119,326

Source: Arthur O. Bauer

As you can see here, the maximum number of permutations is obtained when using 11 cables. In practice, the procedure was such that they would always use between 7 and 11 cables. According to the table this would mean a maximum number of combinations of:

422,197,679,120,000

This number has to be multiplied by the number of possible wheel orders and settings. For a Heeres Enigma (using 3 wheels from a set of 5) , this number has to be muliplied by 60 (Walzenlage) x 17,576 (Grundstellung), which results in:

445,232,784,600,000,000,000

For a U-boat M4, using 3 extra wheels and two thin wheels, this would be:

129,651,786,900,000,000,000,000

6.4 Differences in Enigma models

It has been stated before in this manual that the Enigma is not a single device, but a family of machines, each with their own characteristics. Because of these differences, a messages encoded on one Enigma variant, may not decode on another one. This paragraph describes the differences.

Steckerbrett

Some models have a plug panel and some don't. The theoretical maximum number of patch cables is 13 (as we have 26 letters), but the number of cables supplied with a unit varies. The highest number of permutations is achieved when using 11 patch cables (see paragraph 6.3) and the German Army would always use between 7 and 11 cables.

ETW mapping

The Eintrittswalze (ETW) is the static wheel (stator) to the right of the rightmost movable wheel. The way in which the keyboard is connected to the ETW differs between Enigma models. This often called the ETW *mapping* or ETW *permutation*. The ETW can be mapped in a linear fashion: ABCDEFGH... etc, but also in the order of the keys on the keyboard: QWERTZUIO... On the Japanese machine, the Tirpitz, the contacts of the ETW are organised in a random fashion: KZROUQHY...

Wheel wiring

Although the wiring for the first five wheels used by the German Army (I to V) was the same for all machines (A, M3 and M4), Other machines, such as the models used by the Abwehr, the Railway, Swiss Army and the commercial models, had a completely different wiring.

Number of different of wheels

Some models have 3 rotatable wheels, but the M4 has 4 wheels. Also some models have a range of wheels (e.g. 8) to choose from. The wheels may be placed in the machine in any particular order.

On an Enigma M4 (a 4 wheel machine), the extra wheel (Zusatswalze) is not moved automatically, but can be set manually to an initial position. Furthermore the extra wheel cannot be exchanged with the other three wheels as it is a 'thin' one. The 4th wheel was supplied as a pair with an UKW. For UKWs **B** and **C**, the extra wheels **Beta** and **Gamma** where supplied, hence the name *Griechenwalze* (Greek wheel). They may be used however in any combination. The 4th wheel on an *Abwehr* Enigma (G-series) is in fact the UKW and on this model it **is** moved by the other wheels, due to the mechanical differences in this machine.

UKW mapping and setting

Some models have more than one UKW available. On most models the UKW is fixed, but on some the UKW can be given a start position. Additionally, the G models have a movable UKW, which means that the wheel can be moved by the notches of the wheel next to it.

Number of notches on each wheel

In the basic situation, each wheel has one notch which, after a full revolution, causes the next wheel to be stepped by one position. Some wheels however have two or even more notches, causing more frequent changeovers of the next wheel. The three wheels of the *Abwehr* Enigma have 11, 15 and 17 notches respectively.

Double stepping feature

As a result of the mechanical principle of the stepping mechanism, the middle rotor 'suffers' from a double stepping anomaly as described in a paper by David Hamer. The G models, which use a gear box instead, do not suffer from this double stepping behaviour.

Manufacturer

Before and during WWII, the Enigma machines were built by various manufacturers. Although these machines were mathematically compatible, there are a few cosmetic differences. Furthermore there are physical differences between the Griechenwalze (*thin* wheels) from some manufacturers.

7. Enigma History

7.1 What is an Enigma

According to the dictionary, Enigma means '**Riddle**', which is a perfect name for one of the most well known and mysterious devices. Enigma was used as the name for a coding machine, invented and sold by the German Arthur Scherbius as early as 1918.

The German army used the Enigma coding machine to encipher most of their radio messages before and during WWII (1926 - 1945). Thousands of messages were sent each day to and from the many departments of the German Army all over the world and the device was considered **unbreakable**.

The Enigma is an electro-mechanical device using a system of wired wheels, a keyboard and lamps to encode and decode textual messages. The device contained 26 keys; one for each letter in the alphabet. Numbers and special characters, such as comma, space and question mark, were missing, so they had to be spelled in full. A full description of the working principle of the Enigma can be found in chapter 6.

Whenever a German officer wanted to send a message to his superiors, he would first have to write the message in plain text. The message was then enciphered by a **cipher clerk**. Any spaces were replaced by the letter **X** (as it is hardly used in the German language) and the end of line (i.e. a full stop) was sometimes replaced by **XX**. The cipher clerk would then take the encoded message to the radio operator, who would use telegraphy (i.e. morse code) to broadcast his message. The Enigma was a portable device, contained in a wooden box, with a built-in battery, so that it could be used in the field.

7.2 Bletchley Park

As stated before, the Germans considered their Enigma machine to be unbreakable. This was laregely due to the fact that it was such a complex device with an immense number of possible combinations. Each day, a different setting of the Enigma was used and even if the enemy would capture an Enigma, it would take years to try all possible combinations, by which time the message would have lost its value.

However, history has proved them wrong. In the years before WWII, a few brilliant Polish mathematicians, managed to break into the Enigma traffic, without ever having seen an Enigma. As the war was imminent, the Poles knew that the Germans would soon invade Poland. They then gave away all of their knowlege, including some Enigma replicas, to the French and British intelligence departments. The British, already interested in the Enigma radio traffic, setup a truely secret service in a quiet part of the country, just outside Milton Keynes: Bletchley Park. It is here where most of the German Enigma messages were broken throughout the war.

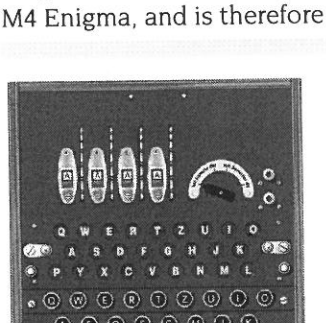
In the years after the war, Bletchley Park was used by the GC&CS (the Government Code and Cipher School) and subsequently GCHQ (Government Communications Headquarters) until it was abandoned in 1991, facing demolition...

Bletchley Park is now a museum where the full history of the Enigma and many other interesing WWII aspects can be seen and touched. It is here, where our interest in the Enigma was born, eventually leading to the developement of the **Enigma-E**.

7.3 Enigma Variations

A lot has been said and written about **the** Enigma. However, when we speak about **the** Enigma, we have to realise that there are in fact many different flavours of Enigmae. First of all there was the commercial Enigma, available before the war, followed by the Army Service Enigma, the Naval Enigma, etc. Some variants of the Enigma are so different, that they are not 'compatible' with the other models. Furthermore, the wiring of the wheels may be different for certain models, despite the fact that the wheels have the same numbers.

This paragraph describes the various models and shows a small image of each of them, taken from our Enigma Simulator for RISC OS. Please note that your **Enigma-E** is is capable of emulating both an M3 and M4 Enigma, and is therefore also compatible with the standard Service machine (Heer).



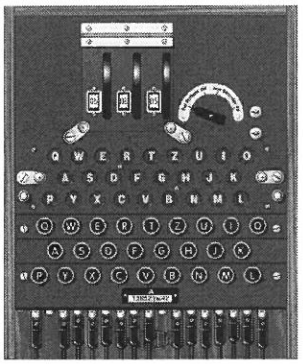
Commercial Enigma

The first Enigma to be available was the Commercial Enigma as it was originally introduced by its inventor Arthur Scherbius. It had three wheels and a settable UKW, hence the reason for having four letter windows. The first one became available in 1920 and it was withdrawn from the market in 1932, after the German Army took it over. Many different versions of the Commercial Enigma have been produced, such as the C, D and K models.

This is an example of an advert for a commercial Enigma coding machine as it appeared in a magazine before 1932.

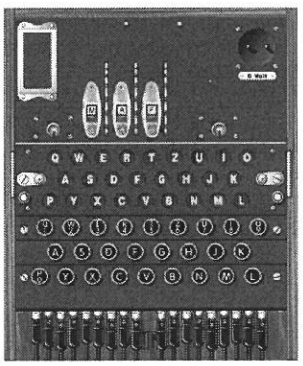
The machines below were used by the various parts of the German Army. The first one was used by the *Heer* and *Luftwaffe* and the other two models were in use by the Navy. Messages were interchangable between these three Enigma machines, provided that the same wheels were used. The Enigma setup procedure for the Navy however, was far more complex than the setup procedure for the other departments of the Army.

Although the M3 has three wheels, whereas the M4 has 4 wheels, messages could be exchanged. In such cases, the M4 would use UKW 'B' in combination with greek wheel 'Beta' or UKW 'C' with greek wheel 'Gamma'. Furthermore, care had to be taken, to ensure that the 4th wheel would not move during encipherment.



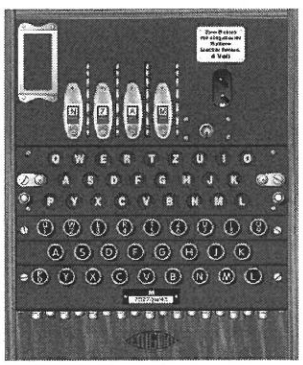
Heeres Enigma

After adoption of the Enigma by the German Army (Wehrmacht), some modifications were made. The wiring of the wheels was changed and new wheels were added. At the same time, a Steckerbrett (plugboard) was added, which added greatly to the complexity of the machine. This machine had numbers (1-26) on the wheels rather than letters (A-Z) and was used by the *Heer* and *Luftwaffe*. It was supplied with 5 wheels, any 3 of which could be used in any particular order. It also had a set of two UKWs (B and C), one of which could be used in combination with the other wheels.



M3 Naval Enigma

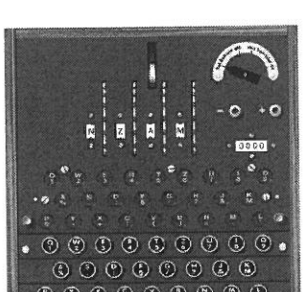
The German Navy (Kriegsmarine) used a slightly different variant of the *Heeres* Enigma. First of all, it had letters on the rotors rather than numbers and later in the war, three more wheels were added. The wiring of the first five wheels was the same as for the Heeres Enigma. The Naval Enigma was difficult to break, especially because of the very complex setup procedures employed by the German Navy.



M4 Naval Enigma

The M4 Enigma was probably the most difficult one of them all. It caused the codebreakers at Bletchley Park great problems, especially during the first part of the war. The M4 was used by the U-boat section of the German Navy and had an extra wheel. It is often referred to as a **4-wheel Enigma**. Basically, the machine is a modified M3 Enigma and the space for the extra wheel was taken from the UKW. The M4 therefore has a 'thin' UKW and a 'thin' 4th wheel, which is not interchangable with the other wheels. Two sets of UKW (B and C) and 4th wheel (Beta and Gamma) were available. The 4th wheel is often referred to as the **Greek Wheel** or *Griechenwalze*

The **Enigma-E** is capable of emulating these three Enigma variants.



Abwehr Enigma

This is probably the most rare Enigma in existence today. It was designed for the Abwehr (the German Intelligence Service) and its transport mechanism is completely different from the other Enigmae. It has no Steckerbrett, and it has only 3 wheels that could be placed in any particular order. The difficulty is however, that the wheels have more than one **notch**, therefore causing the wheel next to it to step more frequently. The wheels had 11, 15 and 17 notches respectively and it has a movable UKW, which means that the UKW is also rotated frequently during encyphering. The machine is also called **Enigma-G** or the **11-15-17** machine.

The interior of the Abwehr Enigma still looks brand new after all these years. On the left is the lever used to release the wheels. The counter at the top is used to keep track of the number of letters entered on the keyboard. The mechanism of this Enigma is similar to an odometer, unlike the other Enigma models.

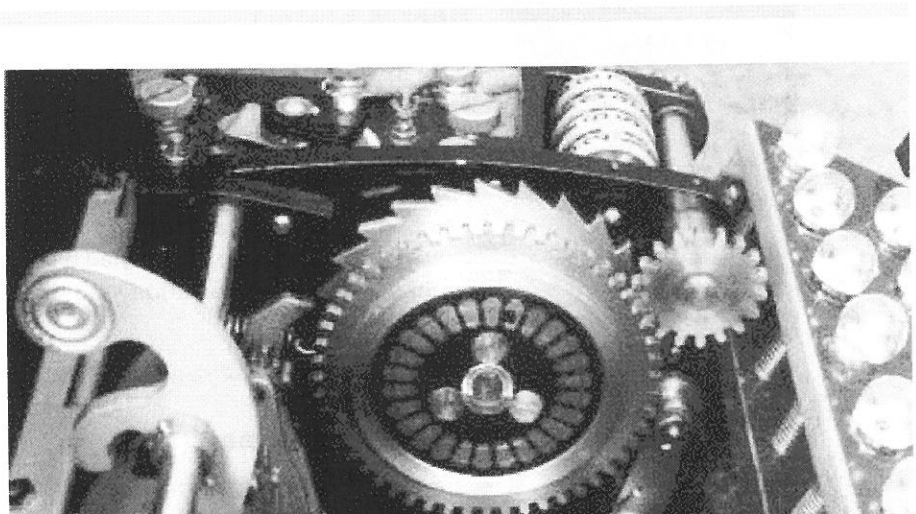
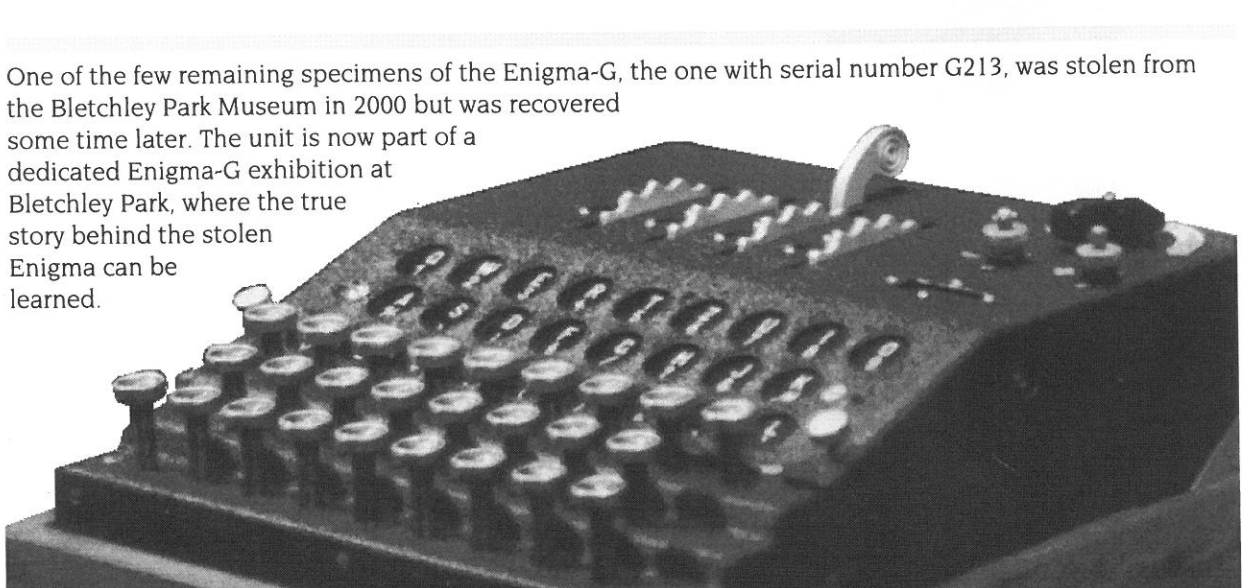
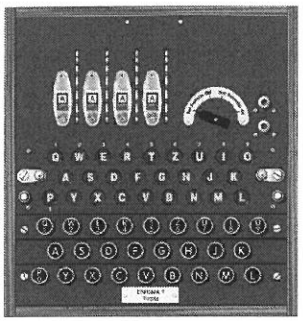


photo by **David Hamer**

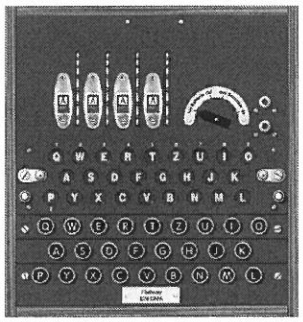
One of the few remaining specimens of the Enigma-G, the one with serial number G213, was stolen from the Bletchley Park Museum in 2000 but was recovered some time later. The unit is now part of a dedicated Enigma-G exhibition at Bletchley Park, where the true story behind the stolen Enigma can be learned.





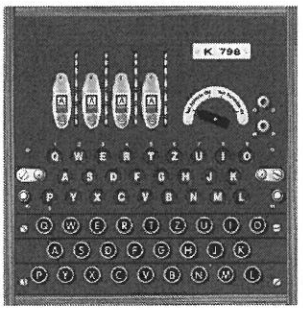
Tirpitz

The Japanese used different coding machines, such as **red** and **purple**, but at some point in the war, they ordered Enigma machines from the Germans. A special model was made for the Japanese: without a Steckerbrett and 3 wheels, from a set of 5. It was based on the commercial Enigma, but had different wiring. A large number of Tirpiz machines were captured by the allies during a raid on the French coast, where they were discovered in a warehouse waiting to be despatched to Japan.



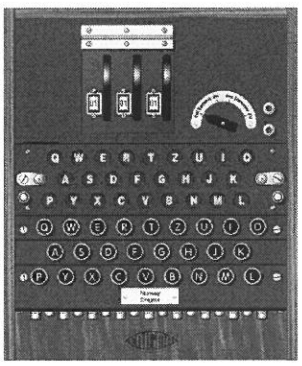
Railway Enigma

This is a rather strange variant of the Enigma as it has never been seen by anyone outside Germany and no machines have been recovered after the war. The machine was used by the German Reichsbahn (railway) and messages were first intercepted in 1940. Despite the fact that this machine was clearly based on a commercial Enigma, it was sometimes very diffucult to break.



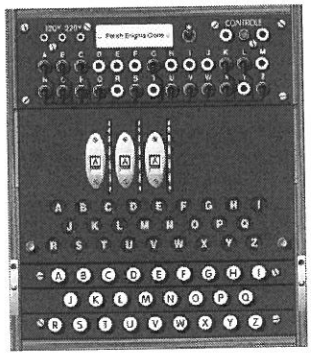
Swiss K

This machine was based on a Commercial Enigma K and was used by various parts of the Swiss Army. It has 3 wheels (from a set of 3) and a single notch on each wheel. As the Swiss didn't want their security to be compromised, they frequently changed the wiring of the wheels. Some Swiss-K models have an external lamp panel, that could be used by a second clerk. Some of these specimen are in remarkable good condition and can be seen in various museums around the world.



Norway Enigma

In the years following WWII, many Enigmae were used by Intelligence Agencies and armies all over Europe. The machine shown here was used by the Norwegian Police Special Brance for many years. It is based on the Heeres Enigma (standard Service model), but the wheels are wired differently. The name 'Norway Enigma' is just used to indicate the difference from a Heeres Enigma.



Polish Replica

This machine was designed and built by Polish cryptographers just before the war, after they first broke the Enigma ciphers. The replica was used to decode messages once the key was broken. The Poles gave away some of these replicas to the French and British Intelligence Services just before Germany invaded Poland in 1939. Note that the Steckerbrett is above the wheels rather than on the front of the machine.

This is the only remaining specimen of the Polish Enigma clone, which is now held at the Sikorski Institute in London. It was built by French technicians between 1939 and 1942

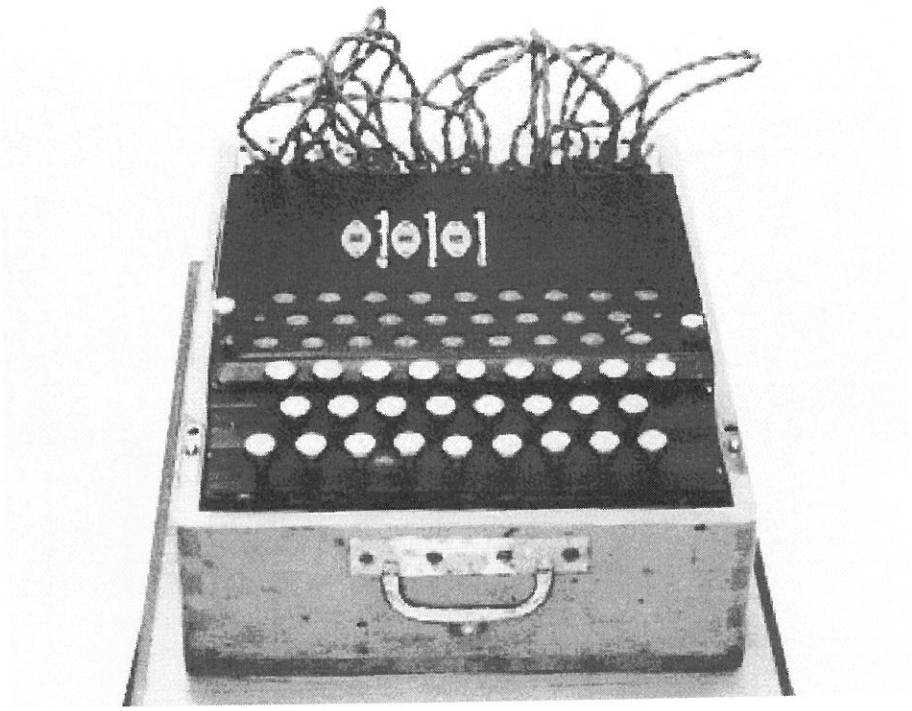


Photo by **David Hamer**

7.4 The Enigma Timeline

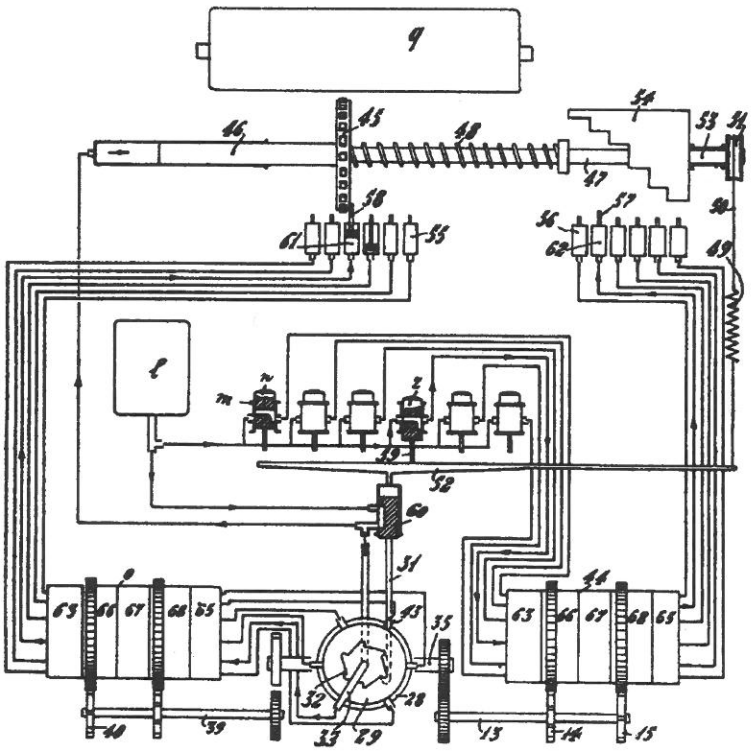
This paragraph describes the full history of the Enigma. Rather than attempting to be complete, it is meant to give you a global impression of the development and use of this coding machine. Although most dates and events are believed to be correct, this cannot be guaranteed. If you find any inconsistencies, please let us know.

1915 Invention of the Rotor Machine

Until recently it was believed that the Enigma, or the Rotor machine in general, was invented by either Arthur Scherbius in Germany (1918) or Hugo Koch in The Netherlands (1919). Both Koch and Scherbius held a number of patents involving an Enigma-like device, and shared a common interest in Koch's Amsterdam based company Securitas.

However, an article by Karl de Leeuw in the Cryptologia issue of January 2003, has revealed that the rotor machine was in fact invented in 1915 by two Dutch navy officers, R.P.C. Sprengler and Th. van Hengel. They developed the machine during their work for the Navy Department in the Dutch East Indies and a prototype was build and tested in the same year. Although Sprengler and Van Hengel initiated a patent application for the device, the Navy prevented them from doing so. They couldn't prevent the device from being patented, however, by Hugo Alexander Koch – an engineer and businessman working in close collaboration with Arthur Scherbius in Germany. Koch's patent application was handled by his brother-in-law, Huybrecht Verhagen, who was a patent attorney working at the firm that was also handling the patent application for the original inventors.

Although Sprengler and Van Hengel fought the granting of the patent to Koch, they were turned down by the Court of Appeal of the Patent Council in 1923, because they were unable to prove that they had been deceived by their patent attorneys. New evidence, however, discovered by Karl de Leeuw, has revealed foul play by their attorneys and challenges the objectivity of the chairman of the Patent Council, H. Bijleveld, who was minister of the navy during the period that Sprengler and Van Hengel invented their machine.

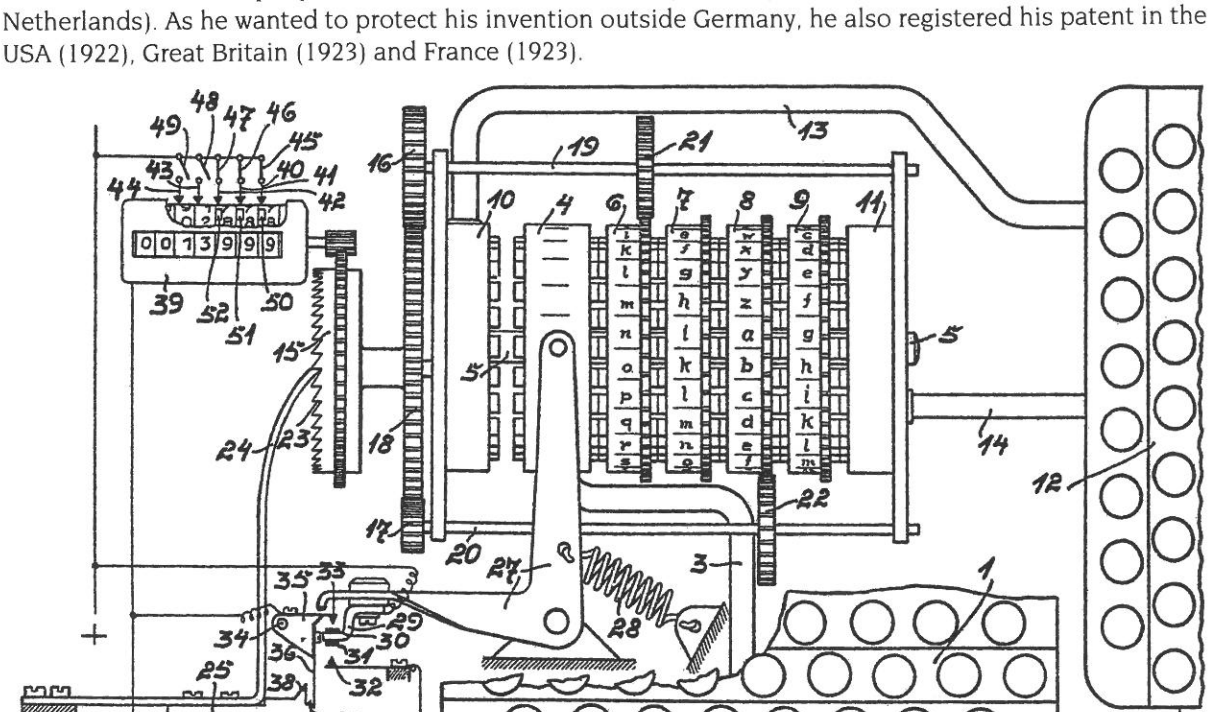


This drawing is part of patent 10700, submitted by Hugo Alexander Koch on 7 October 1919 in The Netherlands. The design clearly shows the use of coding wheels at the bottom. Separate wheels were used for coding and decoding and the device was capable of printing to paper directly.

1918 First Enigma Patent

The official history of the Enigma starts in 1918, when the German **Arthur Scherbius** filed his first patent for the Enigma coding machine. It is listed as patent number 416219 in the archives of the German *Reichspatentamt* (patent office). Please note the time at which the Enigma was invented: **1918**, just after the First World War, more then 20 years before WWII! The image below clearly shows the coding wheels (rotors) in the centre part of the drawing. Below it is the keyboard and to the right is the lamp panel. At the top left is a counter, used to count the number of letters entered on the keyboard. This counter can still be found on certain Enigma models.

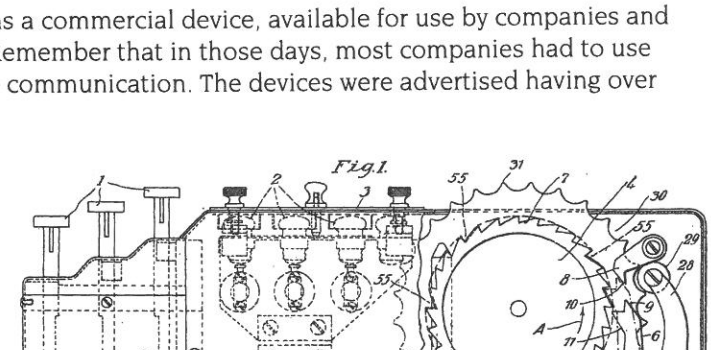
Arthur Scherbius' company **Securitas** was based in Berlin (Germany) and had an office in Amsterdam (The Netherlands). As he wanted to protect his invention outside Germany, he also registered his patent in the USA (1922), Great Britain (1923) and France (1923).



This image is taken from patent number 193,035 that was registered in Great Britain in 1923, long before WWII. It was also registered in a number of other countries, such as France and the USA.

During the 1920s the Enigma was available as a commercial device, available for use by companies and embassies for their confidential messages. Remember that in those days, most companies had to use morse code and radio links for long distance communication. The devices were advertised having over 800.000 possibilities.

In the following years, additional patents with improvements of the coding machine were applied. E.g. in GB Patent 267,482, dated 17 Jan 1927, the Umkehrwalze was added and a later patent of 14 Nov 1929 (GB 343,146) claims the addition of the Ringstellung, multiple notches, etc. One of the drawings of that patent shows a coding device, that we now know as The Enigma, in great detail.



1926 The German Army buys the Enigma rights

Initially, the German Army wasn't interested in Arthur Scherbius' invention and the Enigma had only a limited success as a commercial device. However, in 1926, with advanced plans for another war, security advisors managed to convice their superiors that this would be an ideal device to keep their radio messages secret.

Subsequently, the German Army bought the rights to the Enigma patents and the device remained commercially available until 1932. In order to improve security, the German Army made some important modifications to the Enigma. First of all, they changed the wiring of the wheels so that it would be unknown to an outside party. They also changed the Enigma setup procedure. This is the rather complex series of actions involved in preparing the Enigma for use.

But the most important change of all was probably the addition of a plugboard enabling the operator to swap any pair of letters. As the German word for 'Plug' is 'Stecker', this is often referred to as the *Stecker board*, or **Steckerbrett**. If no patch cable is present, there will be no swapping and the letter is known to be *self-Steckered*. If a cable was connected between, say, the **E** and **G**, this would mean that **E** would be translated into a **G** and **G** would be translated into **E**.

As there are 26 letters in the alphabet, a maximum of 13 cables could be used. However, it has been proven mathematically, that the maximum number of permutations is achieved when using 11 cables. The Steckerbrett added greatly to the complexity of the Engima, especially since any number of cables could be used, from none to 11 (or 13). It would multiply the number of possible combinations by:

532,985,208,200,000

1928 The Poles are interested

In 1928 the Polish secret service became interested in German radio traffic as they saw the danger of a pending war. The German Army already transmitted most of its radio messages in enciphered form, and the Poles wanted to know what this was all about.

1932 The British are interested

In 1932, British intelligence takes an interest in the German coded messages. One of their key military experts, Dylwyn Knox sets out to break the Enigma codes, but without success. However, due the increasing number of radio messages sent by the Germans each day, a new form of intelligence is developed: **Radio Intelligence**. Despite the fact that it was impossible to read the messages, the number of transmissions and the average location from which they were sent, gave valuable strategic information.

1933 The Poles break the Enigma

As stated before, the Poles were the first to recognise the possible danger of a war, and started to work on German ciphers in 1928. In 1932 they recruited three young billiant mathematics students of the University of Poznan: Marian Rejewski, Jerzy Rozycki and Henryk Zygalski. They began to work on the simpler German Naval codes first, until Rejewski was given a separate room and was told to work on Enigma traffic.

At the beginning of January 1933, Rejewski first broke the Enigma codes, based on a combination of mathematics, statistics, computational ability and inspired guesswork. He managed to deduce the full wiring details of each wheel and also determined the interdependance between the various parts of the Enigma, inluding the Steckerbrett. This enabled the Poles to produce replicas of the Enigma that were used to decode the German messages. Some time before, the Polish Intelligence Agency obtained the Enigma setup procedure from a French Secret Agent. From this moment on, the Poles were able to read most of the German radio traffic.

1934 Hitler becomes self-proclaimed Führer

The breakthrough by the Polish cryptographers came right on time as a few weeks later, 30 January 1933 to be exact, Hitler came to power as the new Reichs Chancellor of Germany. One year later, after the death of President Von Hindenburg, Hitler became the new self-proclamed Führer.

1938 The Poles keep breaking the Enigma

From the first breakthrough in January 1933, the Polish cryptographers could read almost all German Enigma radio traffic. In the period between 1934 and 1938 they noticed an enormous increase in radio traffic as Germany prepared to go to war again.

In March 1938 the German Army invaded and took over Austria, which then became part of the German Reich, the so called **Anschluβ**. The Poles, capable of reading most of the German Enigma messages, must have felt the increasing threat of a full scale war.

During this period, the German Army changed the Enigma again, by introducing a new radio procedure and two new wheels in addition to the existing three wheels. However, at this stage, the Germans only changed the Enigma settings once every month. In order to speed up the breaking of Enigma messages, the Polish cryptographers constructed an electro-mechanical machine, called the **Bomba**.

1939 The Poles give away their secrets

By mid 1939, the threat of an invasion reached its peak and on 24 July, the Poles invited the British and French Intelligence Services to Pyry, near Warsaw. At this meeting, the Polish cryptographers shared their knowledge with their foreign counterparts and handed over some Enigma Replicas. For the British, this was a great help which probably saved them some two to three years of research.

On 1 September 1939, Germany invaded Poland, which marks the beginning of WWII.

During the meeting in Pyry, the Poles gave away two Enigma replicas. When Germany invaded Poland, 15 Polish cryptographers fled to France where they continued their work until 1942 in the secret unit named **Bruno**. They ordered some more replicas to be made by French technicians. The only Polish Enigma Replica known to have survived the war, is held at the Sikorski Institute in London. An image of this machine can be found in paragraph 7.3.

Formation of Bletchley Park

As the threat of war loomed, the British Government Code and Cypher School (GC&CS), based in London, was looking for a safer more quiet place to carry out its intelligence work. They would find a private estate, called Bletchley Park that was suitable for their purposes. Bletchley would probably be safe in case of bomb raids and it had good road and train connections to London, The North, Cambridge and Oxford.

In August of 1939, just a week before Poland was invaded by the Germans, The first codebreakers arrived at Bletchley Park. In order to hide their true identity, they masqueraded as *Captain Ridley's Shooting Party*. Initially, a team of some 50 cryptographers started work at Bletchley Park. Among them, the now famous British mathematician Alan Turing.

England is at war

On 3 September, two days after the invasion of Poland, both France and Great Britain declare war on Germany. At the start of the war, the Germans again changed the Enigma setup procedure and from then on, they would change the Enigma settings on a daily basis.

In order to cope with the increasing number of radio messages, many listening stations, the so called **Y-stations** or *intercepts stations* were setup along the coast line. They were operated by radio hams, but also by house wives who were given an intensive training in reading morse code signals. Many house wives were

so good at this, that they could sometimes recognise the 'morse handwriting' of the German operator at the other end. Initially, Bletchley Park also was a listening station, identified as number 10, or in roman numbers: **X**, hence the name **Station X**.

Codename ULTRA

The whole operation at Bletchley Park was so secret, that it was only known to those who actually needed to know. As it was even more secret than *top secret*, they codenamed it **Ultra**. The importance of the Ultra Intelligence and the influence it had on the outcome of the war, has only become known in recent years. And still today, not all facts are out in the open...

1940 First successes at Bletchley Park

In the beginning of 1940, Alan Turing achieves his first breakthrough in breaking Enigma messages. More and more people are recruited to work at Bletchley Park to handle the enormous amount of messages each day. In order to speed up the breaking of Enigma traffic, Turing constructed his own variant of the Polish Bomba, called the **Bombe**.

During this period, Germany invaded Norway and France. At the same time, they introduced three more wheels to the Naval Enigma, giving a total of eight wheels. As each Enigma has three movable wheels, any three out of the total number of eight different wheels could be used, in any order. This would greatly increase the maximum number of permutations!

But that's not all. They soon discovered that the Enigma setup procedures used by the German Navy (Kriegsmarine) was far more complex than the procedure used by other departments of the army (*Heer* and *Luftwaffe*). Furthermore the Navy used code books for almost anything, even the weather report. Despite an occasional break of Naval traffic, the messages sent to and from the U-boats were completely unbreakable. This would keep the cryptographers at Bletchley Park puzzled for a long time to come.

Treatise on Enigma

In 1940, Alan Turing starts to write his Treatise on Enigma, a paper describing the ins and outs of the Enigma, both mechanically and mathematically. This paper has been unknown until its release by the NSA (National Security Agency) of the United States Government in April 1996. Turing must have written this document, sitting in a small room of **the cottage** at Bletchley Park.

At present, the full document of the Treatise on Enigma is held by the PRO (Public Record Office) and is Crown Copyright. However, you may download parts of it for private use, directly from the PRO website. See the links at the end of this chapter for more information.

1941 The Capture of U-110

Apart from writing his Treatise on Enigma, Turing spent most of his time in 1940 and 1941 on the Naval U-boat cyphers. All this time, most of the U-boat Enigma messages remained unbroken. All that changed with the capture of the German U-boat **U-110** on 9 May 1941 by the British HMS Bulldog. The U-boat was attacked with depth charges and was forced to the surface. The captain ordered his men to abandon ship, assuming that the boat would sink... However, the U-boat remained afloat, and the crew of the Bulldog managed to recover an Enigma and some secret documents, which later turned out to be code books. The code books were printed with special ink that would dissolve in water. The sinking of a U-boat would be enough to make the code books unusable. As the allies now had a code book, they had a clue as to what the contents of a message could be.

Breaking the U-boat codes was important as the U-boats sank many supply ships traveling from the USA to the UK every day. There were days when e.g. 140 supply ships would set for the UK, whilst 120 of them were sunk by German U-boats. This part of the war is often refered to as **The Battle of the Atlantic**.

Breaking the daily Enigma keys would still be difficult, as they would have to recover the settings for **Walzenlage** (wheel order), **Ringstellung** (ring settings), **Steckerverbindungen** (patch cables), **Grundstellung** (initial position), etc.

Action this day

In October 1941, Churchill pays Bletchley Park a visit and recognises the importance of the work carried out there. By this that the workload at Bletchley Park must have been enormous. There were too many messages each day, and they were short of money, supplies and most of all staff.

On 21 October 1941, four of the leading codebreakers (Alan Turing, Gordon Welchman, Hugh Alexander and Stuart Milner-Barry) wrote a confidential letter directly to Churchill. For months they had been trying to get their requirements through the normal channels, but to no avail. Hence the reason to write the Prime Minister directly. Churchill, impressed by the letter and conviced of the neccesity of the work carried out at Bletchley Park, responded the next day with a letter, labelled **Action this day**, to General Ismay with the following contents:

```
Secret
In a box

Gen. Ismay

Make sure they have all they want on extreme priority and
report to me that this has been done.
WSC
```

1942 Introduction of the Enigma M4

In february 1942 all U-boat traffic, also known as SHARK, went onto a new key. The new Naval Enigma M4 was introduced, which used 4 wheels instead of the usual 3 and a new Umkehrwalze (reflector). The wiring of the new wheel and the new UKW was easily recovered due to German security blunders, but reading the messages was still impossible. Bletchley Park didn't have any four wheel bombes and the three wheel Bombes weren't capable of handling the extra wheel and reflector combinations. Another capture was needed.

Capture of code books from U-559

On 30 October 1943 the U-559 was forced to the surface by British destroyer HMS Petard. When the captain of the U-559 ordered his crew to abandon ship, two men from the HMS Petard went aboard and recovered two code books before the ship sunk, with the two men still in it. The two code books arrived at BP on 24 November 1942 and appeared to be the *German Weather Short Code Book* and the *Short Signal Book*. They proved vital for getting back into SHARK traffic.

1944 Activity at Bletchley Park

Exactly how many men and women worked at Bletchley Park during its peak is unknown. There are guesses between 1,000 and 10,000 people, the latter probably being more accurate as it's the figure given by the GCHQ. At some point in 1944, 7000 men and women worked there in 4 shifts, every day and night to handle the enormous amount of radio messages: many thousands each day!

People worked in huts (small wooden buildings) and they didn't know what went on in the other huts. They were allowed to socialise with other employees, but they could never talk about work. Which, of course, they didn't.

1945 Hitler commits suicide

The U-boat section of the German Navy was headed by their commander **Karl Dönitz**. Dönitz, uncertain about the security of Enigma, ordered several investigations to see if the Enigma cypher had been compromised. Each time he was assured that breaking the Enigma was impossible. On 30 April 1945 he sent the following message to his crews around the globe:

```
Der Führer ist tod. Der Kampf geht weiter, Dönitz
```

Britain's Best Kept Secret

Despite the fact that some parts of the German army still wanted to continue their battle, Hitler's death more or less marked the beginning of the end. Shortly after his suicide, the war would be over and the allies would be in charge again.

Winston Churchill, always a great fan of the Ultra Intelligence work, visited Bletchley Park shortly after the war was over, and asked for confidentiality. As he didn't want anyone to know anything about what had happened there, he instructed all evidence to be destroyed. Machines were dismantled and most paperwork was burned on site. And for may years this would remain Britain's Best Kept Secret.

It is rumoured that a significant number of captured Enigma machines was subsequently sold or given away to foreign nations, who could use it for their own confidential radio traffic, e.g. between embassies. Enigma machines have been used at least by Norway, Switzerland, Argentina and The Netherlands until the 1960's.

1946 The Cold War

The end of the Second World War, also marks the beginning of the Cold War. It was of vital importance that the former ally, the USSR, would never find out about the Bletchley Park wartime achievements.

By March 1946 they were all gone. Every scrap of 'incriminating' evidence was destroyed, just like Churchill had ordered. With respect to the codebreakers and their ultra secret work, Churchill once called them: *The geese that laid the golden eggs and never cackled.*

Most people went off to other jobs or back to their studies. Some continued their codebreaking efforts under a new name: the Government Communications Headquarters (GCHQ). Turing moved to Manchester University were he worked on the British computer initiative. He also remained active for the GCHQ.

Bletchley Park remained in use by the Post Office and GCHQ as a training centre for teachers, Post Office workers, air traffic control system engineers and members of GCHQ.

1952 Alan Turing arrested

Being an openly gay man, Alan Turing, was considered a security risk. In 1952, he was arrested and put on trial. In order to avoid going to prison, he had to take hormone treatment. He lost his security clearance and found himself under watch.

Eventually, he took his own life in 1954 by eating an apple dipped in cyanide.

1974 Winterbotham's book: The Ultra Secret

The full story about the Enigma and the breaking of its codes, was kept secret for many years, just like Churchill had instructed. The first publication that really came as a shock to many people was the book **The Ultra Secret** by Winterbotham. This was the first time anyone outside Ultra would learn anything about the allied codebreaking efforts.

Winterbotham wrote the book from memory, as he had no access to the classified information of those days. His book therefore contained some minor inaccuracies and errors, but it gives a good insight as to

what happened during WWII. The book caused great upset with the British authorities, but gradually more and more would be revealed in the following years. It also triggered other former codebreakers to tell their story or write a book themselves.

1979 Enigma, by Wladyslaw Kozaczuk

In 1979, the Polish Wladyslaw Kozaczuk wrote a rather complete book describing the wartime effort of the Polish Cryptographers in the time before and during WWII. Unfortunately the book was written in Polish thereby making the information unavailable for most researchers on the subject. In 1984, the book was translated and republished, this time in English. For a long time, there were doubts about the importance of the Polish contribution to the breaking of the Enigma, but recent discoveries in both British and American archives, have revealed credible evidence that the discoveries of the Poles were of vital importance.

1982 The Hut 6 Story, by Gordon Welchman

In 1982, Gordon Welchman, one of the original British codebreakers, who headed Hut 6 for a substantial period, put his memories on paper and released his book: **The Hut 6 Story**. Despite the fact that this publication came 8 years after Winterbotham's book 'The Ultra Secret', it again caused great upset and eventually Welchman lost his security clearance in the USA where he had been living since the war.

The Hut 6 story is a very readable book, describing the early days at Bletchley Park before the war, the formation of Hut 6, the first breaking achievements and the building of the Bombes. It also gives some in-depth details about how the codes were broken and what kind of mistakes the Germans made to compromise the Enigma's security.

1991 Bletchley Park facing demolition

In the years following WWII, Bletchley Park was used by the GC&CS (now called GCHQ) and the Post Office (now called British Telecom) as a training centre. Extra buildings were erected and the old wartime huts were left abandoned. After some 50 years of association with British Intelligence, Bletchley Park was finially decommissioned in 1987.

By 1991, Bletchley Park was almost completely deserted and plans were made for demolition of the existing buildings to make way for housing development. A farewell party was held on the grounds and over 400 former codebreakers were present.

Present time

The Bletchley Park Museum

In February 1992, the Milton Keynes Borough Council, declared most of Bletchley Park a conservation area and The Bletchley Park Trust was formed only three days later. They started negotiations with the landowners and first opened the site to visitors in 1993. Finally, in July 1994, Bletchley Park was officially opened as a museum.

Today, Bletchley Park is a modern museum showing many aspects of the Enigma and codebreaking in general. They have a nice collection of Enigma machines, but also a working replica of a Bombe. The full story of codebreaking can be seen here, from the transmission of German messages in the field, through the intercepts stations, to Bletchley Park and finally to the decision makers.

But there's more. The very rare Lorenz Geheimschreiber (used by Hitler for extremely secret messages) is on display and the first computer ever: **Colossus** (used to break the Lorenz cipher) is being rebuilt here. More and more of the old huts are being restored and new exhibitions are added every now and then.

8. Secrets from the Past: Breaking German Army Ciphers

Contribution by Geoff Sullivan and Frode Weierud

8.1 Introduction

This chapter contains a pre-release of the fruits of an on-going codebreaking project, which can best be described by the title Breaking German Army Ciphers. The project is a joint effort by Geoff Sullivan and Frode Weierud, two of the members of the Crypto Simulation Group (CSG). The project has its origin in an attempt to devise good computerised cryptanalytical techniques that can solve authentic German Army Enigma messages. With this we mean Enigma messages which are shorter than the authorised limit of 250 letters and which have been enciphered on the standard three- wheel, steckered Wehrmacht Enigma also known as the Service Enigma. Because we have no knowledge of the content of these messages, we cannot use the Turing-Welchman Bombe, the electromechanical key finding machine, developed during the war at the UK codebreaking centre Bletchley Park (BP). Our attack is therefore of the variety called a ciphertext-only attack and it is based on statistical techniques and evolutionary computation.

However, the project would never have gotten off the ground if we did not have access to a sufficiently large number of authentic messages on which to develop and refine our cryptanalytical techniques. By lucky circumstances a large number (500+) German Army messages from 1941 and 1945 have survived the end of the war. We have not yet had the time to catalogue them all but so far we have catalogued and transcribed 207 messages of which 195 are in Enigma and 12 are in a hand cipher, which we suspect is a variant of the Doppelkastenschlüssel, Double Playfair. Of the 195 Enigma messages we have so far broken 133, a success rate of 68%.

More detailed information and regular progress reports will be available on a Web Site which is presently under construction. The cryptanalytical details and other cryptological and historical information will be published in due time.

The next paragraph contains several authentic German Army messages from two days in July 1941, 7 July 1941 and 13 July 1941, which never have been published before! For each message, we show the original Spruch, which is short for Funkspruch – radio telegram. The forms do not have exactly the original format but they contain all the information that was entered on the original forms. Two-part messages were always written on two separate message forms. To simplify, we have transcribed both parts in the same file.

8.2 The Messages

At the end of this chapter, we've reproduced the various messages for both days. First of all, we show the main Enigma key for that day, together with the deciphered message keys for each individual message. The daily Enigma key consists of four elements: the UKW (Umkehrwalze, or *reflector*), which in 1941 was always type B, the Walzenlage (wheel order), the Steckers (plug board connections) and the Ringstellung (ring settings). Each message has a header, which consists of: date, letter count and key indicator. A typical header looks like this:

```
1715 - 195 - BUO  IHO
```

The trigram **BUO** is the Grundstellung (base setting) of the three wheel Enigma machine, and **IHO** is the enciphered Spruchschlüssel (message key). The real message key is obtained by first setting up the Enigma machine with the complete daily key, setting the three rotors to the Grundstellung, here **BUO**, and typing the three letters of the enciphered message key, here **IHO**. This will result in the three letters **RAS** which is the message key.

```
fuer m7g     1715   - 195 - BUO IHO -

ENSIV TINIF MFUNK DSPXR
KBKQA DAJZN JZUQW CPHTK
GQQPB XXBDM NQWKJ BYMOG
MYOPT RHCNV ASAAG EZDRC
KGVUJ MKLIW CVVPP TSCIL
DPLRV PNCAU IMMUD RYMGJ
YWNVA DCUCT QGTEJ HGABO
SEXCS RDXGO YKWKI WDIDT
ZTEPX FGMRD YMDQJ KBOEJ
AZLJU PAWMN WYQDG
```

Example of an original Funkspruch (radio telegram)

After the header, the five letter groups of the message follows, in our case 39 groups – a total of 195 letters. However, the first five letter group is not part of the ciphertext. This group, which is called the Kenngruppe (indicator group), will tell the radio/cipher operator which Enigma key has been used to encipher the message. In our example the indicator group is **ENSIV** which tells the operator that he should use the Enigma key which has **SIV** or any permutation of these three letters as one of the four indicator groups (Kenngruppen). For each daily Enigma key on a given cipher network there would be four trigrams that should be embedded in a permuted order into the first group of the cipher text.

We are using the indicator group to identify the different messages. On the 7 July 1941 we have four messages with the indicators **ENSIV**, **TFZGU**, **RFUGZ** and **FNJAU**. For each message, we'll show the contents of the original German message form, followed by the broken message, the plain German version of it and finally the English translation. Here are the Enigma keys for the two dates:

7 July 1941

UKW : **B**
Walzenlage : **245**
Stecker : **AV, BS, CG, DL, FU, HZ, IN, KM, OW, RX**
Ringstellung : **BUL**

Message keys:

No	Part	Kenngruppe	Indicator	Start	Stop
18		ENSIV	BUO IHO	RAS	RIA
19		TFZGU	RIA QDB	WUQ	WXC
20	1tl	RFUGZ	WXC KCH	BLA	BRS
20	2tl	FNJAU	CRS YPJ	LSD	LXX

13 July 1941

UKW : **B**
Walzenlage : **423**
Stecker : **AD, EH, GY, IM, KN, LR, OZ, QV, TX, UW**
Ringstellung : **GTO**

Message keys:

No	Part	Kenngruppe	Indicator	Start	Stop
24	1tl	KHGPR	YJN ZOV	OXE	OCS
24	2tl	YSPQR	OCS ILY	LMA	LPF
25		FHPQX	HLC ZMZ	SDV	TNB

7 July 1941, Funkspruch Nr.: 18

Funkspruch:

Befordert am: 07.07.1941 1725 Uhr Durch:
Funkspruch Nr.: 18 Von/An: f8v/bz2

Absendende Stelle : Div Kdr An: LVI A.K.

```
fuer m7g     1715  - 195 - BUO IHO -

ENSIV TINIF MFUNK DSPXR
KBKQA DAJZN JZUQW CPHTK
GQQPB XXBDM NQWKJ BYMOG
MYOPT RHCNV ASAAG EZDRC
KGVUJ MKLIW CVVPP TSCIL
DPLRV PNCAU IMMUD RYMGJ
YWNVA DCUCT QGTEJ HGABO
SEXCS RDXGO YKWKI WDIDT
ZTEPX FGMRD YMDQJ KBOEJ
AZLJU PAWMN WYQDG
```

Possible prestart: RAS (written in lefthand margin)

German plaintext:

```
AN X ROEM X FUENF SEQS X ARM X KORPS X HOEHE X
ZWO NULL NULL X STARK BESEZT X ANGRIFF ERST NAQ
STARKER ARTILLERIE VORBEREITUNG DURQFUEHRBAR X
HALTE EINAHME VOR SPAETEN ABEND NICHT FUER MOEGLICH
X VON X VON X KESSEL X KESSEL X HAUPTMANN
```

In German:
An LVI Armeekorps.
Hoehe 200 stark besezt (sic). Angriff erst nach starker Artillerie-vorbereitung durchführbar. Halte Einahme (sic) vor späten Abend nicht für möglich.
Von Kessel, Hauptmann

In English:
To LVI Army Corps.
Hill 200 is heavily occupied. Attack is feasible first after strong artillery preparations. Consider a capture for late evening not possible.
Von Kessel, Captain

7 July 1941, Funkspruch Nr.: 19

Funkspruch:

Befordert am: 07.07.1941 1835 Uhr Durch:
Funkspruch Nr.: 19 Von/An:

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

```
fuer m7g     1805  - 69 - RIA QDB -

TFZGU SAYQY FNGVB NIDLQ
GCTAY NLPJD TBQCU KKEHT
HHLQZ QYVNY MZDMU ZRGIH
TFELH JHAY

                          - 125 - QWD ? -
```

Possible prestart: WUQ (written in lefthand margin)

German plaintext:
ERBITTE AUFKLAERUNGSFLIEGER UEBER X SEBESH X SEBESH X UND X NOERDLIQ X DAVON

In German:
Erbitte Aufklärungsflieger über Sebesh und nördlich davon.

In English:
Request reconnaissance flight over SEBESH and northerly from there.

Note:

The term *Fliegerstrasse* is obscure. It is possible it is a special term used by German tank forces, but it can also refer to the corridors that the German airforce (Luftwaffe) kept clear of any enemy air activity. This is the meaning used in the translation.

7 July 1941, Funkspruch Nr.: 20

Funkspruch:

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
SBDPJ BFFKY QWFUS

            - qsl ? de m7g
            - 1715/1805 kr - k
```

Possible prestart: BLA (written in lefthand margin).

Possible prestart: LSD (written in lefthand margin).

German plaintext:
AUFKL X ABTEILUNG X VON X KURTINOWA X KURTINOWA X NORDWESTL 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 X EINS X INF RGT X DREI X AUF FLIEGERSTRASZE MIT ANFANG X EINS SEQS X KM X KM X OSTW X KAMENEC X KAMENEC X DIV X KDR X

In German:
Aufklärungsabteilung, von Kurtinova nordwestlich Sebez, auf Fliegerstrasse Richtung Dubrowki - Opotscka um 1830 Uhr angetreten. Angriff. Infanterie-Regiment 3 geht langsam aber sicher vorwärts. 1706 Uhr, I.(Roem 1) Infanterie-Regiment 3 auf Fliegerstrasse mit Anfang 16 km ostwärts Kamenec.
Divisionskommandeur.

In English:
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.

13 July 1941, Funkspruch Nr.: 24

Funkspruch:

Befordert am: 13.07.1941 0809 Uhr Durch: Kor
Funkspruch Nr.: 24 Von/An: ZD41/JOT (?)

Absendende Stelle : SS-J. Div An: LVI A.K.

```
fuer umx 0730 - 2tle - 1tl 149 - YJN ZOV -

KHGPR MXDHZ VPVUJ TKXCR
NSLFI OIMYH LOSYY FXJYB
WBOIF HPDDN FXWJL DAXNG
LHQVW DQZBX QZFYF EBSEO
GFXUO TVLGL QLUDN INLPD
OKNXE WVEIA OPLKU SLDTL
PRNKC OWZKP TZWXD RIALL
TTYVS DIUT

          2tl - 88 - OCS ILY -

YSPQX JSBXQ MYNBN ETVDP
TYYKC FIDOZ AUQVK QGDAG
ISEFF VNEFG ZWJWB NVFXV
VGVTU CPFPR WKUVK NXFOD
CXKYI LID
```

Possible prestart: OXE (written in lefthand margin).

Possible prestart: LMA (written in lefthand margin).

German plaintext:

```
AN ROEM FUENF SEQS X ARM X KORPS X STRASZE VON X
SCHEMJAKINA X SCHEMJAKINA X BIS UNTERKUNFTSRAUM
SIEGFRIED SIEGFRIED X TONI X DIV X FREI X JEDOQ
GESPERRT DURQ VERKEHRSORGANE X
SIEGFRIED SIEGFRIED X TONI X DIV X BITTET UM
FREIGABE UM IN BEFOHLENEN RAUM ABZUFLIESZEN X
DIV X KDR X
```

In German:
An LVI *Armeekorps*.
Strasse von Schemjakina bis Unterkunftsraum SS-T. Division frei, jedoch gesperrt durch Verkehrsorgane.
SS-T. Divison bittet um Freigabe um in befohlenen Raum abzufliessen.
Divisionskommandeur.

In English:
To LVI *Army Corps*.
The road from SCHEMJAKINA to the accommodation area for SS-T. Div. is free, however closed by traffic organizations. SS-T. Div. requests permission to enter the area in accordance with orders.
Division Commander.

13 July 1941, Funkspruch Nr.: 25

Funkspruch:

Befordert am: 13.07.1941 0854 Uhr Durch: fcl
Funkspruch Nr.: 25 Von/An: ZD41/JOT

Absendende Stelle : An:

```
fuer S03    0830 - 219 - HLC ZMZ

FHPQX FDZCJ JDKVW PYFDW
POQZG TJQYY XAFRH SQESE
RKGJB WBYPE OOKFM MPOMK
QDDOL CPKHY PGUZY XBZYA
NYSAX IPXVQ CPJBF FFDRD
XFIJJ PPPEY ALCYK VLKXQ
HWIRZ ANGWU JBWVJ YCKES
MJQRY KQHCQ OKMMY WMCKV
LZJDV ZXRUM RMNWF DZBQG
XJQAP FFFZT AHJQZ PWQWN
IVZWU IJTHO YXGDC OJUW
```

Possible prestart: SDV (written in lefthand margin).

German plaintext:

```
AN X PANZ X GRUPPE X VIER X SIEGFRIED SIEGFRIED
TONI X DIV X STEHT SEIT X EINS ZWO X SIEBEN X
EINS EINS NULL NULL X UHR MIT ANFAENGEN AM
UNTERKUNFTSRAUM X KANN NIQT EINFLIESZEN X DA X
DRITTE X INF X DIV X UND X AQTE X PANZ X DIV X
BLOQIEREN UND RANM BELEGT HALTE X DIV X KDR X
```

Please note that the underlined word is some kind of typo, which may have been caused by bad transmission or reception of the morse codes, or simply by pressing the wrong key on the Enigma.

In German:
An Panzer Gruppe 4.
SS-T. Division steht seit 12.7. 1100 Uhr mit anfängen am Unterkunftsraum. Kann nicht einfliessen, da 3. Infanterie-Division und 8. Panzer-Division blockieren und Raum belegt halte.
Divisionskommandeur.

In English:
To Panzer Group 4.
SS-T. (Totenkopf - Death's Head) Division stands since 12.7 11:00 at the beginning of the accommodation area. Cannot enter because 3rd Inf. Div. and 8th Tank Div. are blocking and keep the area occupied.
Division Commander.

Dienststelle: .... stelle: ....

Spruch Nr.	Befördert am 19	.... Uhr durch ....
	Aufgenommen am 19	.... Uhr durch ....
....	Erhalten am 19	.... Uhr ....

Fern- / Funk- / Blink- **Spruch Nr.** 18 von fdv an kz 2

Vermerke: vpd 2

Absendende Stelle:	....te Meldung	Ort	Tag Monat	Stunde Minuten
Di. Kdr.				
	Abgegangen			
	Angekommen			
	An LVI AK.			

mltu1 -

spr m Fy 1715 - 195 - auo ilo -

ensiv	tinif	mfunk	osprr
kbxqa	dajzn	jzuqw	cpdta
gqqpb	xxbdm	nqhkj	bymog
myopt	phcnv	asaaq	ezjze
kqvuj	mkliw	cvvpp	tseil
dplrv	pncau	imnud	ryngj
ywnva	dcuct	qgtej	hgaho
nexcs	rdxgo	yhwki	wdidt
ztepx	fgmrd	ymdqj	kboej
aelju	pawmn	wyqrq	

G. Braun G.m.b.H. Karlsruhe

8.3 Backgrounds

The German Army messages are written in pencil on printed messages forms. We do not have access to the originals but only to photocopies. As the message forms seem to be made from some type of greyish, perhaps recycled, paper the photocopies are sometimes very dark and the contrast is poor. It can best be described as dark grey pencil marks on light grey paper. Therefore the transcription is at best a painstaking process. On top of that, the different radio/cipher operators all have slightly different hand writing even if they have all been trained to take down the Morse code in lower case letters and using what seems to be a standardised script. Hence the first step in the codebreaking process is to decipher the operator hieroglyphs and at best make educated guesses at faint or close to illegible letters. The final hurdle in recovering correct plaintext from faulty ciphertext has to do with bad radio reception and poor operators. When plaintext finally appears it is often discovered single letter errors that can not be explained otherwise than by wrong Morse code reception. However, due to the statistical techniques we employ, we are nevertheless able to break messages based on somewhat faulty ciphertext.

The messages are from two periods, June to October 1941 and April 1945. The messages from 1941 seem all to be from the campaign against Russia, Operation Barbarossa. The units all belong to Heeresgruppe Nord (Army Group North) and many of the messages are from Panzergruppe 4 (Tank Group 4) and SS Panzer T (for Totenkopf – Death's Head) Division. Other messages concern Armeekorps XXXXI (Army Corps 41) and Armeekorps LVI (Army Corps 56) and various infantry divisions and regiments. The messages clearly have a historical value but it is doubtful if their content will change anything to our historical perceptions of this period. However, they might be of interest to historians who research the history of German military units and local historians in Lithuania, Latvia and the areas south of St. Petersburg (Leningrad). The messages contain many place names and it is to some extent possible to follow the advance of the German forces though this area.

For the cryptological historians they are of great interest because for the first time it is possible to analyse in detail how the German army radio/cipher operators performed, how well did they respect security regulations and what errors did they make. We have already discovered that the radio operators with the units of Heeresgruppe Nord seemingly were not any better than their error prone colleagues in the German Luftwaffe. Their use of what BP called Cillies and Psillies (psychological Cillies) were of a daily occurrence. The recovered message keys for 7 July 1941 clearly shows Cillies at work:

No.	Part	Kenngruppe	Key Indicator	Start	Stop
18		ENSIV	BUO IHO	RAS	RIA
19		TFZGU	RIA QDB	WUQ	WXC
20	1tl	RFUGZ	WXC KCH	BLA	BRS
20	2tl	FNJAU	CRS YPJ	LSD	LXX

Here we notice that instead of choosing a random three letter group for the Grundstellung of message No. 19 the operator has let laziness rule. He has used the last wheel positions of the previous messages, RIA, as the new Grundstellung for No.19. This repeats for message No. 20, part 1, while for message No. 20, part 2, he has decided to scramble slightly by moving the leftmost wheel one position such that the BRS becomes CRS, the new Grundstellung for part 2. We have other even more horrifying examples of operator laziness. The message key should also be chosen at random but very often the operators chose triplets of their own liking. One example is the radio operator Krüger who again and again uses KRU for his message keys. We will go into further details about German army cipher security in our publication.

What other uses can these messages have? We cannot give a full answer to this as there are probably uses that not even we are able to imagine, but here are a few suggestions. First of all, their structure and statistical information is crucial in fine-tuning various cryptological attacks. Furthermore, they will show how radio communications were an integral part of the German military machine and they will allow amateurs of all kinds to experience first hand how to encipher and decipher German military messages. Those that want can try to repeat the codebreaking feats performed at BP during the war. They can use cribs from the plaintext we supply and experiment building good Bombe menus for the Turing-Welchman Bombe.

The Second World War is now a distant past, however its great sufferings, upheavals and tragedies are frequently used as a background in modern literature. So perhaps some of these messages will be an inspiration to future writers.

Some of the messages carry the signatures of infamous personalities like SS-Brigadenführer (Major General) Heinz Lammerding, who after the war was tried in absentia and sentenced to death by the French for the massacres at Tulle and Oradour-sur-Glane in June 1944. Or, SS-Obersturmbannführer (Lieutenant Colonel) Friedrich Hartjenstein, who in 1941 was commander of the SS Totenkopf Nachschubdienste (supply service – logistics). In 1943, he became Lagerkommandant (Camp Commander) of KL Auschwitz II Birkenau and then Lagerkommandant of KL Natzweiler. After the war, he was sentenced to death by the French, a sentence which was later commuted to life imprisonment. He finally died of a heart attack in a French prison.

None of the messages have so far revealed any secrets or astonishing revelations and neither do we expect this to happen, but they nevertheless give an exiting microscopic view of past historical events. The thrill of breaking a new message is probably very close to the excitement experienced by any archaeologist who discovers fragments of an ancient vase at a new historical excavation. In this sense we are perhaps the first cryptological archaeologists.

8.4 Acknowledgments

We, the authors, are most grateful to Mr. Michael van der Meulen for giving us access to his collection of German Army messages. His help and co-operation continues to be a crucial and inspiring factor for the success of this codebreaking project. Without him we probably would not have embarked on such an undertaking. We are equally indebted to the former Oberstleutnant (Lieutenant Colonel) Waldemar Werther and his wife Hetty, now unfortunately both deceased. Waldemar Werther was instrumental in saving these messages from destruction at the end of the Second World War, and later he made sure the material would survive his death. On his death in the late 1980's, his widow Hetty, followed his wishes and transferred the Army messages to Mr. Michael van der Meulen.

We are also most thankful to Erik Brache and John Molendijk for their continuing help in supplying us with the necessary computing power to break these messages.

8.5 Copyrights