Enigma touch Operating Instructions

Jürgen Müller, juergen@e-basteln.de

Version 1.1, 29.8.24

These instructions describe board version Rev. 3 with firmware 006.
Deviations for board version Rev. 2 are indicated in the text.

Contents

1. Introduction

The *Enigma touch*

The *Enigma touch* is an electronic functional model of the Enigma cipher machine. Various civilian and military variants of the Enigma from the 1930s and 40s can be simulated.

A simple single-board design aims to closely replicate the appearance and function. Electronic components are fitted on the bottom side of the circuit board; the top side remains free and is modeled after the front of the original Enigma, approximately on a 2:3 scale.

The circuit board itself performs many functions: In addition to the front panel, it forms the capacitive keyboard, diffusers and letter masks for the lamp field, sockets for the plugboard and a sounding board for the small piezo speaker. Small graphic displays under the circuit board show the position of the rotors; capacitive sliders reproduce the gear rims with which the rotors can be moved.

The *Enigma touch* is primarily intended for simple assembly as a flat single-board setup. The plugboard of the military Enigma variants is arranged at the back for better handling. However, it can also be detached in order to install the *Enigma touch* in a wooden enclosure that is close to the original arrangement.

About these instructions

These instructions describe the *Enigma touch* replica. The original Enigma is only discussed briefly where required as context for the replica functions. A basic understanding of the Enigma functionality is assumed; the following section recommends some sources on the Internet.

Chapter 2 explains the basic operation of the Enigma and the replica – setting up the Enigma and encrypting and decrypting. Special Enigma models and additional functions of the replica are described in chapter 3. Chapter 4 provides information on building the *Enigma touch*, and chapter 5 on firmware updates.

References for the original Enigma

Excellent 3D animation by Jared Owen explaining the **working principle of the Enigma**. Just under 20 minutes, highly recommended!
https://www.youtube.com/watch?v=ybkkiGtJmkM

A very comprehensive, well-structured and richly illustrated presentation of the **Enigma machines** by two Dutch collectors. The focus is on the machines themselves, with excursions on their use.
https://www.cryptomuseum.com/crypto/enigma/

Functional principle, **military use and decryption of the Enigma**. Extensive website, originally created by Tony Sale, the first curator of the museum in Bletchley Park. https://www.codesandciphers.org.uk/enigma/

Extensive collection of publications, websites and own work on the **history and cryptanalysis of the Enigma** by Frode Weierud, a Norwegian amateur cryptologist. https://cryptocellar.org/enigma/

Historical sample message with **decoding tutorial:**
https://www.cryptomuseum.com/crypto/enigma/msg/p1030681.htm

Explanation of the various military **key procedures** used
(daily key, message key, code groups...)
https://de.wikipedia.org/wiki/Enigma-Schl%C3%BCsselprozedur
https://www.ciphermachinesandcryptology.com/en/enigmaproc.htm

Original messages that you can try to decrypt:

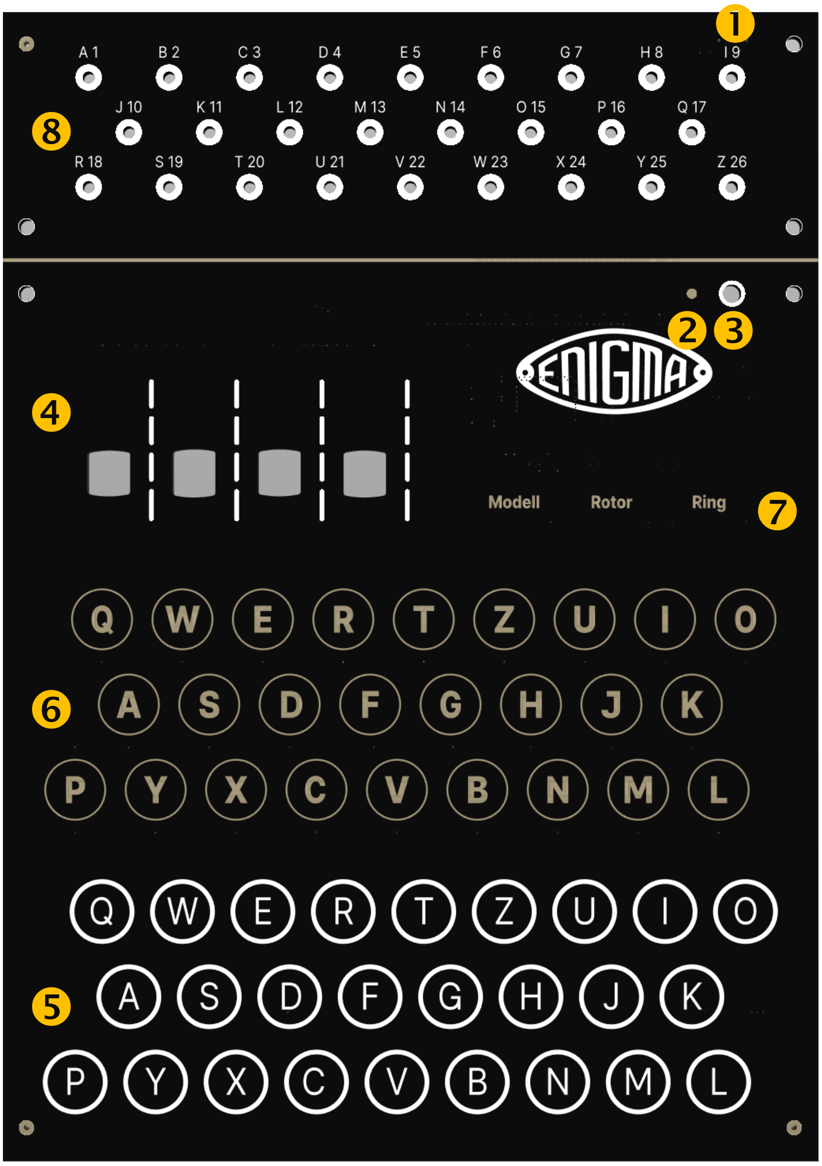
Lots of M4 messages:
https://enigma.hoerenberg.com/index.php?cat=The%20U534%20messages

Enigma I and M3 messages:
https://enigma.hoerenberg.com/index.php?cat=Norrk%C3%B6ping%20messages
https://www.cryptocellar.org/enigma/enigma-modern-breaking.html

A few messages for various Enigma models, including the K and T models.
http://wiki.franklinheath.co.uk/index.php/Enigma/Sample_Messages

2. Operation - Basic functions

Overview and first steps



1. Connect a 5V power adapter to the **USB-C socket** on the back to supply the *Enigma touch* with power and, if necessary, to charge the built-in lithium-polymer battery. 5V/50mA for operation without battery, 5V/250mA for operation and simultaneous battery charging.

2. The **LED** lights up while the battery is being charged, or (for builds without a battery) when 5V is applied to the USB socket.

3. Switch on the *Enigma touch* at the **on/off switch**. The machine state – selected Enigma model, configuration and rotor positions – is retained when switching the machine off and on. The machine always starts in normal encryption mode. After 15 minutes without user activity, the *Enigma touch* switches off automatically.

4. The displays for the **rotors** light up as soon as the *Enigma touch* is switched on. The placement and rotation of the rotors determine the current letter encryption or decryption. The current position of each rotor can be read in the viewing windows. The dashed lines next to each window represent the sprockets which allow manual rotor movement.

   Only the start position at the beginning of an encryption is set via the sprockets; during the subsequent encryption the rotors move on automatically. The ciphertext is *not* displayed in the viewing windows – it appears in the lamp field.

5. The **keypad** is used to enter the plaintext or ciphertext. Each keystroke moves one or more rotors one step forward – in the original via a direct mechanical coupling, driven by a long key stroke – and then lights up a lamp.

6. The **lamp field** displays the letters of the encrypted or decrypted text. As with the original Enigma, a lamp only lights up for as long as a key is held down.

   Enigma does not distinguish between encryption and decryption mode! Its encryption is symmetrical (self-inverse) – if an encrypted text is encrypted a second time with the same initial settings, the plaintext is returned.

   You can now start encrypting or decrypting directly with the currently set Enigma model and the rotor configuration selected for it: Set the starting position of the rotors and start entering text and reading and writing down the ciphertext or decoded plaintext from the lamps. If you want to first select and set up a different Enigma model, this is done using the mode buttons on the replica:

7. The **mode buttons** are a feature of the *Enigma touch* replica, they don't exist on the original Enigma. These buttons are used to select the Enigma variant to be simulated and the rotors in use, to set the adjustable rings on the rotors and to change some replica settings. See the following section for details.

8. We are not yet using the **plugboard** in this chapter. It is only used on the military Enigma models I, M3, and M4, and is described in chapter 3.

Setting up the Enigma

The mode buttons (7) are designed as "radio buttons": Tapping a button selects the respective setup mode and lights up the button. Tapping another mode button switches to its setup mode; tapping the currently active button again leaves setup mode and switches back to regular encryption mode. To prevent the mode buttons from being activated accidentally, they must be held for a short moment (approx. 0.3 seconds).

In each set-up mode, the rotors display different information and can be adjusted using the "sprockets". The mode buttons have dual functions: Holding them down for longer (1.5 seconds) triggers a secondary function. These advanced functions are described in chapter 3.

To configure a new Enigma model and its encryptions settings – which usually change daily in the original key procedures – work through the mode buttons from left to right. If a setting is changed, the dependent settings (buttons further to the right) are reset to the default values. However, it is possible to inspect the current settings at any time without changing anything; this does not change the dependent settings.

Model and replica settings

The Model button lets you select the simulated Enigma model and some replica-specific settings. From left to right in the rotor windows:

- Selection of the **Enigma model**. The table below provides an overview; details on the simulated machines can be found at www.cryptomuseum.com/crypto/enigma.
- Setting the **audio volume** (Rev 3 board only). The keyboard and rotor movement are signaled via different clicking noises, mode button via a higher confirmation tone, errors during set-up ar eindicated by a "cuckoo" warning tone.
- **Lamp brightness** adjustment (five levels).
- Setting the **protocol detail level** – see chapter 3, Logging via USB.
- The **battery charge level** is displayed on the far right. Rev 2 boards only supports the display of a warning when the charge level is very low, Rev 3 additionally displays the approximate charge level in three steps.

Display	Model	Description
I	Enigma I	First military version (Army), with plugboard. Only Enigma with numeric rotor labels.
M3	M3	Navy Enigma, 3 rotors.
M4	M4	Navy (submarine) Enigma, 4 rotors.
D	Enigma D	Early variant, stepping notches on the rotors, not rings.
K	Enigma K	Commercial version, 3 rotors, reflector settable but not stepping, no plugboard.
KD	Enigma K, Reflector D	Model K with rewirable reflector, used by Mil Amt intelligence service.
KR	Railway K	Model K, rotor wiring for German Railway (Reichsbahn).
KS	Swiss K	Model K, rotor wiring for Swiss Army.
T	Tirpitz	Model K variant for Japanese forces. Choice of 8 rotors, 5 turnover positions each.
G	Enigma G (or G31)	Cogwheel mechanism instead of levers to step rotors and reflector. Frequent turnovers, manual back/forth via crank.
G1	Enigma G111	Model G, rotor wiring for Hungarian Army. Only rotors I, II, V are preserved.
G2	Enigma G219	Model G, rotor wiring for Dutch Navy.
G3	Enigma G312	Model G, rotor wiring for German intelligence service (Abwehr).

Rotor arrangement

The Rotor button lets you select the rotors arrangement and – on some machine types – the installed reflector.

- The **rotor** complement is part of the daily key, which had to be known to all participants. The key was determined in advance and communicated via a secure channel – typically in a printed key list for a month in advance. Rotors are always numbered with Roman numerals.
- In the original Enigma, the complete shaft with the rotors was removed from the machine, the rotors pulled off and reassembled in a different order. Some military Enigma models included a larger set of rotors, so that three rotors were selected from a set of five to eight rotors in order to increase the number of possible keys.
- Details on the available rotors and their internal wiring can be found at www.cryptomuseum.com/crypto/enigma and www.cryptomuseum.com/crypto/enigma/wiring.htm.
- In the *Enigma touch*, the available rotors are displayed and selected in the rotor display windows. As each rotor type (Roman numeral) was only provided once with a given Enigma machine, valid rotor combinations can only use each type once. If a rotor is selected twice, it is not possible to exit rotor setup mode – an error tone will sound if you try, and the rotors chosen twice will make a full rotation to give a visual cue.
- For some machines types different **reflectors** can be selected in the left-hand window. They are labeled with letters. On the Enigma M4, the desired combination of reflector (B, C) and thin fourth rotor ("Greek rotor" β, γ) is set here, or alternatively the thicker, rewirable reflector D.

Ring position

The alphabetic or numerical lettering is not fixed on the Enigma rotors but is engraved on a ring that can be rotated relative to the rotor body. In the *Enigma touch*, the Ring button is used to adjust these rings.

In almost all Enigma types, the driving mechanism that controls the movement of the neighboring rotor engages with this ring. By turning the ring, it is therefore possible to change the position of the contact rotor at which the neighboring rotor is moved. This massively increases the number of possible encryption keys. The **"ring position"** is also part of the predefined (daily) key.

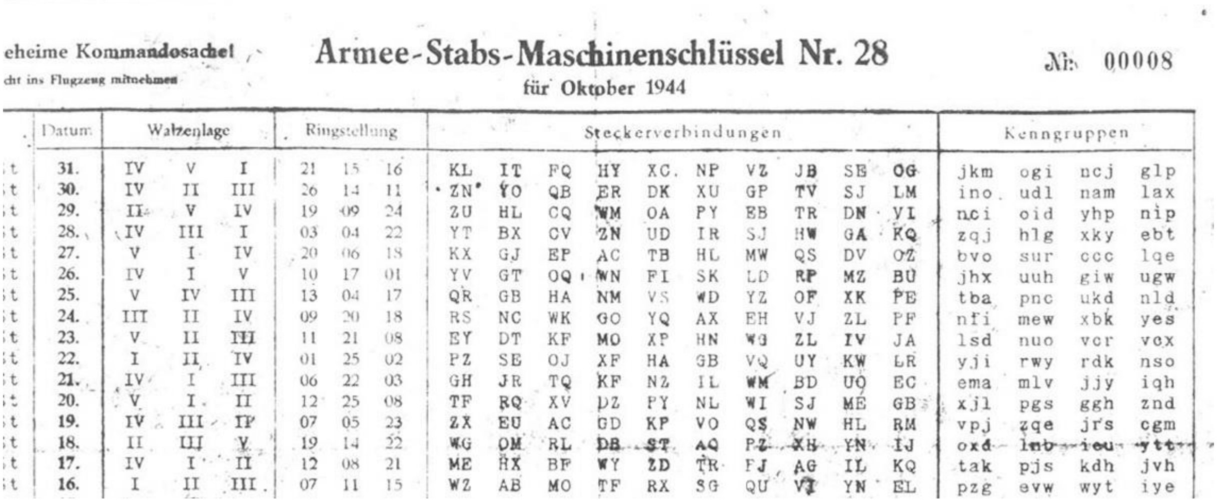
The three normal rotors have an adjustable ring on all simulated Enigma models. On models with an adjustable or moving reflector (Enigma D, G, K, T), this reflector also has a ring that can be adjusted in the left-most window. On the Enigma M4, the ring of the narrow fourth "Greek rotor" can be adjusted in the left-hand window.

Cryptographic procedure: Encrypting a message

To enable the recipient to decode an encrypted message, the sender and recipient must of course use the same key. The rotors and ring position were always pre-agreed for a specific period of time (usually 24 hours). Monthly key lists with these "daily keys" had to be securely distributed in advance in printed form to all participants in a radio network. The initial position of the rotors was selected anew for each message and transmitted in encrypted form as a "message key" before the actual message.

How this was done in detail varied between the army, air force and navy; individual procedures were also changed over time. An overview of these crypto procedures can be found at https://www.ciphermachinesandcryptology.com/en/enigmaproc.htm (Dirk Rijmenants).

This section will show how a message was encrypted and transmitted in the army or air force – after September of 1938, when the handling of the encryption key was changed to eliminate a cryptographic vulnerability.



eheime Kommandosache!

dht ins Flugzeug mitnehmen

Armee-Stabs-Maschinenschlüssel Nr. 28

für Oktober 1944

№ 00008

	Datum	Walzenlage			Ringstellung			Steckerverbindungen										Kenngruppen			
t	31.	IV	V	I	21	15	16	KL	IT	FQ	HY	XC	NP	VZ	JB	SE	OG	jkm	ogi	ncj	glp
t	30.	IV	II	III	26	14	11	ZN	YO	QB	ER	DK	XU	GP	TV	SJ	LM	ino	udl	nam	lax
t	29.	II	V	IV	19	09	24	ZU	HL	CQ	WM	OA	PY	EB	TR	DN	VI	nci	oid	yhp	nip
t	28.	IV	III	I	03	04	22	YT	BX	CV	ZN	UD	IR	SJ	HW	GA	KQ	zqj	hlg	xky	ebt
t	27.	V	I	IV	20	06	18	KX	GJ	EP	AC	TB	HL	MW	QS	DV	OZ	bvo	sur	ccc	lqe
t	26.	IV	I	V	10	17	01	YV	GT	OQ	WN	FI	SK	LD	RP	MZ	BU	jhx	uuh	giw	ugw
t	25.	V	IV	III	13	04	17	QR	GB	HA	NM	VS	WD	YZ	OF	XK	PE	tba	pnc	ukd	nld
t	24.	III	II	IV	09	20	18	RS	NC	WK	GO	YQ	AX	EH	VJ	ZL	PF	nfi	mew	xbk	yes
t	23.	V	II	III	11	21	08	EY	DT	KF	MO	XP	HN	WG	ZL	IV	JA	lsd	nuo	vcr	vox
t	22.	I	II	IV	01	25	02	PZ	SE	OJ	XF	HA	GB	VQ	UY	KW	LR	yji	rwy	rdk	nso
t	21.	IV	I	III	06	22	03	GH	JR	TQ	KF	NZ	IL	WM	BD	UO	EC	ema	mlv	jjy	iqh
t	20.	V	I	II	12	25	08	TF	RQ	XV	DZ	PY	NL	WI	SJ	ME	GB	xjl	pgs	ggh	znd
t	19.	IV	III	IV	07	05	23	ZX	EU	AC	GD	KP	VO	QS	NW	HL	RM	vpj	zqe	jrs	cgm
t	18.	II	III	V	19	14	22	WG	OM	RL	~~DB~~	~~ST~~	AQ	~~PZ~~	~~XH~~	~~YN~~	IJ	~~oxd~~	~~lnb~~	~~ieu~~	~~ytt~~
t	17.	IV	I	II	12	08	21	ME	HX	BF	WY	ZD	TR	FJ	AG	IL	KQ	tak	pjs	kdh	jvh
t	16.	I	II	III	07	11	15	WZ	AB	MO	TF	RX	SG	QU	VI	YN	EL	pzg	evw	wyt	iye

Example: Monthly key table for the Enigma I

Set up the Enigma

- We will use the **daily key** for the 31st of the month (first row of the table) from the key table shown above.
- Model selection: **Enigma I**, the machine type used by the army and air force.
- Rotor setting: select **reflector B** on the far left (the reflector used during the war) and **rotors IV, V, I** according to the daily key (Walzenlage, from left to right).
- Ring setting: Select **ring positions 21, 15, 16** (Ringstellung, from left to right).
- On the plugboard, connect the letter pairs specified in the daily key (Steckerverbindungen) with 10 cables.

Prepare the message

- The plaintext of a message is first adapted to the limited Enigma character set. The most important conventions:
    - Spaces are omitted.

- Umlauts Ä, Ö, Ü become A, O, U.
  - A period at the end of a sentence is coded as "X", a colon as "XX",
  - The frequent letter pair CH is coded as "Q".
  - Numbers are written out in words: NULL, EINS, ZWO, DREI, VIER, FUNF, SEQS, SIEBEN, AQT, NEUN.
  - The letters are grouped into groups of five for a better overview and padded with XX at the end if necessary to obtain a multiple of five.

- So the message "Wetterbericht: Heute sonnig, Höchsttemperatur 26 Grad"
  becomes „WETTE RBERI QTXXH EUTES ONNIG XHOQS TTEMP ERATU RZWOS EQSGR ADXXX".

Selecting and encrypting a message key

- To encrypt a message, the operator selects a random starting position for the rotors, the **message key**. This must of course also be transmitted to the recipient. However, this is not done in plaintext, but the message key itself is encrypted.

- To do this, the operator selects another random rotor position, the **home position**, which is initially set on the rotors. This home position is used to encode the message key. The home position and encrypted message key are then transmitted to the recipient in the message header.

- For example:
  - Select a random home position and set it on the rotors – e.g. DXF.
  - Select a random message key and encrypt it – e.g. RKU becomes FGI.
  - To be transmitted in the message header: DXF FGI

Encrypt the plaintext

- Set the RKU message key on the rotors.

- Enter the plaintext, write down the ciphertext shown in the lamp field.

- Plaintext WETTE RBERI QTXXH EUTES ONNIG XHOQS TTEMP ERATU RZWOS EQSGR ADXXX becomes LBUSL ZJAQF YJHCV NFLFT XDIUU MQKCD ULDDA JKSRT VQBRN NEKRA RGEZM.

Add the message header and code group

- Before the actual ciphertext, a message header is transmitted, consisting of:
  Time – number of letters incl. code group – home position – encrypted message key.

- Another group of five characters is inserted before the ciphertext to indicate which daily key was used – important for messages that may not reach the recipient on the same day, or when a station serves multiple message nets using different keys. To disguise this information somewhat, any one of the four **code groups (Kenngruppen)** from the daily key is chosen, and two random letters are added before it – e.g. DANCJ.

- So the complete message is: **1630 = 60 = DXF FGI =**
  DANCJ LBUSL ZJAQF YJHCV NFLFT XDIUU MQKCD ULDDA JKSRT VQBRN NEKRA RGEZM

Practice message

- Here's another message for practicing the cryptographic procedures. The following (fictitious) message was sent early in the morning on October 29. Can you decode it?
- **0030 = 35 = LTY JCH = HSZQJ BRSLM DMSPX JALYV DYROG JDETL BPUXN**

Taking care of the *Enigma touch*

Cleaning

The matte black front can become a little shiny due to fingerprints, usually on the frequently touched surfaces of the sliders and mode buttons. A soft cloth moistened with a little water is usually sufficient to restore a uniform surface.

For more stubborn dirt, a cloth moistened with detergent solution or glass cleaner can also be used. However, the cleaners also remove previously applied care products and often result in surfaces that have been touched becoming different from the rest of the front all the more quickly. They should therefore only be used when necessary .

Occasional wiping with a plastic care product or silicone oil (wipe off any excess and streaks with a soft cloth) reduces sensitivity to fingerprints and restores a deep black surface.

Rechargeable battery

Lithium-ion batteries should not be stored fully discharged to maintain their capacity. The protective circuit in the battery protects against deep discharge, but it is recommended to charge the battery a little before storing it for extended periods of time.

In the *Enigma touch*, the battery is charged with 200 mA charging current. Batteries with a capacity of 500 to 1000 mAh should therefore be fully charged in 2½ to 5 hours and then provide an operating time of 10 to 20 hours or a storage time of at least 2 years.

If the rechargeable battery appears inflated or has visible external damage, please do not use it! When removing the battery from the circuit board (double-sided adhesive tape), use a fireproof surface and wear safety goggles. Dispose of the battery properly.

3. Special Enigma models, extended functions

Plugboard

The military Enigma variants I, M3 and M4 are equipped with a plugboard. In the original, it is arranged vertically in front of the control panel, in the *Enigma touch* behind it for better handling.

Letters can be connected in pairs on the plugboard. This has the effect of swapping them, once before the encoding path enters the rotors and again after it exits and continues to the lamp field. In the original Enigma, connecting cables with two-pole plugs and crossed wires were used. Spring-loaded shorting bars in the two-pole sockets mapped the respective letter onto itself when the socket was unconnected.

The *Enigma touch* uses single-pole connections between the letter pairs. It automatically takes the plugboard into account during encryption if one of the Enigma I, M3 or M4 models is active. Connections can be made and changed at any time.

Technically, any number of 0 to 13 cables can be plugged in. In the historical message procedures, between 5 and 10 connections were specified – the number increased over the years. Cryptographically, 11 connections would have been optimal, as this results in the highest possible number of different combinations.

The arrangement and labeling of the sockets varied between the Enigma models. To support all relevant models, the *Enigma touch* uses a combination that did not exist in exactly this form on the original machines: The combined alphabetical/numerical labeling of the early M1/M2 variants is used, in the numerically ascending order of the M4 model. This means that the plugboard can also serve as an alphabetical/numerical translation table, which was attached to the cover of some machines as part of the printed operating instructions.

Wirable reflector D

Several Enigma variants, both for civilian and military use, used a special reflector "Dora" ("Umkehrwalze Dora" or UKWD for short), which could be wired by the user. In the *Enigma touch*, the UKWD can be used in the Enigma models KD, M3 and M4.

The UKWD could be opened to reconnect the letters in pairs using short internal cables. Only one pair of letters (J-Y) was permanently connected – more on this in the "Special features" section below. The manual wiring of the UKWD was time-consuming; therefore it was not rewired daily but e.g. weekly. The necessary connections are noted as letter pairs on the monthly key tables.

On the *Enigma touch* this rotor is also wired by hand, via the plugboard:

- Insert 12 or 13 connections.
- Press and hold the Model button.
- After one second, "D OK" appears in the display if the wiring is complete and valid. Otherwise, "D ??" is displayed and an error tone sounds.
- A valid wiring must connect all 26 letters in pairs. The pair J-Y must either be connected or these two letters may remain the only unconnected ones.

- Alternatively, the wiring can be done in Bletchley Park notation (see below). The *Enigma touch* recognizes this by the fact that the pair J-Y is neither connected nor open, and instead the letters B-O are paired.

- A wiring accepted with "D OK" is saved permanently and remains available even after a restart of the *Enigma touch*. If the wiring is invalid, the previously saved configuration of the UKWD is not changed.

Special features

In Germany, the letter positions of the UKWD were designated alphabetically in an irregular manner: The direction of rotation is opposite to that of the normal rotors, and the positions of J and Y are shifted. The British codebreakers were not aware of this, and they used a "Bletchley Park notation" with a regular direction of rotation to analyze the UKWD. The German notation can be found in historical key tables, and the British notation in documents on decryption at Bletchley Park. Therefore, the *Enigma touch* supports both input formats.

Two letters could not be freely wired by the user but were permanently paired. The original UKWD had mounting screws at the corresponding positions, so that there was no room for connection terminals. In German notation these are the letters J and Y, in British notation the letters B and O.

Bletchley Park notation	A **B** C D E F G H I J K L M N **O** P Q R S T U V W X Y Z
German notation	A **Y** Z X W V U T S R Q P O N **J** M L K I H G F E D C B

Designation of the UKWD contacts according to German and British notation.
The positions highlighted in bold are connected by a fixed wire bridge.

When the *Enigma touch* is started up for the first time, the UKWD is wired in the same way as in the Enigma KD unit which was rediscovered in 2009 in the archives of the Swedish intelligence service FRA, cf. https://cryptomuseum.com/crypto/enigma/k/kd.htm. This wiring is retained until a valid new wiring is plugged and saved as described above. The pre-assigned wiring cannot be recalled afterwards but must be plugged and saved again if required.

Input	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Output, Bletchley Park notation	K O T V P N L M J I A G H F B E W Y X C Z D Q S R U
Output, German notation	Q G K I L X B Z D Y C E W V T U A S R O P N M F J H

Default wiring of the UKWD after initial installation of the Enigma touch firmware.

Counter machines (Enigma G)

The driving mechanism that moves the rotors of the classic Enigma is not reversible: If a rotor "pulls along" its left neighbor, the user can turn the right rotor back to the previous position (e.g. to correct a typing error), but the left rotor is not automatically rotated back along with it. Unless the user has observed the left rotor's movement and also turns it back by hand, an incorrect rotor position is created and the entire subsequent encryption process is invalid.

As early as 1928, an alternative mechanism was therefore developed in which the rotors were firmly coupled by a gearbox. With a small plug-in crank, the user could turn back the complete rotor set step by step to correct errors. An additional four-digit counter, which counted the number of scrambled letters and was also turned back, helped with orientation. Machines of this type are therefore also known as "counter enigmas".

The *Enigma touch* simulates the Enigma G, a counter machine originally built for civilian applications. It was also used by the German secret service (Abwehr) and the military of various nations. Three such variants with special rotor complements are also included in the simulation, see chapter 2, "Model and replica settings".

- If a counter machine is simulated, its four-digit counter is displayed at the bottom left of the rotor windows.
- In normal key operation, the user can turn the individual rotors independently at any time to set a new start position, as with the classic Enigma variants. The separate disengaging lever, which disengaged the rotors from their gears in the original Enigma-G to allow individual adjustment, is not required in the replica.
- The "crank" for manually turning the entire rotor mechanism forwards or backwards is activated by pressing and holding the Ring button. A crank symbol appears in the right-most rotor window and the right-most sprocket operates the crank. The other sprockets are deactivated in this mode. You can continue to encrypt or decrypt normally while the crank is active.
- Crank mode is ended by pressing any mode button.

Logging via USB

Reading and writing down the ciphertext from the lamp field while typing in the plaintext requires a lot of attention from the operator. In military use, the Enigma was often operated by two-man teams – one operator to enter the plaintext, one to read and write down the ciphertext.

To increase convenience and avoid errors, the "Schreibmax" writing add-on was offered as an option: A strip printer that was connected to the lamp field with many parallel lines and automatically typed out the displayed letters.

The *Enigma touch* can also log its output via the USB port:

- Connect the *Enigma touch* to a computer via USB.
- The USB device registers as a CDC (Communication Device Class, virtual serial port). A suitable USB driver is pre-installed under Windows version 7 and up, Mac OS X and up, and on all reasonably current Linux distributions.
- Start any terminal program on the computer and open a connection on the CDC port. Baud rate, parity etc. can be set as required.

In the Model setting mode you can select how detailed the logging should be:

🗋 Logging off.

🗎 Only the output text is logged, line by line in groups of four or five.
This mode corresponds to the original Schreibmax function.

▥ Input, output and the resulting rotor position are logged,
in a new line for each letter.

In addition to the plain and/or ciphertext, changes to the machine settings are also logged – whenever a character is encrypted with the new settings for the first time. This means that the log can be used to fully trace what was encrypted with which settings.

Show rotor wiring

A long press of the Rotor button enters a mode in which the internal wiring of the currently active rotors is displayed. Each Enigma model came with a specific complement of rotors. Their wiring is documented e.g. at www.cryptomuseum.com/crypto/enigma/wiring.htm. The built-in display in the *Enigma touch* is particularly useful for displaying the current wiring of the freely wirable reflector D.

- The three rotors on the right and the reflector on the left are displayed.
  The wiring of rotors β and γ of the Enigma M4 cannot be displayed.
- The left-hand column of the pairs of letters indicates the contact that is oriented towards the left-hand neighboring rotor or reflector.
- Due to the limited display space the notation is always alphabetical, even for the Enigma I which uses numerical labeling of the rotor positions.
- The wiring of reflector D is always displayed in German notation, even if the wiring was entered in Bletchley Park notation. (Cf. chapter 3, Wirable reflector D.)

Diagnostic mode

Holding the Model button for a very long time (5 seconds, ignoring the message "D ??" after 1.5 seconds) starts the diagnostic mode:

- The firmware version is shown on the display – see chapter 5, Firmware version history.
- Keyboard and lamp test: Pressing any letter key lights up the corresponding LED in the lamp field.
- The raw data of the capacitive sensors is output on the USB connection as soon as any button or slider is operated. This raw data is not documented here as it is only relevant for trouble-shooting during development or initial PCB tests.

Diagnostic mode can only be ended by switching the *Enigma touch* off and on again.

4. Assembly instructions

The *Enigma touch* circuit board is pre-assembled with almost all SMD components. This chapter provides information on adding the remaining components (power switch, displays, piezo speaker and battery) and on building different enclosure variants.

Function test

An initial function test is already possible with the partially assembled circuit board – i.e. (also) without displays, power button, LiPo battery and piezo speaker. It should be carried out before starting the additional assembly steps below in order to be able to isolate possible problems later on.

- Power the *Enigma touch* via USB; it switches on automatically.
- The Model lamp lights up briefly (0.3 s).
- The Enigma is now ready for operation in normal encryption mode as model M4.
  Each time a letter key is pressed, an LED on the lamp panel lights up.
- The mode buttons should work: A short tap (at least 0.3 seconds) lights up the respective LED, the next tap switches it off again.
- Diagnostic mode can be started for a systematic test of all letter keys and LEDs: Press and hold the Model button for at least 5 seconds. Then test the keypad. To exit diagnostic mode, disconnect the power supply.

Additional tests are possible after connecting a computer with a terminal program via USB:

- The *Enigma touch* is preset to detailed recording via USB. Each keystroke in encryption mode outputs a line with the entered and encoded characters as well as the rotor positions.
- The function of the sliders (sprockets) and the plugboard can also be checked via the USB output: If the rotor position or the connections on the plugboard are changed manually, the *Enigma touch* outputs the new settings in the USB protocol as soon as the next letter key is pressed.

Mechanical rework

Remove the side rails

On the long sides of the PCB there are narrow rails with locating holes and position markers, which were used for automatic component placement. Deep pre-fabricaetd V-grooves allow the rails to be easily broken off. To gain enough leverage on the narrow rail, clamp it in a workbench if necessary or insert it into a suitable groove.

Rework the edges

Some of the edges of the circuit board show slight offsets from milling during production, and the long edges are not completely smooth after breaking off the rails. If the edges remain visible in the finished build, they can be smoothed with sandpaper and blackened with permanent marker to taste.

Attention, the sanding dust is harmful to health – work with good ventilation or extraction, wear a dust mask!

Detached plugboard

The *Enigma touch* is primarily intended for simple assembly as a flat single-board model. However, the plugboard can also be detached to install the *Enigma touch* in a wooden box that comes closer to the original.

As the construction of such a enclosure is quite complex, this variant is probably rarely used. Nevertheless it is discussed here first, since if it is desired to cut off the plugboard, this is best done before the further steps:

- If suitable parallel shears are available on which the PCB can be positioned and held precisely despite the populated components, this is the preferred way to cut off the plugboard. The dividing line is drawn on both sides of the PCB.
- Alternatively, the plugboard can be broken off after the PCB has been pre-scored as deeply as possible from both sides. The following points provide details:
    - A snap-off knife with a new (complete) blade is suitable for scoring. Do not score with the cutting side, but with the notch on the back of the blade! It shaves off thin strips of the PCB material.
    - Score many times at the dividing line on both sides to gradually deepen the groove in the board. The original material thickness of 1.6 mm should be reduced to less than 1 mm in the groove. The fiber-glass reinforced epoxy material is surprisingly resistant to bending and breaking!
    - When bending the circuit board, soldered components could be damaged if the board material is deformed. Therefore, clamp the board in a workbench directly at the dividing line, such that only the plugboard protrudes. To clamp without damageing any components, add spacer strips (approx. 10*10 mm²) with gaps for the components (LED D30, switch SW35).
    - Then bend the plugboard firmly until it breaks off. It is normal to hear some crunching and tearing of fibers.
- Smooth the edges with sandpaper. ***Attention, the sanding dust is harmful to health - work with good ventilation or extraction, wear a dust mask!***

The plugboard and main board are reconnected using a ribbon cable:

- Connector strips J4, J5 are 2*13-pole SMD post connectors, pin pitch 2.54 mm.
- Use two matching 26-pin IDC connectors (Insulation Displacement Connector) and 26-pin ribbon cable. Cable length approx. 25 cm allows the plugboard to be positioned at the front.

Populate components and options

On/off switch

The SW34 on/off switch is mounted so that its button protrudes through the pre-drilled hole in the circuit board. Occasionally, no-name push-buttons are offered that are designed for this "reverse mount" arrangement – but only with a (too) short stem.

An OMRON B3F-1060 or similar button is recommended – with pins for regular through-hole mounting and a stem approx. 3 mm long. The pins are bent and, if necessary, shortened so that the switch body can be soldered onto the four pads provided. The button then protrudes approx. 1.5 mm from the circuit board.

Displays

The two displays required are available as OEM products under various names, e.g. from AliExpress. Look for the following specifications:

- OLED 1.3", 128*64 pixels, white,
- Controller IC SH1106,
- SPI interface with 30-pin connection.

The 30-pin FPC (Flexible Printed Circuit) connection with 0.7 mm pitch is intended for direct soldering on the board; FPC connectors with this pitch are unfortunately not available. To solder the displays:

- Apply flux to the solder pads of the circuit board and/or FPC connector.

- Position the display to match the silkscreen print.

- Carefully adjust the FPC connector to the solder pads and temporarily fix it with adhesive tape.

- Solder with a conventional soldering iron. "Drag soldering" with a concave soldering tip works very well. However, it is also possible to solder the connection pads individually with a normal soldering tip.

- Remove adhesive tape, remove excess flux.

To fix the displays mechanically, a drop of adhesive or double-sided adhesive tape can be used between the display and the circuit board – leaving the viewing windows free, of course. However, a strip of single-sided adhesive tape over the lower, free end of the displays and the circuit board is also sufficient and is easier to remove if necessary.

External power supply

The circuit board is prepared for power supply via the USB-C socket: 5V, approx. 50 mA in operation without battery, 250 mA when operating and charging the battery at the same time.

If a separate power connector is preferred for installation in an enclosure, this can be connected to the solder pads J6. If the USB connection is to be used in parallel for data transfer but *not* for the power supply (to avoid two 5V sources connected in parallel), jumper JP1 can be cut. This disconnects the 5V line of the USB connection.

LED D30 (next to the power switch) indicates whether the LiPo battery is being charged. If the *Enigma touch* is set up without a battery, the function of the LED can be changed to light up when the 5V supply is available. To do this, cut the "Charge" jumper on JP2 and instead bridge the solder pads for "+5V" with a drop of solder.

Lithium polymer battery

The installation of a lithium-polymer battery is optional; the *Enigma touch* can also be operated directly from an external 5V power supply. However, for more convenient handling – and because all original Enigmas were battery-operated too – a rechargeable battery is recommended. A flat LiPo battery can be attached with double-sided adhesive tape under the keyboard, near the J7/J8 connectors:

- Lithium-polymer battery, rated voltage 3.7 V, charging voltage max. 4.2 V.
  Recommended capacity 500 to 1000 mAh.
- ***The battery must have a built-in protection circuit (BPS, Battery Protection System),*** which protects it against deep discharge and provides additional protection against overcharging and thermal problems.
- Connector J8 is a two-pin JST PH 2.0 socket. Batteries with matching plugs are common – but there is no standard for polarity. ***Always check the polarity before connecting!*** If necessary, the contacts on the battery-side plug can be pushed out and swapped.
- Alternatively, loose wire ends can be soldered to the pads J7.
- A LiPo charging IC (MCP73831-2ACI) charges the battery optimally and gently with preconditioning, constant current charging and final constant voltage charging. The maximum charging voltage is set by the IC to 4.2 V, the maximum charging current by resistor R12 to just under 200 mA (I_{max} = 1000V / R12).

Piezo speaker

A small piezo disk is used as the speaker, with the PCB acting as a sounding board. Disks with a diameter of up to 25 mm can be mounted on the back of the PCB using double-sided adhesive tape – either above the displays or over the unused plugboard connectors J4/J5.

The impedance of the piezo should be 400 ohms or higher. It is drive in the *Enigma touch* with 3 V_{pp} or 6 V_{pp} depending on the volume level set. Connected the piezo to the solder pads J3; polarity does not matter.

Enclosures and cables

Low-profile frame

If the *Enigma touch* is set up as a single-board model, a low-profile enclosure with a baseplate is still recommended – to protect the component on the underside from damage and because touching the board from below can trigger spurious entries on the capacitive keypad.

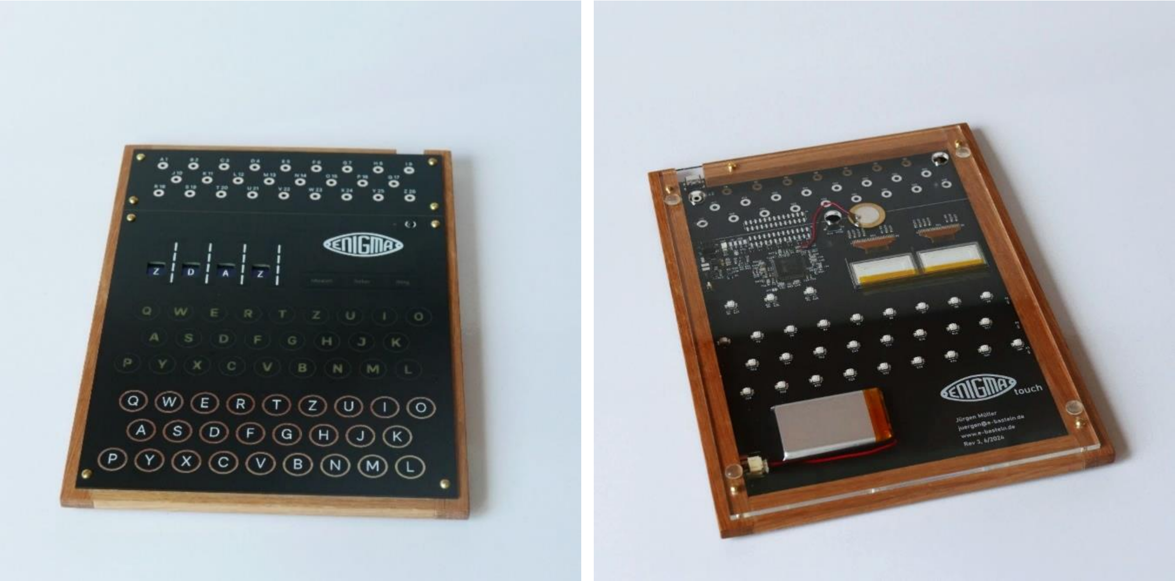
The circuit board measures 237.5 x 170.0 mm². Except for the USB socket in the back, all populatzed components are at least 10 mm away from the edge, so this area can be used for mounting a frame or enclosure.

A suggestion for an easy-to-assemble enclosure is shown below. It consists of a narrow oak frame reminiscent of the original Enigma's transport boxes and an acrylic base plate that allows a view of the simple circuit design. The frame leaves an opening for the USB socket, is glued at the corners and stabilized by screwing on the baseplate. In the example, the baseplate also has larger holes for wall mounting and for the switch for firmware updates.

Required material and dimensions:

- Oak slats 7*15 mm²; lengths 2 * 250 mm, 1 * 150 mm, 1 * 135 mm
- Base plate, acrylic 3 mm thick, size 240 * 170 mm²
- Screws 2.5 * 8 mm, 8 to mount PCB, 5 to mount baseplate
- Non-slip feet, 4 pieces

If you like it more elegant, you can use miter cuts at the corners. However, the side walls of the real Enigma transport boxes were not mitred either but used dovetail joints.



Enigma Touch with flat frame and transparent base

Three-dimensional wooden enclosure

Installation in a wooden box that more closely resembles the original Enigma is possible, but considerably more complex. As the execution will depend heavily on the personal ambition for fidelity to the original, budget, craftsmanship and effort, only a few tips are given here.

To detach the plugboard, see the section "Detached plugboard" in chapter 4.

The example shown below uses

- Beech plywood 8 mm, 186 * 240 mm² each, for top and bottom,
- Beech slats 20*8 mm² (lid) and 52*8 mm² (base) as side panels,
- Beech strip 56 * 8 mm² for the front flap,
- Piano hinges 10 mm (width when closed) for lid and front flap.

Some thoughts on design details:

- Carrying handle: Both folding metal carrying handles and leather straps were used in original Enigma variants.

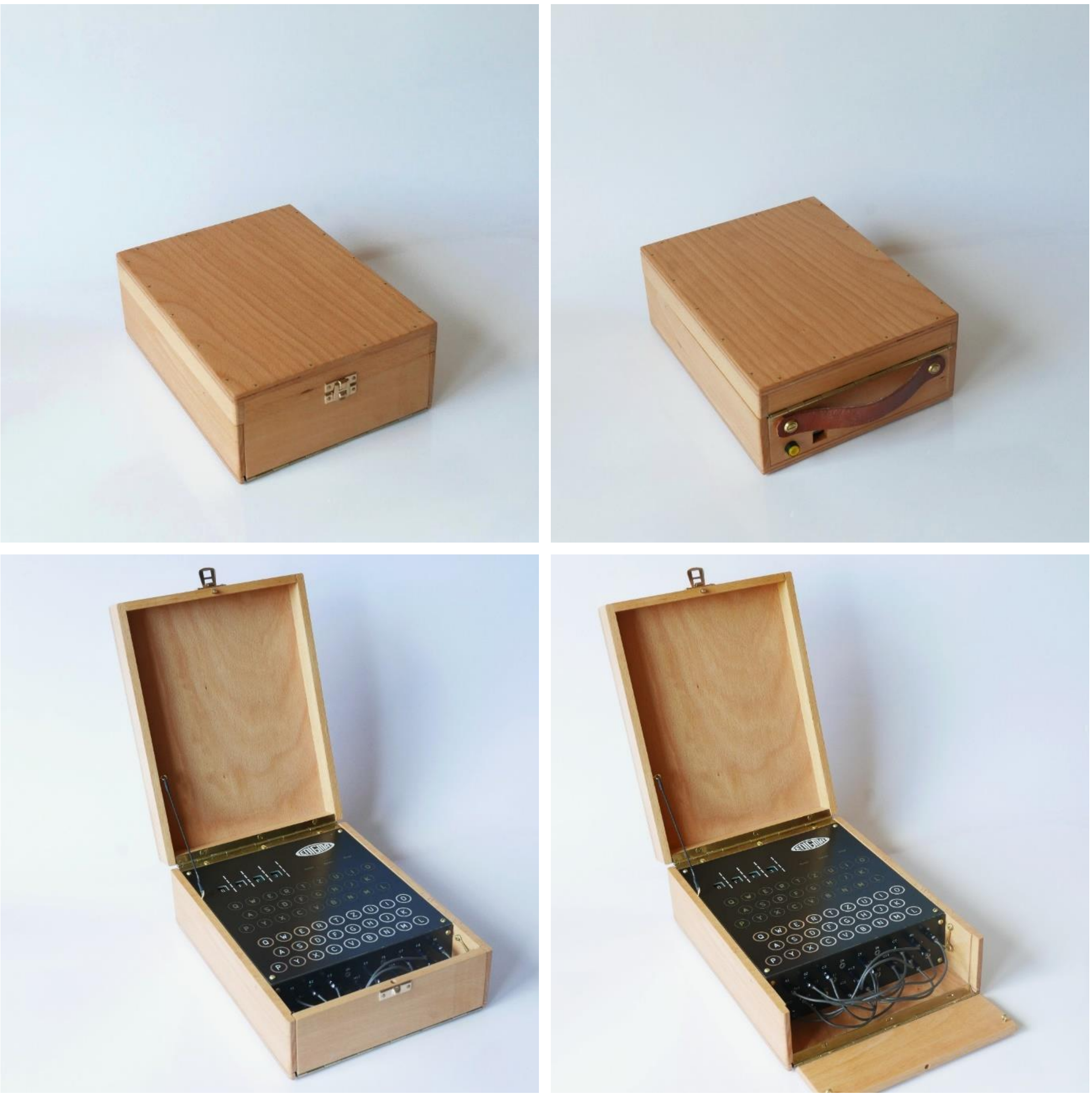
- Lid hinge and support: Most Enigma models used piano hinges to which the lid was permantly attached. The opened lid was supported by folding metal rails which were lowered between the enclosure and the Enigma when the lid was closed. For space reasons, I used a simple cord for support instead. – The Enigma M4 had two separable hinges so that its lid could be removed.

- Front hinge: On all Enigmas with plugboard and hinged front, the edges of the base plate and front flap are beveled at 45° so that the visible edge of the piano hinge aligns with the lower edge of the enclosure. I have done this in the example, but would not necessarily go to the trouble of doing it again.

- Lid lock: A recessed locking mechanism which sat flush with the box surface was used on all civilian and military Enigmas. It is very characteristic and also makes functional sense, as the transport case can be carried by the handle on the back and placed on the flat front. Unfortunately, this latch is no longer available, certainly not in a reduced scale of 2:3. I have saved myself the effort of reproducing it and have used an inexpensive cigar-box latch.

- In the original, the box sidewalls are joined with finger joints. For the sake of simplicity, I have glued them with butt joints. The lid and base are screwed to the side parts in the original; the scaled-down model uses brass nails instead.

When installing in a wooden enclosure, the **USB connection in the back of** the plugboard cannot be used. If a socket is already pre-mounted, remove it using hot air – or break it off if necessary. Instead, a panel-mounted USB-B socket can be installed, with its connection cable soldered to solder pads J2.



Enigma Touch in wooden enclosure with offset plugboard

Plugboard cables

To use the plugboard to simulate the military Enigma models I, M3, M4 or to set up the rewirable reflector D, connecting cables are required. A maximum of 10 cables are sufficient to swap letters using the plugboard, depending on the historical key settings. To configure the UKWD (reflector D, see chapter 3, Wirable reflector D), 12 cables are required.

- The matching miniature plugs (“Zwergstecker”) are mainly used in model making, for example for model railroads. Their pin diameter is 2.6 mm.
- Stranded wire with a cross-section of 0.5 mm² (AWG 20) is well suited as a cable material, with the most flexible insulation possible, e.g. made of silicone. The usual H05V-K stranded wire with a 0.75 mm² cross-section and PVC insulation tends to be too stiff.
- A cable length of 15 cm (plus plug) enables even the longest diagonal connections.
- If the plugs are too loose or too tight in the sockets of the *Enigma touch*, widen the sliced pins slightly with a knife or compress them with flat pliers.

5. Firmware updates

If new firmware versions become available, you can install them yourself. You will need a Windows PC with a USB connection to the *Enigma touch* and the freely available programming software "STM32CubeProgrammer" from the manufacturer of the CPU, ST Microelectronics.

The currently installed firmware version is displayed in diagnostic mode; see chapter 3, Diagnostic mode.

Installation via STM32CubeProgrammer

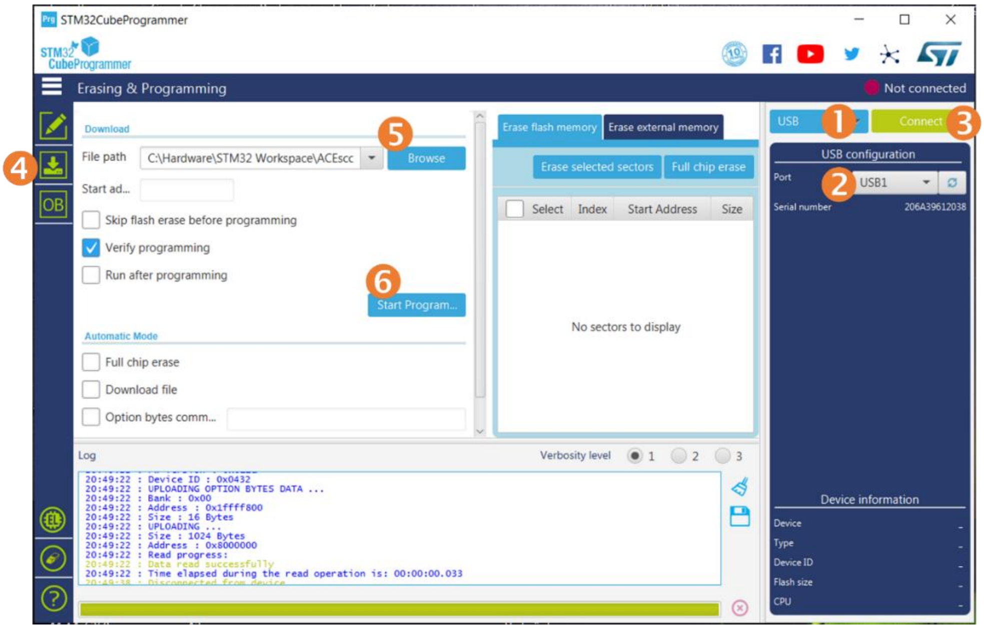
The programming software can be downloaded directly from ST Microelectronics after free registration, www.st.com/en/development-tools/stm32cubeprog.html. Without registration, a slightly older version which also uses less memory is available from German publisher Heise, www.heise.de/download/product/STM32CubeProgrammer.

New firmware is provided as an .ELF file. It can be installed as follows:

- Set switch SW35 on the back of the *Enigma touch* to PROG.
- Establish USB connection to the PC, switch on Enigma. In PROG mode there is no visual operating display, but the PC should recognize a USB device "STM32 Bootloader".
- Start the STM32CubeProgrammer software, then (see the screenshot below):

  1. Select USB interface
  2. Search port, should detect USB1
  3. Establish connection
  4. Select programming dialog
  5. Select the .ELF file, also possible via drag & drop
  6. "Start Programming"

- Acknowledge confirmation dialogs, Disconnect (3)
- Set switch SW35 back to RUN mode (or NORM for Rev 2 boards).



□ Skip flash erase before programming
☑ Verify programming
□ Run after programming

□ Full chip erase
□ Download file
□ Option bytes comm...

Verbosity level ● 1 ○ 2 ○ 3

```
20:49:22 : Device ID : 0x0432
20:49:22 : UPLOADING OPTION BYTES DATA ...
20:49:22 : Bank : 0x00
20:49:22 : Address : 0x1ffff800
20:49:22 : Size : 16 Bytes
20:49:22 : UPLOADING ...
20:49:22 : Size : 1024 Bytes
20:49:22 : Address : 0x8000000
20:49:22 : Read progress:
20:49:22 : Data read successfully
20:49:22 : Time elapsed during the read operation is: 00:00:00.033
20:49:38 : Disconnected from device
```

Firmware version history

FW006, August 2024

- Mode buttons must be pressed a little longer (ignore accidental touches)
- Battery indicator and volume display on Rev 2 boards corrected

FW005, July 2024

- Manually changing the rotor position resets the group counter for USB logging
- Click when moving the rotors is always audible even at half volume setting

FW004, June 2024

- Audio output (Rev 3 board only)
- Display of the battery charge status in the model dialog (Rev 3 board only)
- Low battery warning: flickering lights
- Better support for counter enigmas: Counter is displayed in the left rotor windows, crank symbol is displayed in the right rotor window.
- Better response of the rotor display and slider when many rotors are moving at the same time.

FW003, August 2023

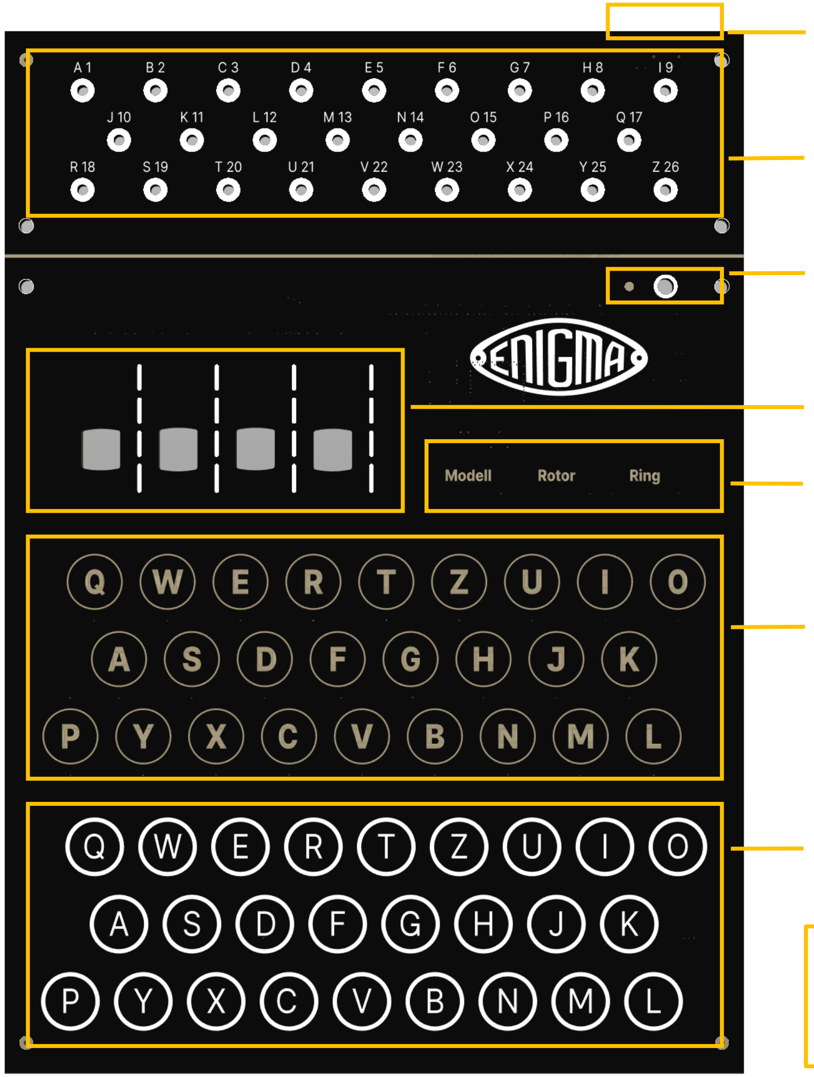
- Fixed a bug with the double step anomaly
- Error in the numbering of UKWD positions fixed
- Extended recording: plugboard and UKWD wiring are recorded
- Enigma model D added. (Similar to Enigma K, but driver notches fixed to the rotor body instead of the adjustable rings)
- Visual error message when exiting rotor mode if a rotor is selected multiple times: Faulty rotor selection windows rotate through once.

FW 002, December 2022

- First published version
- Error in the double step and in the numbering of UKWD positions!

Enigma touch Quick Reference

Controls Overview



USB-C port: 5V power supply, optional data logging. Recharge battery when lamps begin to flicker!

Plug board, active for Enigma models I, M3, and M4. Connect pairs of letters as specified in the code settings. Also used to re-wire reflector D via *Modell* mode key.

Power button; Enigma state is preserved. Automatic shutdown after 15 minutes of inactivity. Charging indicator (if LiPo battery installed), or 5V power supply indicator.

Rotor display, sliders to “turn” rotors. Used during encryption and for machine setup.

Setup mode buttons, see table on back for details. This is a feature of the *Enigma touch* replica only. All mode lights are off in normal encryption mode.

Lamp board displays encrypted or decrypted characters. There is no difference between encryption and decryption mode, since the Enigma code is symmetrical (self-inverse).

Keyboard for character input. Press and hold a key until the rotors have moved and a lamp lights up.

Introduction to the real Enigma:
www.cryptomuseum.com
youtu.be/ybkkiGtJmkM

Enigma Models Replicated by Enigma touch

Machine descriptions and rotor wiring details:
See www.cryptomuseum.com/crypto/enigma
and www.cryptomuseum.com/crypto/enigma/wiring.htm

Display	Machine	Description
I	Enigma I	First military version (Army), with plug board. Only Enigma with numeric rotor labels.
M3	M3	Navy Enigma, 3 rotors.
M4	M4	Navy (submarine) Enigma, 4 rotors.
D	Enigma D	Early variant, notches on rotors, not rings
K	Enigma K	Commercial version, 3 rotors, reflector settable but not stepping, no plug board.
KD	Enigma K, Reflector D	Model K with rewirable reflector, used by Mil Amt intelligence service.
KR	Railway K	Model K, rotor wiring for German Railway.
KS	Swiss K	Model K, rotor wiring for Swiss Army.
T	Tirpitz	Model K variant for Japanese forces. Choice of 8 rotors, 5 turnover positions each.
G	Enigma G (or G31)	Cogwheel mechanism instead of levers to step rotors and reflector. Frequent turnovers, manual back/forth stepping via crank.
G1	Enigma G111	Model G, rotor wiring for Hungarian Army. Only rotors I, II, V are preserved.
G2	Enigma G219	Model G, rotor wiring for Dutch Navy.
G3	Enigma G312	Model G, rotor wiring for German intelligence service (Abwehr).

Mode Buttons for Machine Setup

Touch any button to activate the corresponding setup mode.
Touch active mode button again to return to encryption mode.
Hold any button for 1second for extended functions.

Mode	Description
Modell	Select the Enigma model to be simulated; choose replica settings: audio volume, lamp brightness and verbosity for USB logging.
Rotor	Select the active rotor set and reflector (where applicable). You cannot leave this mode when a rotor has been selected more than once.
Ring	Set the rotors' index rings (position of lettering relative to the internal wiring)
Modell (long press)	Set up reflector D – reflector D can be rewired by the user. Make the desired connections on the plug board, then long-press *Modell*. Letters J and Y must be paired or open, all other letters must be paired! Displays "D OK" if wiring is valid, "D ??" if not.
Rotor (long press)	View Rotor Wiring – display the internal wiring of all rotors and the reflector (left). Useful to inspect rewirable reflector D.
Ring (long press)	Crank Mode – for the Enigma G models, enables cranking the complete set of geared rotors back and forth. Use the rightmost slider to turn the crank. Press any mode button to leave crank mode.

Enigma touch Quick Reference – Rev 3.0 for PCB Rev 3
juergen@e-basteln.de, www.e-basteln.de