Enigma touch Bedienungsanleitung

Jürgen Müller, juergen@e-basteln.de
Version 1.0, 24.8.24

Diese Anleitung beschreibt die Platinenversion Rev. 3 mit Firmware 006.
Abweichungen für die Platinenversion Rev. 2 sind im Text angegeben.

Inhalt

1. Einführung

Die Enigma touch

Die *Enigma touch* ist ein elektronisches Funktionsmodell der Enigma-Schlüsselmaschine. Verschiedene zivile und militärische Varianten der Enigma aus den 1930er und 40er Jahren werden nachgebildet.

Ein einfacher Einplatinen-Aufbau soll das Erscheinungsbild und die Funktion möglichst getreu nachbilden. Elektronische Bauteile sind ausschließlich auf der Unterseite der Platine als SMD-Komponenten bestückt. Die Oberseite bleibt frei und ist der Front der Original-Enigma nachempfunden, etwa im Maßstab 2:3.

Die Platine selbst übernimmt dabei viele Funktionen: Neben der Frontplatte bildet sie die kapazitive Tastatur, Diffusoren und Buchstabenmasken für das Lampenfeld, Buchsen für das Steckerbrett und einen Resonanzboden für den Piezo-Lautsprecher. Kleine grafische Displays unter der Platine zeigen die Stellung der Schlüsselwalzen; kapazitive Schieberegler bilden die Zahnkränze nach, mit denen die Walzen gedreht werden können.

Die *Enigma touch* ist vor allem für den einfachen Aufbau als flaches Einplatinen-Modell gedacht. Das Steckerbrett der militärischen Enigma-Varianten ist dabei zur besseren Handhabung hinten angeordnet. Es kann aber auch abgetrennt werden, um die *Enigma touch* in ein Holzgehäuse einzubauen, das der Original-Anordnung entspricht.

Diese Anleitung

Die vorliegende Anleitung beschreibt die *Enigma touch*-Replika. Auf die Original-Enigma wird nur dort kurz eingegangen, wo es als Kontext für die Funktion der Replika erforderlich ist. Ein Grundverständnis der Enigma-Funktion wird vorausgesetzt; der folgende Abschnitt empfiehlt einige Quellen im Internet dazu.

Kapitel 2 erklärt die grundlegende Bedienung der Enigma und der Replika – das Einrichten der Enigma und das Ver- und Entschlüsseln. Spezielle Enigma-Modelle und zusätzliche Funktionen der Replika sind in Kapitel 3 beschrieben. Kapitel 4 gibt Hinweise zum Aufbau der *Enigma touch*, und Kapitel 5 zu künftigen Firmware-Updates.

Quellen zur Original-Enigma

Hervorragende 3D-Animation von Jared Owen, die das **Funktionsprinzip der Enigma** erklärt. Knapp 20 Minuten, Originalton auf Englisch, eine maschinell generierte deutsche Tonspur ist verfügbar. Unbedingt empfehlenswert!
https://www.youtube.com/watch?v=ybkkiGtJmkM

Eine sehr umfangreiche, gut strukturierte und reich bebilderte Darstellung der **Enigma-Maschinen**, von zwei holländischen Sammlern (in englischer Sprache). Der Fokus liegt auf den Maschinen selbst, mit Exkursen zu ihrer Verwendung.
https://www.cryptomuseum.com/crypto/enigma/

Funktionsprinzip, **militärische Verwendung und Dechiffrierung der Enigma**. Umfangreiche Website, ursprünglich erstellt von Tony Sale, dem ersten Kurator des Museums in Bletchley Park. (In englischer Sprache.)
https://www.codesandciphers.org.uk/enigma/

Sehr umfangreiche Sammlung von Veröffentlichungen, Webseiten und eigenen Arbeiten zur **Geschichte und Crypto-Analyse der Enigma**, von Frode Weierud, einem norwegischen Amateur-Kryptologen. (In englischer Sprache.)
https://cryptocellar.org/enigma/

Die deutsche Wikipedia bietet mehrere umfangreiche Seiten zur Enigma, die einen guten **Überblick in deutscher Sprache** bieten. Als Einstieg hier die Hauptseite zur Enigma; weitere Wikipedia-Seiten sind von dort verlinkt:
https://de.wikipedia.org/wiki/Enigma_(Maschine)

Historische Beispielnachricht mit **Tutorial zur Dekodierung:**
https://www.cryptomuseum.com/crypto/enigma/msg/p1030681.htm

Erläuterung der verschiedenen militärischen **Schlüsselprozeduren**, die verwendet wurden (Tagesschlüssel, Spruchschlüssel, Kenngruppen…)
https://de.wikipedia.org/wiki/Enigma-Schl%C3%BCsselprozedur
https://www.ciphermachinesandcryptology.com/en/enigmaproc.htm

Original-Nachrichten, an deren Entschlüsselung Sie sich versuchen können:

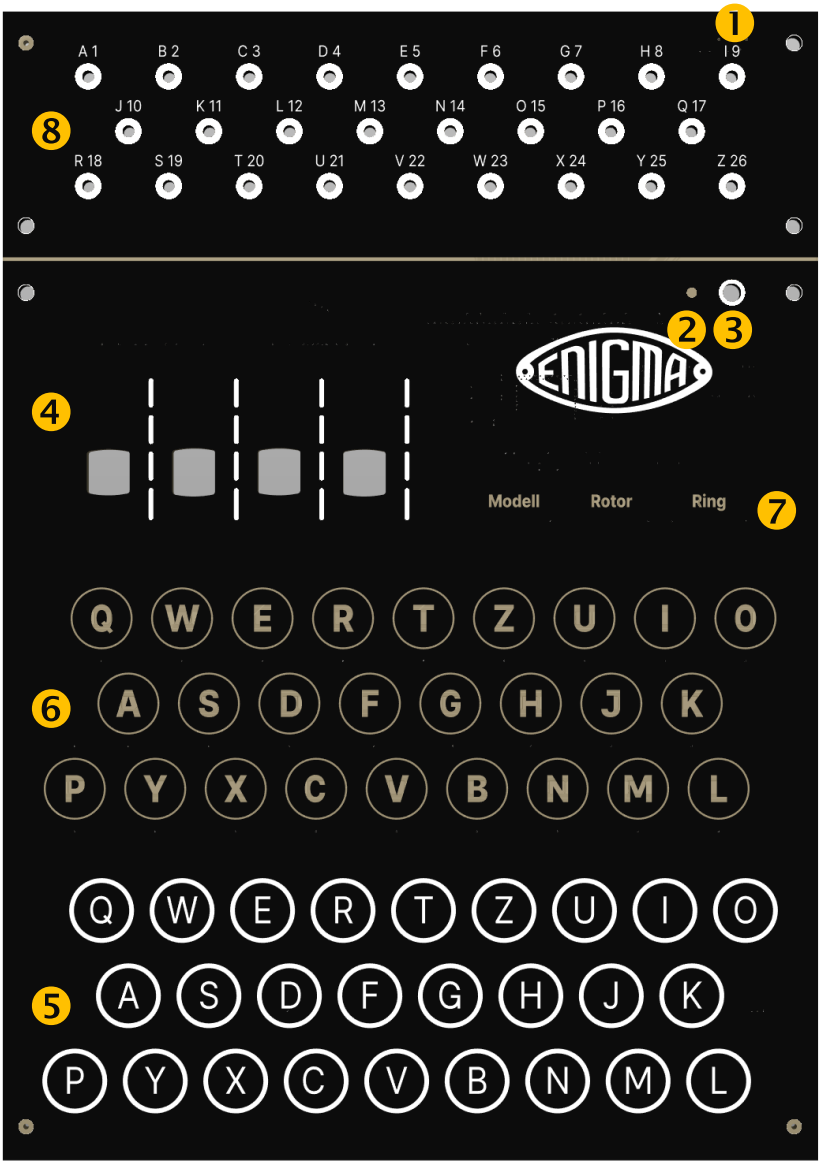
Viele M4-Nachrichten:
https://enigma.hoerenberg.com/index.php?cat=The%20U534%20messages

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

Ein paar Nachrichten für verschiedene Enigma-Modelle, incl. K und T-Modell.
http://wiki.franklinheath.co.uk/index.php/Enigma/Sample_Messages

2. Bedienung – Grundfunktionen

Überblick und erste Schritte



1. Schließen Sie an der **USB-C-Buchse** an der Rückseite ein 5V-Netzteil an, um die *Enigma touch* mit Strom zu versorgen und ggf. den eingebauten Lithium-Polymer-Akku aufzuladen. 5V/50mA bei Betrieb ohne Akku, 5V/250mA bei Betrieb und gleichzeitiger Akku-Ladung.
2. Die **LED** leuchtet, solange der Akku geladen wird, oder (bei Aufbau ohne Akku) wenn 5V an der USB-Buchse anliegen.
3. Schalten Sie die *Enigma touch* am **Ein-/Ausschalter** ein. Der Zustand – ausgewähltes Enigma-Modell, Bestückung und Position der Schlüsselwalzen – bleibt beim Aus- und Einschalten erhalten. Die Maschine startet immer im normalen Verschlüsselungsmodus. Nach 15 Minuten ohne Benutzeraktivität schaltet die *Enigma touch* sich automatisch aus.

4. Die Anzeigen für die **Walzen (Rotoren)** leuchten auf, sobald die *Enigma touch* eingeschaltet ist. Die Reihenfolge und Rotation der Walzen bestimmen die aktuelle Buchstabenvertauschung beim Ver- oder Entschlüsseln. In den Sichtfenstern kann die aktuelle Stellung jeder Walze abgelesen werden. Die gestrichelten Linien neben jedem Fenster stellen die Zahnkränze dar, mit denen sich die Walzen verdrehen lassen.

   Nur die Startposition zu Beginn einer Verschlüsselung wird über die Zahnkränze eingestellt, danach bewegen sich die Rotoren automatisch weiter. In den Sichtfenstern wird *nicht* der Schlüsseltext angezeigt – der erscheint im Lampenfeld.

5. Die **Tastatur** dient zur Eingabe des Klar- oder Schlüsseltexts. Jeder Tastendruck bewegt einen oder mehrere Rotoren einen Schritt vorwärts – im Original durch eine direkte mechanische Kopplung mit großem Tastenhub – und lässt dann eine Lampe aufleuchten.

6. Das **Lampenfeld** zeigt die Buchstaben des ver- bzw. entschlüsselten Textes an. Wie bei der Original-Enigma leuchtet eine Lampe nur so lange auf, wie eine Taste gedrückt gehalten wird.

   Die Enigma kennt keinen Unterschied zwischen Verschlüsselungs- und Entschlüsselungsmodus! Die Verschlüsselung ist symmetrisch (selbst-invers) – wenn ein verschlüsselter Text mit dem gleichen Starteinstellungen ein weiteres Mal verschlüsselt wird, kommt wieder der Klartext heraus.

   Sie können jetzt direkt mit dem Verschlüsseln oder Entschlüsseln beginnen, mit dem aktuell eingestellten Enigma-Modell und der dafür ausgewählten Walzenbestückung: Stellen Sie die Startposition der Walzen ein und beginnen Sie, Text einzugeben und den Schlüsseltext von den Lampen abzulesen und zu notieren. Wenn Sie zuvor ein anderes Enigma-Modell auswählen und einrichten möchten, geschieht das über die Modus-Taster der Replika:

7. Die **Modus-Taster** gibt es nur an der Replika, nicht an der Original-Enigma. Hier werden das simulierte Enigma-Modell und die eingesetzten Schlüsselwalzen ausgewählt, die verstellbaren Ringe an den Walzen eingestellt, und einige Replika-Einstellungen geändert. Details dazu sind im folgenden Abschnitt beschrieben.

8. Das **Steckerbrett** nutzen wir in diesem Kapitel noch nicht. Es wird nur bei einigen militärischen Enigma-Modellen (I, M3, M4) verwendet und ist im Kapitel 3 beschrieben.

Einrichten der Enigma

Die Modus-Taster (7) sind als „Radio Buttons“ ausgeführt: Antippen eines Tasters wählt den jeweiligen Einricht-Modus und lässt den Taster aufleuchten. Antippen eines anderen Modus-Tasters schaltet auf dessen Einricht-Modus um; nochmaliges Antippen des gerade aktiven Tasters schaltet zurück in den regulären Verschlüsselungs-Modus. Damit sie nicht versehentlich betätigt werden, müssen die Modus-Tasten einen kurzen Moment gedrückt bleiben (ca. 0,3 Sekunden).

In jedem Einricht-Modus zeigen die Walzen unterschiedliche Informationen an und können über die „Zahnkränze“ verstellt werden. Die Modus-Taster sind doppelt belegt: Längeres Halten (1 Sekunde) löst eine zweite Funktion aus. Diese fortgeschrittenen Funktionen sind in Kapitel 3 beschrieben.

Zur Einrichtung eines neuen Enigma-Modells und der – in den Original-Schlüsselvorschriften meist täglich wechselnden – Schlüsseleinstellungen werden die Modus-Tasten von links nach rechts durchlaufen.

Wird eine Einstellung verändert, dann werden die davon abhängigen Einstellungen (Tasten weiter rechts) auf Standardwerte zurückgesetzt. Nach den aktuellen Einstellungen zu schauen, ohne etwas zu verändern, ist aber jederzeit möglich und verändert die abhängigen Einstellungen nicht.

Modell und Replika-Einstellungen

Die Modell-Taste erlaubt die Wahl des simulierten Enigma-Modells und einiger Replika-spezifischer Einstellungen. Von links nach rechts in den Rotorfenstern:

- **Auswahl des Enigma-Modells**. Die Tabelle unten gibt einen Überblick; Details zu den simulierten Maschinen z.B. unter www.cryptomuseum.com/crypto/enigma.
- Einstellung der **Audio-Lautstärke** (nur Platine Rev 3). Buchstabentastatur und Rotorbewegung erzeugen unterschiedliche Klick-Geräusche, Modus-Taster einen höheren Bestätigungston, Fehler beim Einrichten einen „Kuckuck"-Hinweiston.
- Einstellung der **Lampenhelligkeit** in fünf Stufen.
- Einstellung der **Protokoll-Detailstufe** – siehe Kapitel 3, Mitschrift über USB.
- Ganz rechts wird außerdem der **Akku-Ladestand** angezeigt. Platine Rev 2 unterstützt nur die Anzeige einer Warnung bei sehr niedrigem Ladestand, Rev 3 zusätzlich den ungefähren Ladestand in drei Stufen.

Display	Modell	Beschreibung
I	Enigma I	Erste militärische Version (Reichswehr). Steckerbrett, numerische Walzenbeschriftung.
M3	M3	Marine-Enigma, 3 Walzen.
M4	M4	U-Boot Enigma, 4 Walzen.
D	Enigma D	Frühe Version, Mitnehmer fest an den Rotoren.
K	Enigma K	Kommerzielle Version, 3 Walzen, UKW einstellbar aber nicht angetrieben.
KD	Enigma K, UKW D	Modell K mit frei verdrahtbarer UKW, für Geheimdienst Militärisches Amt.
KR	Reichsbahn	Modell K, Walzen für Reichsbahn.
KS	K Schweiz	Modell K, Walzen für Schweizer Armee.
T	Tirpitz	Modell K Variante für japanische Streitkräfte. 8 Walzen zur Wahl, mit je 5 Schaltpositionen.
G	Enigma G (G31)	Zahnräder statt Hebel bewegen Walzen und UKW. Viele Schaltpositionen, Kurbel für Positions-Korrektur vor/zurück.
G1	Enigma G111	Modell G, Walzen für ungarische Armee. Nur Walzen I, II, V sind erhalten.
G2	Enigma G219	Modell G, Walzen für holländische Marine.
G3	Enigma G312	Modell G, Walzen für deutschen Geheimdienst (Abwehr).

Walzen-Bestückung

Die Rotor-Taste erlaubt die Auswahl der Walzen und – bei einigen Maschinentypen – der Umkehrwalze (Reflektor).

- Die **Walzenbestückung** ist Teil des Schlüssels, der allen Teilnehmern bekannt sein musste. Der Schlüssel änderte sich in der Regel täglich, wurde vorab festgelegt und unter Geheimhaltung mitgeteilt – etwa in einer gedruckten Schlüsselliste für einen Monat im Voraus. Walzen sind immer mit römischen Zahlen nummeriert und im Schlüssel notiert.
- In der Original-Enigma wurde die komplette Welle mit den Schlüsselwalzen aus der Maschine genommen, die Walzen abgezogen und in unterschiedlicher Reihenfolge neu montiert. Zu einigen militärischen Enigma-Modellen gehörte ein größerer Walzensatz, so dass drei Walzen aus einem Satz von fünf bis acht Walzen ausgewählt wurden, um die Anzahl der möglichen Schlüssel zu vergrößern.
- Details zu den verfügbaren Walzen und ihrer internen Verdrahtung finden sich auf www.cryptomuseum.com/crypto/enigma und www.cryptomuseum.com/crypto/enigma/wiring.htm.
- In der *Enigma touch* werden die verfügbaren Walzen in den Rotor-Sichtfeldern angezeigt und ausgewählt. Da für eine Maschine jeder Walzentyp (römische Zahl) nur einmal vorhanden ist, können gültige Walzenkombinationen jeden Typ nur einmal verwenden. Wenn eine Walze doppelt ausgewählt ist, ist es nicht möglich, den Rotor-Modus zu verlassen – es wird ein Fehlerton ausgegeben, und die doppelt gewählten Walzen werden als optischer Hinweis einmal durchrotiert.
- Im linken Sichtfenster kann bei einigen Maschinentypen die **Umkehrwalze** ausgewählt werden. Sie ist mit einem Buchstaben bezeichnet. Bei der Enigma M4 wird an dieser Stelle die gewünschte Kombination aus Umkehrwalze (B, C) und dünnem vierten Rotor („Griechenwalze“ β, γ) eingestellt, oder alternativ die dickere, frei verdrahtbare Umkehrwalze D.

Ringstellung

Die umlaufende Buchstaben-Beschriftung ist nicht fest auf den Enigma-Walzen aufgebracht, sondern auf einem Ring, der relativ zum Walzenkörper verdreht werden kann. In der *Enigma touch* gelangt man über die Ring-Taste zur Einstellung dieser Ringe.

Bei fast allen Enigma-Typen ist der Mitnehmer-Mechanismus, der die Bewegung der Nachbarwalze steuert, an diesen Ring gekoppelt. Durch Verdrehen des Rings lässt sich also verändern, bei welcher Stellung der Kontaktwalze die Nachbarwalze bewegt wird. Dies vergrößert die Anzahl der möglichen Schlüssel massiv. Auch die **„Ringstellung“** gehört zum vorab festgelegten (Tages-)schlüssel.

Die drei normalen Rotoren tragen bei sämtlichen simulierten Enigma-Modellen einen einstellbaren Ring. Bei Modellen mit einstellbarer oder mitlaufender Umkehrwalze (Enigma D, G, K, T) trägt diese Umkehrwalze ebenfalls einen Ring, der im linken Fenster eingestellt werden kann. Bei der Enigma M4 ist im linken Fenster der Ring der schmalen „Griechenwalze“ einstellbar.

Schlüsselprozedur: Verschlüsseln einer Nachricht

Damit eine verschlüsselte Nachricht vom Empfänger wieder entschlüsselt werden kann, müssen Sender und Empfänger natürlich den gleichen Schlüssel verwenden. Die Walzenbestückung und Ringstellung waren immer für einen bestimmten Zeitraum (in der Regel 24 Stunden) festgelegt. Monatliche Schlüssellisten mit diesen „Tagesschlüsseln" mussten vorab in gedruckter Form auf sicherem Weg zu allen Teilnehmern eines Funknetztes gebracht werden. Die Anfangsstellung der Rotoren wurde für jede Nachricht neu gewählt und als „Spruchschlüssel" vor der eigentlichen Nachricht verschlüsselt übertragen.

Wie das im Detail geschah, variierte im militärischen Einsatz zwischen Heer, Luftwaffe und Marine; einzelne Abläufe wurden mit der Zeit auch verändert. Einen Überblick über diese „Schlüsselprozeduren" gibt https://www.ciphermachinesandcryptology.com/en/enigmaproc.htm (Dirk Rijmenants, englisch), oder die Wikipedia auf https://de.wikipedia.org/wiki/Enigma-Schl%C3%BCsselprozedur (deutsch).

In diesem Abschnitt soll beispielhaft gezeigt werden, wie eine Nachricht bei Heer oder Luftwaffe verschlüsselt und übermittelt wurde – und zwar nach September 1938, als die Handhabung des Spruchschlüssels verändert wurde, um eine kryptografische Schwachstelle zu beheben.

eheime Kommandosache!
cht ins Flugzeug mitnehmen

Armee-Stabs-Maschinenschlüssel Nr. 28

für Oktober 1944

Nr. 00008

	Datum	Walzenlage			Ringstellung			Steckerverbindungen										Kenngruppen			
t	31.	IV	V	I	21	15	16	KL	IT	FQ	HY	XC	NP	VZ	JB	SB	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	YI	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	vex
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	II	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	XB	YN	IJ	oxd	lnb	icu	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

Beispiel: Schlüsseltafel für die Enigma I

Enigma einrichten

- Wir verwenden aus der abgebildeten Schlüsseltafel den **Tagesschlüssel** für den 31. des Monats (erste Tabellenzeile).
- Modell **Enigma I** auswählen (den bei Heer und Luftwaffe eingesetzten Typ).
- Rotor-Einstellung: ganz links **Umkehrwalze B** wählen (die während des Kriegs eingesetzte Umkehrwalze), sowie **Rotoren IV, V, I** gemäß Tagesschlüssel (von links nach rechts).
- Ring-Einstellung: **Ringstellungen 21, 15, 16** auswählen (von links nach rechts).
- Auf dem Steckerbrett mit 10 Kabeln die im Tagesschlüssel angegebenen Buchstabenpaare verbinden.

Nachricht vorbereiten

- Der Klartext einer Nachricht wird zunächst auf den beschränkten Enigma-Zeichensatz angepasst. Die wichtigsten Konventionen:
    - Leerzeichen werden weggelassen.
    - Umlaute Ä, Ö, Ü werden zu A, O, U.
    - Ein Punkt am Satzende wird als „X“ kodiert, ein Doppelpunkt als „XX“, die häufige Buchstabenfolge CH als „Q“.
    - Zahlen werden in Worten ausgeschrieben: NULL, EINS, ZWO, DREI, VIER, FUNF, SEQS, SIEBEN, AQT, NEUN.
    - Die Buchstaben werden zur besseren Übersicht in Fünfergruppen gruppiert und am Ende ggf. mit XX aufgefüllt.
- Also wird aus der Nachricht: „Wetterbericht: Heute sonnig, Höchsttemperatur 26 Grad“ der zu übermittelnde Text: WETTE RBERI QTXXH EUTES ONNIG XHOQS TTEMP ERATU RZWOS EQSGR ADXXX

Spruchschlüssel wählen und verschlüsseln

- Zum Verschlüsseln einer Nachricht wählt der Operator eine zufällige Anfangsstellung der Rotoren, den **Spruchschlüssel**. Dieser muss natürlich auch dem Empfänger übermittelt werden. Das geschieht aber nicht im Klartext, sondern der Spruchschlüssel wird seinerseits verschlüsselt.
- Dazu wählt der Operator eine weitere zufällige Rotorstellung, die **Grundstellung**, die zunächst an den Rotoren eingestellt wird. Mit dieser Grundstellung wird der Spruchschlüssel kodiert. Grundstellung und kodierter Spruchschlüssel werden dann im Nachrichtenkopf an den Empfänger übermittelt.
- Also beispielsweise:
    - Grundstellung zufällig wählen und auf den Rotoren einstellen – z.B. DXF.
    - Spruchschlüssel zufällig wählen und verschlüsseln – z.B. RKU wird zu FGI.
    - Im Nachrichtenkopf wird übermittelt: DXF FGI

Klartext verschlüsseln

- Spruchschlüssel RKU auf den Walzen einstellen.
- Klartext eingeben, Schlüsseltext notieren.
- Aus WETTE RBERI QTXXH EUTES ONNIG XHOQS TTEMP ERATU RZWOS EQSGR ADXXX wird LBUSL ZJAQF YJHCV NFLFT XDIUU MQKCD ULDDA JKSRT VQBRN NEKRA RGEZM.

Nachrichtenkopf und Kenngruppe hinzufügen

- Vor dem Schlüsseltext wird noch eine weitere Fünfergruppe eingefügt, die angibt, welcher Tagesschlüssel verwendet wurde – wichtig bei Nachrichten, die z.B. erst am nächsten Tag den Empfänger erreichen. Um diese Information etwas zu verschleiern, wählt man eine beliebige der vier **Kenngruppen** aus dem Tagesschlüssel und stellt ihr noch zwei zufällige Buchstaben voran – z.B. DANCJ.
- Davor wird noch der Nachrichtenkopf übermittelt:
  Uhrzeit – Buchstabenzahl incl. Kenngruppe – Grundstellung – verschlüsselter Spruchschlüssel

- Also lautet die komplette Nachricht: **1630 = 60 = DXF FGI =**
  DANCJ LBUSL ZJAQF YJHCV NFLFT XDIUU MQKCD ULDDA JKSRT VQBRN NEKRA RGEZM

Übungsnachricht

- Die folgende (fiktive) Nachricht wurde frühmorgens am 29. Oktober übermittelt. Können Sie sie entschlüsseln?
- **0030 = 35 = LTY JCH = HSZQJ BRSLM DMSPX JALYV DYROG JDETL BPUXN**

Pflege der Enigma touch

Reinigung

Die seidenmatte Front kann durch Fingerspuren etwas glänzender werden, meist an den häufig berührten Flächen der Schieberegler und der Modus-Tasten. In der Regel genügt ein mit etwas Wasser befeuchtetes weiches Tuch, um wieder eine einheitliche Oberfläche zu erzielen.

Bei hartnäckigerer Verschmutzung kann auch ein mit Spülmittel-Lösung oder Glasreiniger befeuchtetes Tuch verwendet werden. Die Reiniger entfernen aber auch vorher aufgebrachte Pflegemittel und führen oft dazu, dass berührte Flächen sich anschließend umso schneller wieder vom Rest der Front unterscheiden. Sie sollten also nur bei Bedarf eingesetzt werden.

Gelegentliches Abwischen mit Kunststoff-Pflegemittel oder Silikonöl (Überstand und Schlieren mit einem weichen Tuch wieder abwischen) verringert die Empfindlichkeit für Fingerabdrücke und liefert wieder eine tiefschwarze Oberfläche.

Akkumulator

Lithium-Ionen-Akkumulatoren sollen möglichst nicht vollständig entladen gelagert werden, um ihre Kapazität zu erhalten. Die Schutzschaltung im Akku schützt vor Tiefentladung, aber es ist empfehlenswert, vor einer langen Einlagerung den Akku noch einmal etwas aufzuladen.

In der *Enigma touch* wird der Akku mit 200 mA Ladestrom geladen. Akkus mit einer Kapazität von 500 bis 1000 mAh sollten also in 2½ bis 5 Stunden vollständig geladen sein und dann eine Betriebszeit von 10 bis 20 Stunden oder eine Einlagerungszeit von mindestens 2 Jahren liefern.

Sollte der Akkumulator aufgebläht sein oder äußere Beschädigungen aufweisen, bitte nicht mehr verwenden! Beim Lösen des Akkus von der Platine (doppelseitiges Klebeband) eine feuerfeste Unterlage verwenden und Schutzbrille tragen. Akku fachgerecht entsorgen.

3. Spezielle Enigma-Modelle, erweiterte Funktionen

Steckerbrett

Die militärischen Enigma-Varianten I, M3 und M4 sind mit einem Steckerbrett ausgestattet. Im Original ist es senkrecht vor dem Bedienfeld angeordnet, bei der *Enigma touch* dahinter.

Auf dem Steckerbrett können Buchstaben paarweise verbunden werden. Dadurch werden sie vertauscht, einmal vor dem Eintritt in die Rotoren und nochmals nach dem Austritt vor dem Weg zum Lampenfeld. Im Original wurden hierzu Verbindungskabel mit zweipoligen Steckern und gekreuzten Leitungen verwendet. Gefederte Kurzschlussbügel in den zweipoligen Buchsen bildeten bei unverbundener Buchse den jeweiligen Buchstaben auf sich selbst ab.

Die *Enigma touch* verwendet einpolige Verbindungen zwischen den Buchstabenpaaren und berücksichtigt sie bei der Verschlüsselung, wenn eines der Modelle I, M3 oder M4 aktiv ist. Verbindungen können jederzeit gesteckt und verändert werden.

Technisch kann eine beliebige Anzahl von 0 bis 13 Kabeln gesteckt werden. In den historischen Schlüsselprozeduren wurden zwischen 5 und 10 Verbindungen vorgegeben – die verwendete Anzahl stieg über die Jahre. Kryptografisch optimal wären 11 Verbindungen gewesen, da sich so die höchstmögliche Anzahl an verschiedenen Kombinationen ergibt.

Die Anordnung und Beschriftung der Buchsen variierten zwischen den Enigma-Modellen. Um alle Modelle simulieren zu können, verwendet die *Enigma touch* eine Kombination, die es in genau dieser Form nicht an den Original-Maschinen gab: die kombinierte alphabetisch/numerische Beschriftung der frühen Varianten M1/M2, in der regelmäßigen numerisch aufsteigenden Anordnung des Modells M4. So kann das Steckerbrett gleichzeitig auch als Übersetzungstabelle alphabetisch/numerisch dienen, die bei manchen Maschinen als Teil der Gebrauchsanweisung im Deckel angebracht war.

Verdrahtbare Umkehrwalze D

Mehrere Enigma-Varianten, sowohl für den zivilen wie den militärischen Einsatz, nutzten eine spezielle Umkehrwalze „Dora“ (kurz: UKWD), die vom Anwender verdrahtet werden konnte. In der *Enigma touch* kann die UKWD in den Enigma-Typen KD, M3 und M4 eingesetzt werden.

Die UKWD konnte geöffnet werden, um die Buchstaben paarweise durch kurze Kabel neu zu verbinden. Nur ein Buchstabenpaar (J-Y) war fest verbunden – mehr dazu im Abschnitt „Besonderheiten“ weiter unten. Die manuelle Verkabelung der UKWD war aufwendig; daher wurde sie nicht täglich, sondern z.B. wöchentlich neu verdrahtet. Die nötigen Verbindungen sind als Buchstabenpaare auf den monatlichen Schlüsseltafeln notiert.

Auch an der *Enigma touch* muss diese Walze von Hand verdrahtet werden, und zwar über das Steckerbrett:

- 12 oder 13 Verbindungen stecken.
- Taste Modell drücken und halten.
- Nach einer Sekunde erscheint in der Anzeige „D OK“, wenn die Verkabelung vollständig und gültig ist. Sonst erscheint „D ??“ und es ertönt ein Fehlerton.

- Eine gültige Verkabelung muss alle 26 Buchstaben paarweise verbinden. Dabei muss das Paar J-Y verbunden sein, oder dieses Paar darf als einziges unverbunden bleiben.
- Alternativ kann die Verkabelung in der Bletchley-Park-Notation vorgenommen werden (s. unten). Dies erkennt die *Enigma touch* daran, dass nicht das Paar J-Y verbunden oder offen ist, sondern stattdessen die Buchstaben B-O gepaart sind.
- Eine mit „D OK“ übernommene Verdrahtung wird dauerhaft gespeichert und ist auch nach einem Neustart weiter verfügbar. Bei ungültigen Verdrahtungen wird die zuvor gespeicherte Belegung der UKWD nicht verändert.

Besonderheiten

In Deutschland wurden die Buchstabenpositionen der UKWD in unregelmäßiger Weise alphabetisch bezeichnet: Die Umlaufrichtung ist der der normalen Walzen entgegengesetzt, und die Positionen von J und Y sind verschoben. Den britischen Codebrechern war dies nicht bekannt, und sie verwendeten für die Analyse der UKWD eine „Bletchley-Park-Notation“ mit regulärer Laufrichtung. In historischen Schlüsseltafeln findet man die deutsche, in Unterlagen zu Dechiffrierung in Bletchley Park die britische Notation. Daher unterstützt die *Enigma touch* beide Eingabeformate.

Zwei Buchstaben waren nicht vom Anwender frei verdrahtbar, sondern fest gepaart. Die originale UKWD hatte an den entsprechenden Positionen Montageschrauben, so dass kein Platz für Schraubklemmen blieb. In deutscher Notation sind dies die Buchstaben J und Y, in britischer die Buchstaben B und 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
Deutsche 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

Bezeichnung der UKWD-Kontakte nach deutscher und britischer Notation.
Die fett hervorgehobenen Positionen sind durch eine feste Drahtbrücke verbunden.

Bei der ersten Inbetriebnahme der *Enigma touch* ist die UKWD so verdrahtet wie in der Enigma KD, die im Jahr 2009 im Archiv des Schwedischen Nachrichtendienstes FRA wiederentdeckt wurde, vgl. https://cryptomuseum.com/crypto/enigma/k/kd.htm. Diese Belegung bleibt so lange erhalten, bis eine gültige neue Verdrahtung gesteckt und gespeichert wurde. Die vorbelegte Verdrahtung kann anschließend nicht wieder abgerufen werden, sondern muss bei Bedarf neu gesteckt und gespeichert werden.

Eingang	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
Ausgang, 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
Ausgang, Deutsche 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

Standardverdrahtung der UKWD nach Erstinstallation der Enigma touch-Firmware.

Zählwerks-Maschinen (Enigma G)

Der Mitnehmer-Mechanismus, der die Rotoren der klassischen Enigma weiterbewegt, ist nicht reversibel: Wenn ein Rotor seinen Nachbarn „mitnimmt“, dann kann der Anwender – zur Korrektur eines Tippfehlers – zwar den Rotor auf die vorige Stellung zurückdrehen, aber der Nachbar-Rotor wird nicht automatisch mit zurückbewegt. Wenn der Anwender dessen Bewegung nicht beobachtet

hat und sie ebenfalls von Hand zurückdreht, entsteht eine falsche Rotorstellung, und die komplette nachfolgende Verschlüsselung ist ungültig.

Bereits im Jahr 1928 wurde daher eine alternative Mechanik entwickelt, bei der die Rotoren durch ein Getriebe fest verkoppelt waren. Mit einer kleinen einsteckbaren Kurbel konnte der Anwender den kompletten Rotorsatz schrittweise zurückdrehen, um Fehler zu korrigieren. Ein zusätzliches Zählwerk, das die Anzahl der verschlüsselten Buchstaben zählte und ebenfalls zurückgedreht wurde, half bei der Orientierung. Maschinen dieses Typs werden daher auch „Zählwerk-Enigmas“ genannt.

Die *Enigma touch* simuliert die Enigma G, eine ursprünglich für zivile Anwendungen gebaute Maschine. Sie wurde auch im Geheimdienst (Abwehr) und im Militär verschiedener Nationen eingesetzt. Drei solcher Varianten mit spezieller Rotorbestückung sind ebenfalls in der Simulation vorgesehen, vgl. Kapitel 2, „Modell und Replika-Einstellungen“.

- Wird eine Zählwerksmaschine simuliert, dann wird der vierstellige Zähler unten links in den Rotorfenstern eingeblendet.
- Im normalen Schlüsselbetrieb kann der Anwender jederzeit die einzelnen Walzen unabhängig drehen, um eine neue Startposition einzustellen, wie bei den klassischen Enigma-Varianten. Der separate Auskuppel-Hebel, mit dem in der originalen Enigma-G die Walzen von ihrem Getriebe entkoppelt wurden, ist in der Replika nicht erforderlich.
- Die „Kurbel“ zum manuellen Vorwärts- oder Rückwärtsdrehen der gesamten Walzenmechanik wird durch langes Drücken der Ring-Taste aktiviert. Im rechten Rotor-Fenster erscheint zusätzlich ein Kurbel-Symbol, und der rechte Zahnkranz bedient die Kurbel. Die anderen Zahnkränze sind in diesem Modus deaktiviert. Gleichzeitig kann weiter ver- oder entschlüsselt werden.
- Durch Drücken irgendeiner Modus-Taste wird der Kurbel-Modus beendet.

Mitschrift über USB

Das Ablesen und Mitschreiben des Schlüsseltexts vom Lampenfeld erfordert viel Aufmerksamkeit vom Bediener. Im militärischen Einsatz wurde die Enigma häufig von Zweimann-Teams bedient – ein Bediener zum Eingeben des Klartexts, einer zum Ablesen und Aufschreiben des Schlüsseltexts.

Um den Komfort zu erhöhen und Fehler zu vermeiden, wurde der Schreibzusatz „Schreibmax“ als Option angeboten: Ein Streifendrucker, der mit vielen parallelen Leitungen am Lampenfeld angeschlossen wurde und die ausgegebenen Buchstaben automatisch mitschrieb.

Die *Enigma touch* kann über den USB-Anschluss ebenfalls ihre Ausgaben zu Protokoll geben:

- Enigma touch per USB an einen Computer anschließen.
- Das USB-Gerät meldet sich als CDC an (Communication Device Class, virtueller serieller Port). Ein passender USB-Treiber ist unter Windows ab Version 7, Mac OS ab OS X sowie auf allen halbwegs aktuellen Linux-Distributionen vorinstalliert.
- Ein beliebiges Terminal-Programm auf dem Computer starten und eine Verbindung auf dem CDC-Port öffnen. Baudrate, Parität etc. können beliebig eingestellt werden.

Im Modell-Einstelldialog kann gewählt werden, wie ausführlich die Mitschrift sein soll:

Mitschrift aus.

Nur der Ausgabetext wird mitgeschrieben, zeilenweise in Vierer- oder Fünfergruppen. Dieser Modus entspricht der historischen Schreibmax-Funktion.

Eingabe, Ausgabe und resultierende Rotorstellung werden mitgeschrieben, in jeweils einer neuen Zeile je Buchstabe.

Zusätzlich zum Schlüssel- oder Klartext werden auch Änderungen bei den Maschineneinstellungen mitprotokolliert – immer dann, wenn das erste Mal ein Zeichen mit den neuen Einstellungen verschlüsselt wird. So lässt sich aus dem Protokoll vollständig nachvollziehen, was mit welchen Einstellungen verschlüsselt wurde.

Rotor-Verdrahtung anzeigen

Ein langer Druck auf die Rotor-Taste öffnet einen Modus, in dem die innere Verdrahtung der derzeit aktiven Walzen angezeigt wird. Die verwendeten Walzen sind für jedes Enigma-Modell festgelegt; ihre Verdrahtung kann auch z.B. unter www.cryptomuseum.com/crypto/enigma/wiring.htm nachgeschlagen werden. Die eingebaute Anzeige in der *Enigma touch* ist insbesondere auch nützlich, um die aktuelle Verdrahtung der frei verschaltbaren Umkehrwalze D anzuzeigen.

- Angezeigt werden die drei rechten Rotoren, sowie links die Umkehrwalze.
  Die Rotoren β und γ der Enigma M4 können nicht angezeigt werden.
- Die linke Spalte der Buchstabenpaare bezeichnet jeweils den Kontakt, der zur linken Nachbarwalze bzw. Umkehrwalze hin orientiert ist.
- Die Notation ist aus Platzgründen immer alphabetisch, auch bei der Enigma I, die eine numerische Beschriftung der Walzen nutzt.
- Die Belegung der Umkehrwalze D wird immer in der deutschen Notation angezeigt, auch wenn die Verdrahtung in Bletchley-Park-Notation eingegeben wurde. (Vgl. Kapitel 3, Verdrahtbare Umkehrwalze D.)

Diagnose-Modus

Wenn die Modell-Taste sehr lange gedrückt wird (5 Sekunden, dabei die Meldung „D ??“ nach 1,5 Sekunden ignorieren), geht die *Enigma touch* in einen Diagnose-Modus:

- Im Display wird die Firmware-Version angezeigt – vgl. Kapitel 5, Firmware-Versionsgeschichte.
- Tastatur- und Lampentest: Jede Buchstabentaste lässt die entsprechende LED im Lampenfeld aufleuchten.
- Auf der USB-Verbindung werden die Rohdaten der kapazitiven Sensoren ausgegeben, sobald irgendeine Taste oder ein Schieberegler bedient wird. Diese Rohdaten werden hier nicht dokumentiert, da sie nur für die Fehlersuche bei Entwicklung oder erster Inbetriebnahme relevant sind.

Der Diagnose-Modus kann nur durch Aus- und Einschalten der *Enigma touch* verlassen werden.

4. Aufbau-Hinweise

Die Enigma touch-Platine ist mit fast allen SMD-Komponenten bereits vorbestückt. Dieses Kapitel gibt Hinweise zum Ergänzen der zusätzlichen Komponenten (Einschalter, Displays, Piezo-Lautsprecher und Akkumulator) und zum Bau verschiedener Gehäusevarianten.

Funktionstest

Ein erster Funktionstest ist bereits mit der teilbestückten Platine möglich – also (auch) ohne Displays, Einschalt-Taster, LiPo-Akku und Piezo-Lautsprecher. Er sollte vor Beginn der ergänzenden Arbeiten einmal durchgeführt werden, um eventuelle spätere Probleme eingrenzen zu können.

- Die *Enigma touch* per USB mit Strom versorgen; sie schaltet sich automatisch ein.
- Die Modell -Lampe leuchtet einmal kurz auf (0,3 s).
- Die Enigma ist jetzt im normalen Verschlüsselungsmodus als Modell M4 betriebsbereit. Jeder Druck auf eine Buchstabentaste lässt eine LED auf dem Lampenfeld aufleuchten.
- Die Modus-Taster sollten funktionieren: Kurzes Antippen (mindestens 0,3 Sekunden) lässt die jeweilige LED aufleuchten, das nächsten Antippen wieder erlöschen.
- Für einen systematischen Test aller Buchstaben-Taster und LEDs kann der Diagnose-Modus gestartet werden: Taste Modell für mindestens 5 Sekunden drücken. Dann die Tastatur durchtesten. Zum Verlassen des Diagnose-Modus die Stromversorgung unterbrechen.

Wenn per USB ein Rechner mit Terminalprogramm angeschlossen ist, sind zusätzliche Tests möglich:

- Die Enigma touch ist „ab Werk“ auf ausführliche Mitschrift über USB eingestellt. Jeder Tastendruck im Verschlüsselungsmodus gibt eine Zeile mit eingegebenem und codiertem Zeichen aus sowie den Rotorpositionen aus.
- Auch die Funktion der Schieberegler (Zahnkränze) und des Steckerbretts kann über die USB-Ausgabe bereits geprüft werden: Wenn die Rotorstellung oder die Verbindungen auf dem Steckerbrett manuell verändert werden, dann gibt die *Enigma touch* die neuen Einstellungen im USB-Protokoll aus, sobald die nächste Buchstabentaste gedrückt wird.

Mechanische Nacharbeiten

Stege entfernen

An den Längsseiten der Platine befinden sich schmale Stege mit Aufnahme-Bohrungen und Positionsmarken, die bei der automatischen Bestückung genutzt wurden. Die Stege sind beidseitig mit einer tiefen V-Nut abgesetzt und können einfach abgebrochen werden. Um den schmalen Steg besser halten zu können, Steg ggf. in einer Werkbank einspannen oder in eine geeignete Nut einsetzen.

Kanten nacharbeiten

Die Platinenkanten zeigen teilweise leichte Absätze vom Fräsen in der Fertigung; die Längskanten sind nach dem Abbrechen der Stege nicht ganz glatt. Wenn die Kanten im fertig aufgebauten Modell sichtbar bleiben, können sie mit Sandpapier geglättet und nach Geschmack mit Permanentmarker geschwärzt werden.

Achtung, der Schleifstaub ist gesundheitsschädlich – bei guter Lüftung oder Absaugung arbeiten, Staubschutzmaske tragen!

Abgesetztes Steckerbrett

Die *Enigma touch* ist vor allem für den einfachen Aufbau als flaches Einplatinen-Modell gedacht. Das Steckerbrett kann aber auch abgetrennt werden, um die *Enigma touch* in ein Holzgehäuse einzubauen, das der Original-Anordnung entspricht.

Da der Bau eines solchen Gehäuses recht aufwendig ist, wird diese Variante vermutlich selten genutzt. Sie ist hier als erstes dargestellt, da das Abtrennen des Steckerbretts am besten vor den weiteren Arbeitsschritten geschieht:

- Wenn eine geeignete Schlagschere vorhanden ist, auf der sich die Platine trotz der vorhandenen Bestückung präzise positionieren und halten lässt, ist das der bevorzugte Weg, um das Steckerbrett abzutrennen. Die Trennlinie ist auf beiden Platinenseiten eingezeichnet.
- Alternativ kann das Steckerbrett über einer Kante abgebrochen werden, nachdem die Platine von beiden Seiten möglichst tief vorgeritzt wurde. Die folgenden Punkte geben Hinweise zu dieser Variante:
    - Zum Ritzen eignet sich ein Cuttermesser mit neuer (vollständiger) Klinge. Nicht mit der Schneide ritzen, sondern mit der Kerbe an der Rückseite der Klinge! Sie trägt jeweils einen dünnen Span des Platinenmaterials ab.
    - An der Trennlinie von beiden Seiten viele Male ritzen und die Platine nach und nach einkerben. Die ursprünglichen Materialstärke von 1,6 mm soll an der Kerbe auf 1 mm oder weniger reduziert werden. Das glasfaserverstärkte Epoxid-Material ist erstaunlich widerstandsfähig gegen Biegen und Brechen!
    - Beim Biegen der Platine könnten aufgelötete Bauteile im Randbereich beschädigt werden, wenn sich das Platinenmaterial verformt. Daher die Platine möglichst direkt an der Kante in eine Werkbank einspannen, so dass nur das Steckerbrett frei herausragt. Dabei im Randbereich Leisten (ca. 10*10 mm²) beilegen, die die Bauteile (Leuchtdiode D30, Schalter SW35) aussparen.
    - Dann das Steckerbrett beherzt biegen, bis es abbricht. Dass es dabei etwas knirscht und das Reißen von Fasern zu hören ist, ist normal.
- Die Bruchkanten mit Schleifpapier glätten. ***Achtung, der Schleifstaub ist gesundheitsschädlich – bei guter Lüftung oder Absaugung arbeiten, Staubschutzmaske tragen!***

Steckerbrett und Hauptplatine werden später durch ein Flachbandkabel wieder verbunden:

- Steckerleisten J4, J5 sind 2*13-polige SMD-Pfostenleisten, Rastermaß 2,54 mm.
- Dazu passen zwei 26-polige IDC-Stecker (Insulation Displacement Connector) und 26-poliges Flachbandkabel. Kabellänge ca. 25 cm, damit das Steckerbrett vorn platziert werden kann.

Komponenten und Optionen bestücken

Ein-/Ausschalter

Der Ein-/Ausschalter SW34 wird so montiert, dass sein Knopf durch die vorgebohrte Öffnung der Platine auf die Bedienseite ragt. Vereinzelt werden Taster angeboten, die für diese „Reverse Mount“ Anordnung vorgesehen sind – aber nur mit (zu) kurzem Knopf.

Empohlen wird ein Taster OMRON B3F-1060 oder vergleichbar – mit Pins für Durchgangslöcher und einem ca. 3 mm langen Knopf. Die Pins werden so gebogen und ggf. gekürzt, dass der Schalter kopfüber auf den vier vorgesehenen Pads verlötet werden kann. Der Knopf ragt dann ca. 1,5 mm aus der Platine heraus.

Displays

Die zwei benötigten Displays sind als OEM-Produkt unter diversen Bezeichnungen z.B. bei AliExpress erhältlich:

- OLED 1.3“, 128*64 Pixel, weiß,
- Controller SH1106,
- SPI-Interface mit 30-poligem Anschluss.

Der 30-polige FPC (Flexible Printed Circuit)-Anschluss mit Rastermaß 0,7 mm ist zum direkten Verlöten auf der Platine vorgesehen; FPC-Steckverbinder mit diesem Rastermaß sind leider nicht erhältlich. Die Displays werden wie folgt aufgelötet:

- Flussmittel auf Lötpads der Platine und/oder FPC-Anschluss geben.
- Display entsprechend dem Bestückungsaufdruck positionieren.
- FPC-Verbinder sorgfältig auf die Lötpads justieren, mit Klebeband provisorisch fixieren.
- Mit konventionellem Lötkolben verlöten. „Drag soldering“ mit einer Lötspitze mit Hohlkehle funktioniert sehr gut. Es ist aber auch möglich, die Anschluss-Pads einzeln mit normaler Lötspitze zu löten.
- Klebeband entfernen, überschüssiges Flussmittel entfernen.

Um die Displays mechanisch zu fixieren, kann ein Tropfen Klebstoff oder doppelseitiges Klebeband zwischen Display und Platine verwendet werden – die Sichtfenster bleiben dabei natürlich frei. Ein Streifen einseitiges Klebeband über dem unteren, freien Ende der Displays und der Platine genügt aber auch und ist bei Bedarf leichter zu entfernen.

Externe Stromversorgung

Die Platine ist vorbereitet für die Stromversorgung über die USB-C-Buchse: 5V, ca. 50 mA im Betrieb ohne Akku, 250 mA bei gleichzeitigem Betrieb und Aufladen des Akkus.

Wenn beim Einbau in ein Gehäuse eine separate Buchse für die Stromversorgung bevorzugt wird, kann diese an die Lötpads J6 angeschlossen werden. Soll zusätzlich der USB-Anschluss zur Datenübertragung genutzt werden, aber *nicht* für die Stromversorgung (um zwei parallelgeschaltete 5V-Quellen zu vermeiden), kann Jumper JP1 aufgetrennt werden. Dann ist die 5V-Leitung des USB-Anschlusses nicht mehr verbunden.

LED D30 (neben dem Einschalter) zeigt an, ob der LiPo-Akku geladen wird. Wenn die *Enigma touch* ohne Akku aufgebaut wird, kann die Funktion der LED so geändert werden, dass sie bei anliegender

5V-Versorgung leuchtet. Dazu am Jumper JP2 die Brücke „Charge“ auftrennen und stattdessen die Lötpads für „+5V“ mit einem Tropfen Lötzinn überbrücken.

Lithium-Polymer-Akku

Der Einbau eines Lithium-Polymer-Akkus ist optional; die *Enigma touch* kann auch direkt an einem 5V-Netzteil betrieben werden. Zur angenehmeren Handhabung – und weil auch alle Original-Enigmas batteriebetrieben waren – wird ein Akku aber empfohlen. Ein flacher LiPo-Akku kann mit doppelseitigem Klebeband unter der Tastatur, in der Nähe der Anschlüsse J7/J8, befestigt werden:

- Lithium-Polymer-Akku, Nennspannung 3,7 V, Ladespannung max. 4,2 V.
  Empfohlene Kapazität 500 bis 1000 mAh.
- ***Der Akku muss unbedingt eine eingebaute Schutzschaltung haben (BPS, Battery Protection System),*** die ihn vor Tiefentladung schützt und eine zusätzliche Absicherung gegen Überladen und thermische Probleme liefert!
- Steckverbinder J8 ist eine zweipolige JST PH 2.0 Buchse. Akkus mit passendem Stecker sind gängig – aber es gibt keinen Standard für die Polarität. ***Vor dem Anschluss unbedingt die Polarität überprüfen!*** Bei Bedarf können die Steckkontakte am akku-seitigen Stecker gelöst und getauscht werden.
- Alternativ können lose Anschlussdrähte an die Pads J7 gelötet werden.
- Der Akku wird durch ein Lade-IC (MCP73831-2ACI) geladen, das ihn mit Vorkonditionierung, Konstantstromladung und abschließender Konstantspannungsladung optimal und schonend lädt. Die maximale Ladespannung ist durch das IC auf 4,2 V festgelegt, der maximale Ladestrom durch Widerstand R12 auf knapp 200 mA (I_{max} = 1000V / R12).

Piezo-Lautsprecher

Als Lautsprecher wird eine einfache Piezo-Scheibe verwendet, die die Platine als Resonanzboden verwendet. Scheiben mit bis zu 25 mm Durchmesser können auf der Rückseite der Platine mit doppelseitigen Klebeband montiert werden – entweder oberhalb der Displays oder im Bereich der unbenutzten Steckerbrett-Verbinder J4/J5.

Die Impedanz des Piezos soll 400 Ohm oder höher betragen. Er wird in der *Enigma touch* je nach eingestellter Lautstärkestufe mit 3 V_{pp} oder 6 V_{pp} betrieben. Angeschlossen wird er an die Lötpads J3, die Polarität ist dabei gleichgültig.

Gehäuse und Kabel

Flacher Rahmen

Wenn die *Enigma touch* als Einplatinen-Modell aufgebaut wird, ist ein flaches Gehäuse mit Bodenplatte trotzdem empfehlenswert – zum Schutz der Komponente auf der Unterseite vor Beschädigung, und weil Berührungen der Platine von unten Fehleingaben auf der kapazitiven Tastatur auslösen können.

Die Platine misst 237.5 x 170.0 mm². Rundum ist eine Auflagefläche von 10 mm Breite frei für die Montage eines Rahmens oder Gehäuses, mit Ausnahme der USB-Buchse hinten rechts.

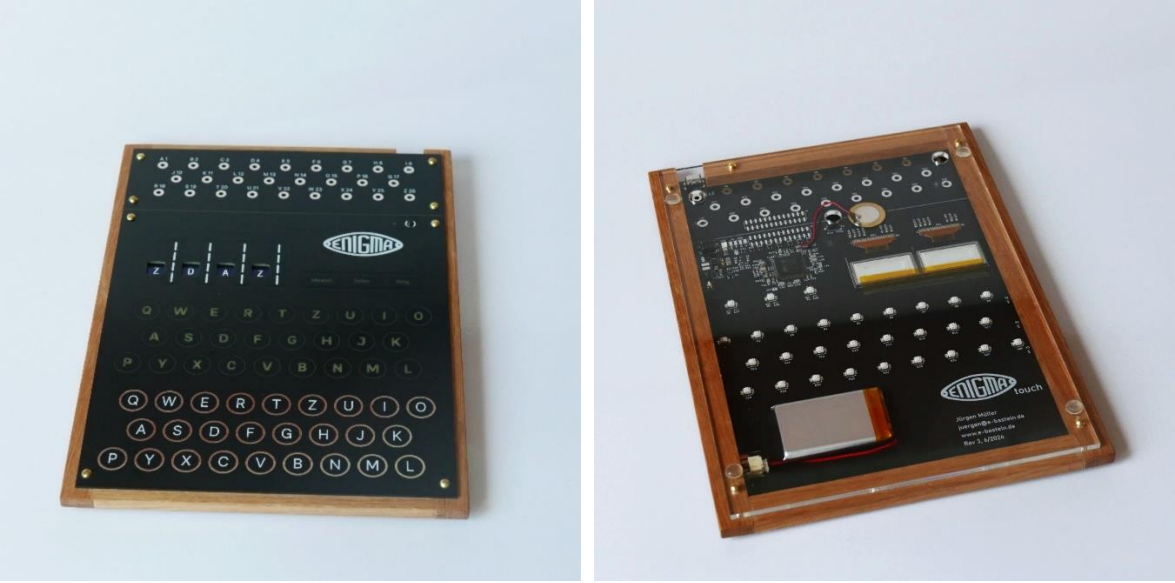
Ein Vorschlag für ein einfach aufzubauendes Gehäuse ist unten abgebildet. Es besteht aus einem schmalen Eichenholz-Rahmen als Anklang an die Transportkästen der Original-Enigma und einer

Acryl-Bodenplatte, die den Blick auf den einfachen Schaltungsaufbau erlaubt. Der Rahmen spart die USB-Buchse aus, ist an den Ecken verleimt und wird durch Verschrauben mit der Bodenplatte stabilisiert. Im Beispiel hat die Bodenplatte außerdem Bohrungen zum Aufhängen an der Wand sowie für den Schalter für Firmware-Updates.

Benötigtes Material und Maße:

- Holzleisten Eiche 7*15 mm²; Längen 2 Stück 250 mm, 1 Stück 150 mm, 1 Stück 135 mm
- Bodenplatte, Acryl XT 3 mm, Größe 240 * 170 mm²
- Schrauben 2,5 * 8 mm, 8 Stück Oberseite, 5 Stück Unterseite
- Rutschfeste Füße, 4 Stück

Wer es eleganter mag, kann Gehrungsschnitte an den Ecken verwenden. Allerdings waren die Seitenwände der echten Enigma-Transportkästen auch nicht auf Gehrung geschnitten, sondern mit gezinkten Kanten verbunden.



Enigma Touch mit flachem Rahmen und transparentem Boden

Dreidimensionales Holzgehäuse

Der Einbau in ein Holzgehäuse, das der Original-Enigma näherkommt, ist möglich, aber deutlich aufwendiger. Da die Ausführung stark abhängt vom Anspruch an die Originaltreue, Budget, handwerklichen Geschick und Aufwand, werden hier nur einige Hinweise gegeben.

Zum Abtrennen des Steckerbretts vgl. den Abschnitt „Abgesetztes Steckerbrett“ in Kapitel 4.

Das unten gezeigte Beispiel verwendet

- Buche-Sperrholz 8 mm, je 186 * 240 mm², für Decke und Boden,
- Buchenleisten 20*8 mm² (Deckel) und 52*8 mm² (Unterteil) als Seitenwände,
- Buchenleiste 56 * 8 mm² für die Frontklappe,
- Scharnierbänder 10 mm (Breite im geschlossenen Zustand) für Deckel und Frontklappe.

Einige Überlegungen zu Ausführungsdetails:

- Tragegriff: Im Original wurden sowohl klappbare Metall-Tragebügel als auch Lederriemen verwendet.

- Deckelscharnier und -arretierung: Die meisten Enigma-Modelle nutzten Scharnierbänder, an denen der Deckel fest montiert war. Der aufgeklappte Deckel wurde durch Metallbügel abgestützt, die beim Zuklappen zwischen Gehäuse und Enigma versenkt wurden. Ich habe aus Platzgründen stattdessen eine feste Schnur verwendet. – Die Enigma M4 hatte zwei trennbare Einzelscharniere, so dass ihr Deckel abnehmbar war.
- Front-Scharnier: Bei allen Enigmas mit Steckerbrett und klappbarer Front sind die Kanten von Bodenplatte und Frontklappe unter 45° abgeschrägt, so dass die sichtbare Kante des Scharnierbands direkt an der unteren Gehäusekante liegt. Ich habe das im Beispiel so ausgeführt, würde den Aufwand aber nicht unbedingt noch einmal treiben.
- Deckel-Verriegelung: Der flächenbündig versenkte Verriegelungs-Mechanismus wurde offenbar an allen zivilen und militärischen Enigmas verwendet. Er ist sehr charakteristisch und auch funktional sinnvoll, da der Transportkasten am rückseitigen Griff getragen und auf der flachen Front abgestellt werden kann. Leider ist dieser Verschluss nicht mehr erhältlich; schon gar nicht im verkleinerten Maßstab 2:3. Ich habe mir den Aufwand gespart, ihn nachzuempfinden, und einen preiswerten Schatullen-Verschluss verwendet.
- Die Seitenteile sind im Original mit gezinkten Verbindungen versehen. Ich habe sie der Einfachheit halber auf Stoß verleimt. Deckel und Boden sind im Original mit den Seitenteilen verschraubt, im verkleinerten Modell mit Messingnägeln verbunden und verleimt.

Beim Einbau in ein Holzgehäuse ist der **USB-Anschluss** am Steckerbrett nicht nutzbar. Die bestückte Buchse muss ggf. unter Heißluft – oder notfalls mit Gewalt – entfernt werden. Stattdessen kann eine USB-B-Buchse zur Gehäusemontage verwendet werden, deren Anschlusskabel an den Lötpads J2 verlötet wird.

Enigma Touch im Holzgehäuse mit abgesetztem Steckerbrett

Kabel für das Steckerbrett

Soll das Steckerbrett benutzt werden, um die militärischen Enigma-Modelle I, M3, M4 zu simulieren oder die Umkehrwalze D neu zu verdrahten, werden Verbindungskabel benötigt. Für die Buchstaben-vertauschung per Steckerbrett genügen max. 10 Kabel, je nach historischer Schlüsselvorschrift. Um die Umkehrwalze D zu konfigurieren (vgl. Kapitel 3, Verdrahtbare Umkehrwalze D), werden 12 Kabel benötigt.

- Die Miniaturstecker werden als “Zwergstecker“ angeboten und vor allem im Modellbau verwendet, etwa für Modelleisenbahnen. Ihr Stiftdurchmesser ist 2,6 mm.
- Als Kabelmaterial ist Litze mit 0,5 mm² Querschnitt (AWG 20) gut geeignet, mit möglichst flexibler Isolierung z.B. aus Silikon. Die übliche Schaltlitze H05V-K mit 0,75 mm² Querschnitt und PVC-Isolierung ist eher zu steif.
- Eine Kabellänge von 15 cm (plus Stecker) ermöglicht auch die längsten, diagonalen Verbindungen auf dem Steckerbrett.
- Sollten die Stecker zu locker oder zu fest in den Buchsen der *Enigma touch* sitzen, können die geviertelten Stifte leicht aufgebogen oder zusammengedrückt werden.

5. Firmware-Updates

Sollten neue Firmware-Versionen verfügbar werden, können Sie diese selbst installieren. Benötigt wird ein Windows-PC mit USB-Verbindung zur *Enigma touch* und die frei erhältliche Programmier-Software „STM32CubeProgrammer“ vom Hersteller der verwendeten CPU, ST Microelectronics.

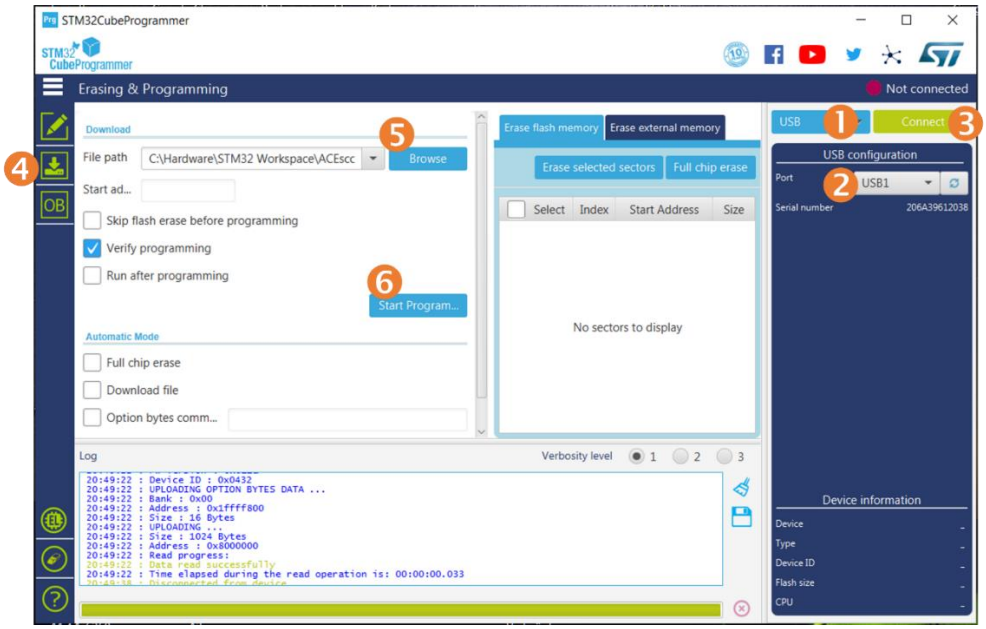
Die aktuell installierte Firmware-Version wird im Diagnose-Modus angezeigt; vgl. Kapitel 3, Diagnose-Modus.

Installation über STM32CubeProgrammer

Die Programmier-Software kann nach einer kostenlosen Registrierung direkt von ST Microelectronics heruntergeladen werden, www.st.com/en/development-tools/stm32cubeprog.html. Ohne Registrierung ist eine etwas ältere Version, die auch weniger Speicherplatz belegt, beim Heise Verlag erhältlich, www.heise.de/download/product/STM32CubeProgrammer.

Neue Firmware wird als .ELF-Datei zur Verfügung gestellt. Sie kann wie folgt installiert werden:

- Schalter SW35 auf der Unterseite der *Enigma touch* auf PROG umschalten.
- USB-Verbindung zum PC herstellen, Enigma einschalten. Im PROG-Modus gibt es keine visuelle Betriebsanzeige, aber der PC sollte ein USB-Gerät „STM32 Bootloader“ erkennen.
- STM32CubeProgrammer Software starten, dann (vgl. Screenshot unten):
    1. USB-Interface wählen
    2. Port suchen lassen, sollte USB1 erkennen
    3. Verbindung herstellen
    4. Programmier-Dialog wählen
    5. Die .ELF-Datei auswählen, geht auch per Drag & Drop
    6. „Start Programming“
- Bestätigungs-Dialoge quittieren, Disconnect (3)
- Schalter SW35 zurück in den RUN-Modus stellen (bzw. NORM für Rev 2-Platinen).



Firmware-Versionsgeschichte

FW006, August 2024

- Modus-Tasten müssen etwas länger gedrückt werden (ignorieren versehentliches Berühren)
- Batterieanzeige und Lautstärke-Anzeige auf Platinen Rev 2 korrigiert

FW005, Juli 2024

- Manuelles Ändern der Rotorstellung setzt den Gruppen-Zähler für USB-Logging zurück
- Klick beim Rotor-Bewegen ist auch bei halber Lautstärkeeinstellung immer hörbar

FW004, Juni 2024

- Audio-Ausgabe (nur Platine Rev 3)
- Anzeige des Akku-Ladestandes im Modell-Dialog (nur Platine Rev 3)
- Warnung bei niedrigem Akkustand: flackernde Lampen
- Bessere Unterstützung für Zählwerk-Enigmas: Zähler wird in den linken Rotor-Fenstern angezeigt, Kurbel-Symbol wird im rechten Rotor-Fenster angezeigt.
- Besseres Ansprechen der Rotor-Anzeige und Schieberegler, wenn viele Rotoren sich gleichzeitig bewegen.

FW003, August 2023

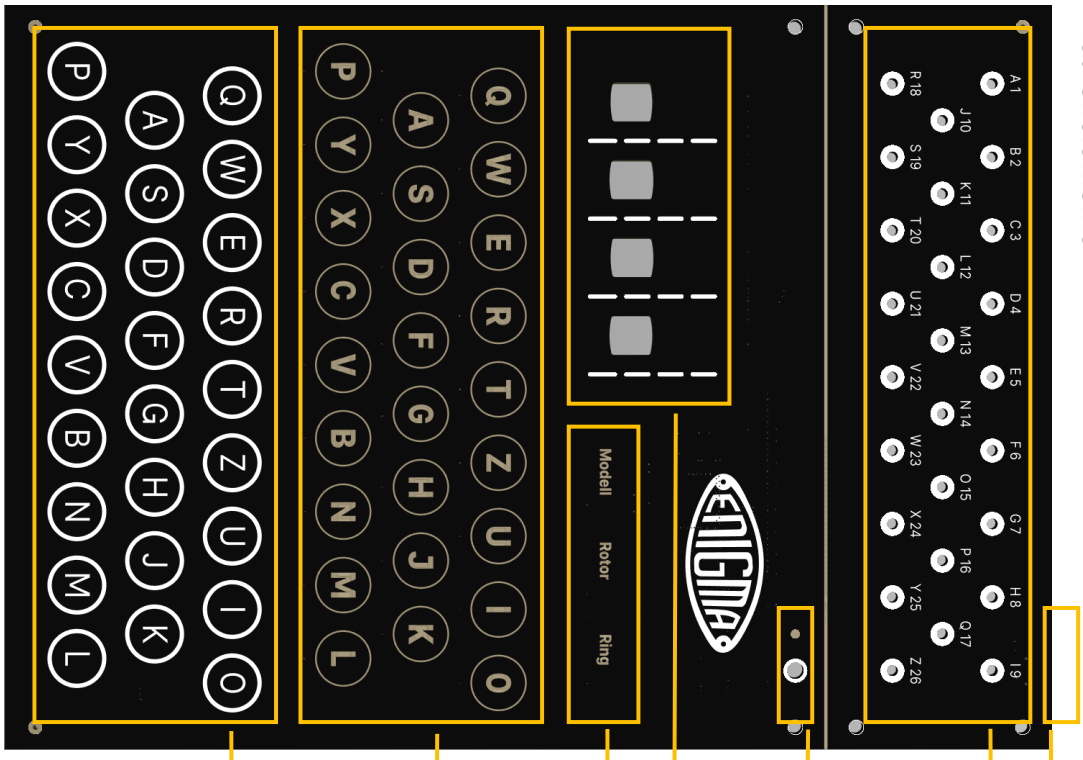
- Fehler bei der Doppelschritt-Anomalie behoben
- Fehler bei der Nummerierung der UKWD-Positionen behoben
- Erweiterte Mitschrift: Steckerbrett und UKWD-Verdrahtung werden protokolliert
- Enigma Modell D hinzugefügt. (Ähnlich Enigma K, aber Mitnehmer-Kerben fest am Walzenkörper statt an den verstellbaren Ringen)
- Visueller Fehlerhinweis beim Verlassen des Rotor-Modus, wenn eine Walze mehrfach verwendet werden soll: Fehlerhafte Rotor-Auswahlfenster rotieren einmal durch.

FW 002, Dezember 2022

- Erste veröffentlichte Version
- Fehler beim Doppelschritt und bei der Nummerierung der UKWD-Positionen!

6. Kurzreferenz

Enigma touch Kurzanleitung



Bedienelemente

USB-C Buchse (5V Stromversorgung, Daten-Mitschrift).

Steckerbrett für Enigma-Modelle I, M3, und M4.
Verbinde Buchstaben-Paare wie im Schlüssel gegeben.
Auch zur Verdrahtung der Umkehrwalze (UKW) D.

Ein/Aus-Taster; Enigma-Status bleibt erhalten.
Automatische Abschaltung nach 15 Min. Inaktivität.
Akku-Ladeanzeige (wenn LiPo-Akku installiert),
oder Anzeige für 5V Stromversorgung.

Walzen-Anzeige, Slider zum "Drehen" der Walzen.
Für Schlüsselbetrieb und zur Maschinen-Einrichtung.

Einricht-Modus, siehe Tabelle auf der Rückseite.
(Nur in der Replika, nicht im Original.) Im Schlüsselbetrieb sind alle Modus-Lampen ausgeschaltet.

Lampenfeld zeigt verschlüsselte oder entschlüsselte Buchstaben an, solange eine Taste gedrückt wird.
Verschlüsselungs- und Entschlüsselungsmodus unterscheiden sich nicht, da der Code symmetrisch ist.

Tastatur für die Eingabe von Klar- oder Schlüsseltext.
Taste gedrückt halten bis die Walzen sich bewegt haben und eine Lampe aufleuchtet.

Material zur Original-Enigma:
www.cryptomuseum.com
youtu.be/ybkkiGtJmkM

Simulierte Enigma-Varianten

Details zu den Varianten und Walzen-Verdrahtung:
www.cryptomuseum.com/crypto/enigma,
www.cryptomuseum.com/crypto/enigma/wiring.htm

Display	Modell	Beschreibung
I	Enigma I	Erste militärische Version (Reichswehr). Steckerbrett, numerische Walzenbeschriftung.
M3	M3	Marine-Enigma, 3 Walzen.
M4	M4	U-Boot Enigma, 4 Walzen.
D	Enigma D	Frühe Version, Mitnehmer fest an den Rotoren.
K	Enigma K	Kommerzielle Version, 3 Walzen, UKW einstellbar aber nicht angetrieben.
KD	Enigma K, UKW D	Modell K mit frei verdrahtbarer UKW, für Geheimdienst Militärisches Amt.
KR	Reichsbahn	Modell K, Walzen für Reichsbahn.
KS	K Schweiz	Modell K, Walzen für Schweizer Armee.
T	Tirpitz	Modell K Variante für japanische Streitkräfte. 8 Walzen zur Wahl, mit je 5 Schaltpositionen.
G	Enigma G (G31)	Zahnräder statt Hebel bewegen Walzen und UKW. Viele Schaltpositionen, Kurbel für Positions-Korrektur vor/zurück.
G1	Enigma G111	Modell G, Walzen für ungarische Armee. Nur Walzen I, II, V sind erhalten.
G2	Enigma G219	Modell G, Walzen für holländische Marine.
G3	Enigma G312	Modell G, Walzen für deutschen Geheimdienst (Abwehr).

Einrichten der Replika

Taster antippen, um einen Einricht-Modus zu wählen.
Aktiven Modus-Taster nochmals tippen → Verschlüsselungsmodus.
Taster eine Sekunde halten für erweiterte Funktionen.

Modus	Beschreibung
Modell	Wähle den simulierten Enigma-Typ, wähle Replika-Einstellungen: Audio-Lautstärke, Lampenhelligkeit und Umfang der USB-Mitschrift.
Rotor	Wähle die Walzenbestückung und die UKW. Dieser Modus kann nicht verlassen werden, wenn eine Walze doppelt ausgewählt ist.
Ring	Index-Ringe der Walzen einstellen. (Position der Beschriftung relativ zur internen Verdrahtung.)
Modell (lange halten)	UKW D kann vom Nutzer neu verdrahtet werden. Verbindungen auf dem Steckerbrett stecken, dann *Modell* halten. J und Y müssen gepaart oder offen sein, alle anderen Buchstaben gepaart! Zeigt "D OK" an bei gültiger Verdrahtung, sonst "D ??".
Rotor (lange halten)	Zeigt die interne Verdrahtung aller Rotoren und der UKW (links). Nützlich um die Verdrahtung der änderbaren UKW D zu überprüfen.
Ring (lange halten)	"Kurbel-Modus", nur für die Enigma G-Modelle. Der komplette Rotorsatz kann über sein Zahnrad-getriebe vor- und zurückbewegt werden. Der rechte Slider dreht die Kurbel.

Enigma touch Kurzanleitung – Rev 3.0, für PCB Rev 3
juergen@e-basteln.de, www.e-basteln.de