How To Use The Enigma Machine

The Enigma Machine is an accurate simulation of the M3 Enigma cipher machine used by the German Navy during the Second World War. This particular Enigma model utilised 3 rotors (selected from a total of 8), and had a choice of 2 reflectors. Other Enigmas of the time used more rotors and had extra reflectors available. Each of the rotors has a selectable ring position, as well as an initial or start position, and a plug board is also supported.

Before explaining how to use *The Enigma Machine* it would be useful to describe the physical construction of a real Enigma machine, and explain what rotors, reflector, plug board etc. actually are.

How the Enigma worked

The Enigma Machine consisted of a wooden cabinet enclosing a typewriter keyboard and a set of 26 lamps (one for each letter of the alphabet). At the top of the machine was a slot into which three wheels or rotors could be fitted onto a shaft.

The rotors were furnished with electrical contacts and buried inside were wires that connected the contacts on one side to those on the other in a scrambled order. The cabinet contained a battery, and when a key was pressed, electric current would flow from the keyboard through each of the three rotors in turn, through a reflector, then back through the rotors, and finally through one of the lamps making it light up.

A number of different rotors were available (8 in this case) and the operator would choose which rotors to use and the order in which to use them. The operator could also select which reflector to use (2 were available).

The rotors had adjustable rings which could be turned with respect to the inner core. The ring for each rotor could be set by the operator in any one of 26 possible positions (A to Z).

The initial positions of the rotors could also be set by the operator, according to which letters on their rims showed through a window in the machine.

On the front of the cabinet was the plug board, which consisted of a set of 26 sockets into which wires with plugs at both ends could be inserted. Its effect was an additional swapping of pairs of letters and hence added a further level of scrambling to the encryption process.

The cumulative effect of rotating rotors, rings, reflector and plugs meant that the number of possible different configurations of the machine was absolutely enormous. It was considered therefore to be a very secure method of encrypting messages (it was thought unbreakable in fact though this proved not to be the case).

As each key on the keyboard was pressed, one of the lamps would light up (obviously not the same letter that had been pressed). It was the operator's job to write down which lamps lit up.

As keys were pressed the rotors would also rotate. This meant that the same letter of the alphabet would be encoded to a different letter each time it was used in a message. (If this weren't the case it would have been almost trivial to crack an Enigma message.) Effectively each letter in a message was encoded using its own unique code. It was this fact that made the Enigma so difficult to defeat. It took some of the best mathematical brains in Europe to beat it, and doing so was the spur that led to the development of modern electronic computers.

The reciprocal nature of the design meant that if the letter A were encoded into, for example, a B at some point in a message, then a B would be encoded into an A at the same point. Consequently encoding and decoding were the same process, they were reversible. If encoded 'ciphertext' were passed through the machine again, the result would be the original message or 'plaintext' (provided of course that the machine was set up in the same way).

One further consequence of the design was that a letter would never encode to itself. This proved to be the Enigma's Achilles' Heel.

Encoding your messages

Use copies of the Coding Sheet below to encode your messages. Enter your original message in the boxes marked 'plaintext'. (It's usual in cryptography to break messages up into blocks of 4 or 5 characters to hide the clues that word lengths might give to someone trying to crack the message.) The Enigma machine didn't encode spaces (nor punctuation characters), so either leave out the spaces in your message or replace them with X's. Pad out the last set of boxes with X's so your message is a multiple of 4 characters in length. If you wish to encode numbers in your message, you must spell them out.

Now set up the rotors, rings, reflector and plugs of *The Enigma Machine* with reference to the Key Guide below. Either choose settings at random, or use a row from the sample Code Book. Record your settings at the top of the Coding Sheet.

Encode your message by typing each letter in turn and copying down the letter shown on the display into the 'ciphertext' box immediately below the plaintext.

You can check that you've encoded your message properly by decoding it again. First reset the rotors by pressing the **ESC** or **HOME** key. Then type in the ciphertext one letter at a time and verify that it matches the plaintext in the boxes above.

Messages to decode

Here are some sample messages for you to practice decoding. Answers upside down below.

1. Encoded using the default rotor, reflector and plug settings (i.e. you don't need to change them).

OPGN DXCF WEVT NRSD ULTP

2. Encoded with rotors 7, 1, 3 and reflector C.

ZUZB PCBG EOGY TRPB VUXG QTIX AWHT ZDZV ITOA

3. This is a real message (in German naturally) sent by Admiral Dönitz to the U-boat commanders just after Hitler's death, on 30 April 1945. Use the Day 1 settings from the Code Book below to decode it. (Note that umlauts can't be encoded directly so are represented by extra E's.)

WGLS CWYJ NLAY YMPW KSPP IKBK QDUA JVKO BLSS HIBO MHWO

Answers

1. THIS IS A SECRET MESSAGE

2. ENIGMA WAS USED DURING THE SECOND WORLD WAR

3. In German: Der Führer ist tot. Der Kampf geht weiter. Dönitz
Or, translated into English: The Führer is dead. The battle will continue. Dönitz

Key Guide

F1 – displays the menu.

F2 – selects the rotors. Move the cursor (highlighted in red) using the arrow keys and enter **1** to **8** for each of the left, centre and right rotors. Note that you can't use the same rotor more than once, and changing a rotor automatically resets its ring and initial positions to **A**. Press the **ENTER** or **RETURN** key to return to the menu.

F3 – sets the ring positions for the rotors. Move the cursor using the arrow keys and enter **A** to **Z** for each of the left, centre and right rotors. Press the **ENTER** or **RETURN** key to return to the menu.

F4 – sets the current reflector. Enter **B** or **C**. Press the **ENTER** or **RETURN** key to return to the menu.

F5 – sets the plug board. Move the cursor (highlighted in red) using the arrow keys and enter up to 13 pairs of letters **A** to **Z**. Note that you can't connect a letter to itself, nor use the same letter more than once. Press the **DELETE** key or space bar to erase a letter. Press the **ENTER** or **RETURN** key after the last pair to return to the menu.

F6 – sets the rotor initial or start positions. Move the cursor using the arrow keys and enter **A** to **Z** for each of the left, centre and right rotors. Note that pressing **F6** will always reset all the rotor current positions to their initial or start positions. Press the **ENTER** or **RETURN** key to return to the menu.

F7 – displays the current rotor positions (**A** to **Z** for each of the left, centre and right rotors) for information only. As the letters in a message are typed the rotors rotate, so their positions are continually changing. The right-hand rotor moves on every key press, and at certain positions the rotation 'carries' to the next rotor in line. Press the **ENTER** or **RETURN** key to return to the menu.

F8 – saves the current settings (rotors, rings, reflector, plug board, initial positions) to non-volatile memory.

F9 – loads from memory saved settings.

ESC or **HOME** – resets all the rotors to their initial or start positions (i.e. clears the message). The display is cleared.

DELETE or **BACKSPACE** key – undoes the last letter entered and steps the rotors back one position. Note that there is only a single level of undo (the real Enigmas didn't have an undo at all!).

When you have completed all the settings, return to the menu by pressing **F1** then enter your message one letter at a time and note down the encoded letters shown on the display.

Default settings **-** rotors 1, 2, 3; rings A, A, A; initial A, A, A; reflector B; no plugs.

Enigma Code Book

Day	Rotors	Rings	Reflector	Plugs
1	5 6 1	G G P	B	E-O F-P L-Y
2	5 1 3	T T X	B	E-M T-V U-Y
3	1 3 6	W O U	C	B-K D-Q J-O
4	1 5 6	Z K O	B	I-T M-P O-Q
5	3 1 4	F C I	C	B-T F-V Q-U
6	3 5 2	W J Y	C	A-S L-R O-X
7	4 7 2	E W F	B	A-U B-F D-H
8	4 5 8	Z A N	B	D-K G-O N-Q
9	1 3 2	Q M A	B	B-V E-I F-G
10	5 2 1	Z G T	C	B-O F-N W-X
11	2 4 5	N H M	B	A-Q E-H T-X
12	2 1 5	B Z Q	C	A-U F-W I-Y
13	3 4 1	L V D	C	D-K E-S I-L
14	3 2 7	D X G	B	C-T F-J X-Z
15	5 4 2	C S D	B	B-P G-S J-U
16	4 2 5	M K P	C	E-R F-Q U-W
17	1 4 8	Q G T	B	A-X B-M H-W
18	6 2 5	K F G	B	J-P O-Q X-Z
19	8 4 1	B U W	C	C-I F-W G-Z
20	4 2 1	P A Z	C	I-J K-U R-W
21	4 1 2	J D G	C	B-E L-N Q-R
22	1 3 4	G J L	B	E-F M-N T-U
23	5 8 3	J J J	C	B-R D-L O-Y
24	2 3 1	I A M	C	A-Y E-P T-V
25	7 5 3	P I Z	B	G-R J-N U-Z
26	3 1 4	Q T O	B	A-P G-R Q-V
27	3 5 4	I Z I	C	B-M F-J I-Q
28	5 7 1	M H A	B	B-W D-R I-Q
29	5 7 2	Y D F	B	A-G E-X W-Y
30	1 3 8	G Q L	C	C-G K-W L-U
31	1 5 6	J P P	C	C-E I-P J-R

Enigma Coding Sheet

Rotors			

Reflector	

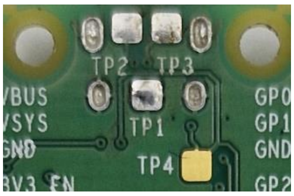
Date:

Rings			
Initial			

Plugs						

Plaintext																
Ciphertext																
Plaintext																
Ciphertext																
Plaintext																
Ciphertext																
Plaintext																
Ciphertext																
Plaintext																
Ciphertext																
Plaintext																
Ciphertext																
Plaintext																
Ciphertext																
Plaintext																
Ciphertext																
Plaintext																
Ciphertext																
Plaintext																
Ciphertext																
Plaintext																
Ciphertext																

Construction

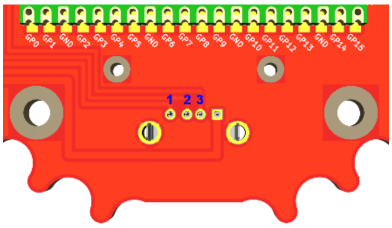


First tin the three test pads marked TP1, TP2 and TP3 on the bottom side of the *Pico* PCB (underneath its micro USB socket, see photograph on the right). Be careful not to use too much solder (just a very thin layer on the gold surface is sufficient) and, if available, add a little flux as well. Then position the *Pico* PCB on the bottom side of the *Enigma* PCB and line it up carefully. (The orientation should be obvious.)

There are four small corner holes on the *Enigma* PCB and these must line up with corresponding holes in the *Pico* PCB. Separate the included four small pins with side cutters and insert them into these holes to facilitate accurate alignment. Apply a little solder to the four corner pads on the *Pico* adjacent to these guide pins to hold the board in place (but don't solder the pins themselves) then remove the four pins.

Turn the *Enigma* PCB over and check that the three test pads are lined up accurately with the corresponding holes in the *Enigma* PCB. Then apply solder (ideally a thin solder) to the three holes with a needle soldering iron tip so as to fill the holes and make connections between the two PCBs. Be careful not to bridge the holes.

Solder the USB keyboard socket to the top side of the *Enigma* PCB.



You can check that the test pads have made good connections by testing continuity between the pairs of points in the two images marked 1, 2 and 3 (on the top and bottom sides of the PCB). You can also test for bridges between pins.

If the connections are good then solder the rest of the *Pico* pads.

Fit and solder the electrolytic capacitors (C1 and C2) paying attention to their polarity (negative is marked by a stripe on the side of the body).

Bend the legs of the regulator (REG1) at right angles and solder it such that the metal heatsink is flat on the board and the side with the writing is facing upwards.

Next fit the battery snap (BATTERY). Support holes are drilled on the board for the battery snap leads. Feed the leads up through the support holes from the bottom side of the board and then down the solder holes. Red is positive and black is negative.

Insert 4 AA cells into the battery box, observing the correct polarity.

Solder the 7-way header to the LCD display (soldering the side of the header with the shorter end of the pins). Make sure that it is at right angles to the display. Push fit the LCD to the circuit board then connect the battery box to the battery snap. If the board is working correctly the LED on the *Pico* PCB should flash twice (it will flash twice again when a keyboard is attached).

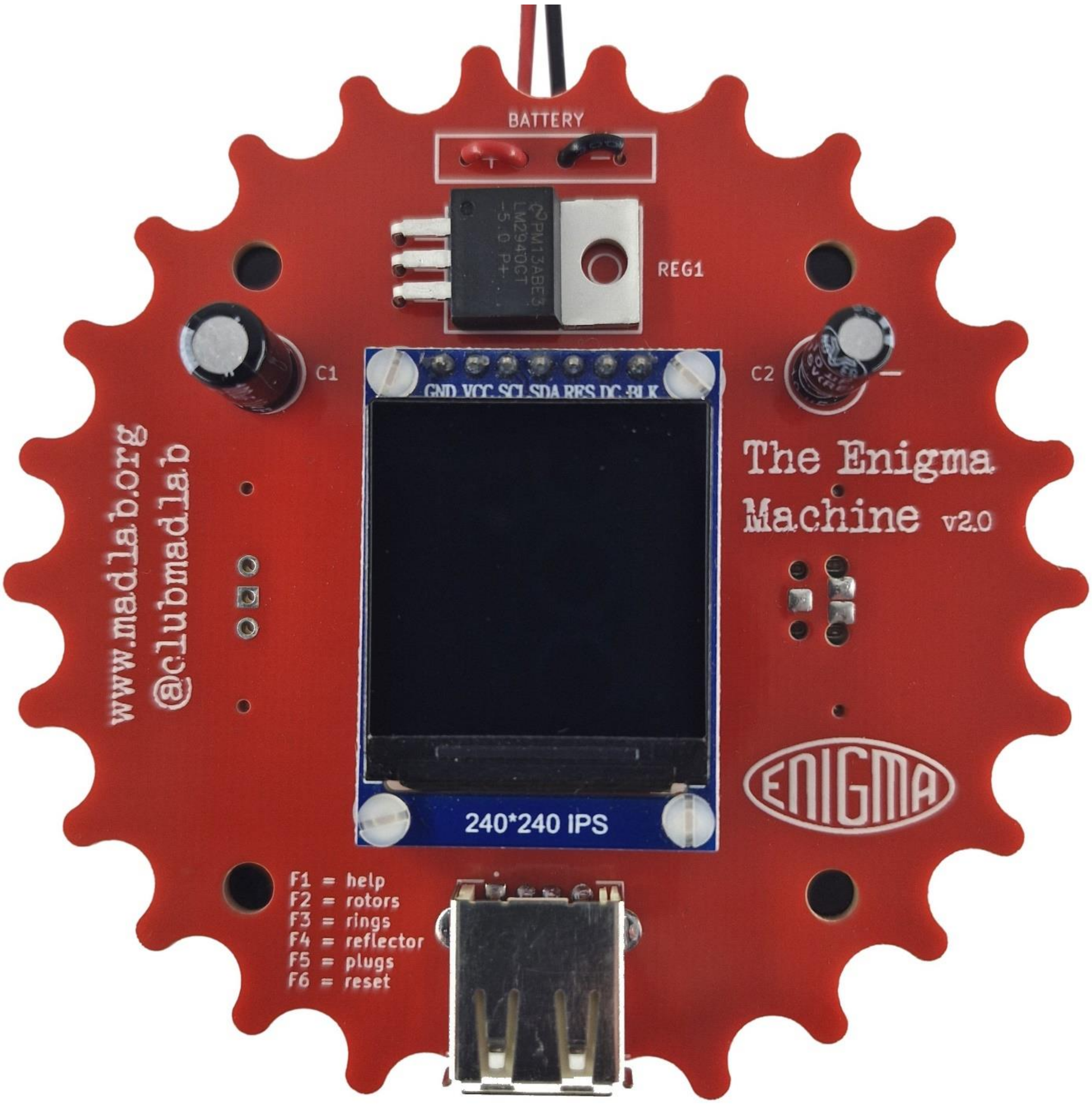
After the self-test a splash screen should appear on the display for a couple of seconds then a "Keyboard not detected" message should appear. Connect a standard wired PC keyboard to the USB socket and the error message should be replaced by a logo and credit screen. Press any key on the keyboard to display the main menu.

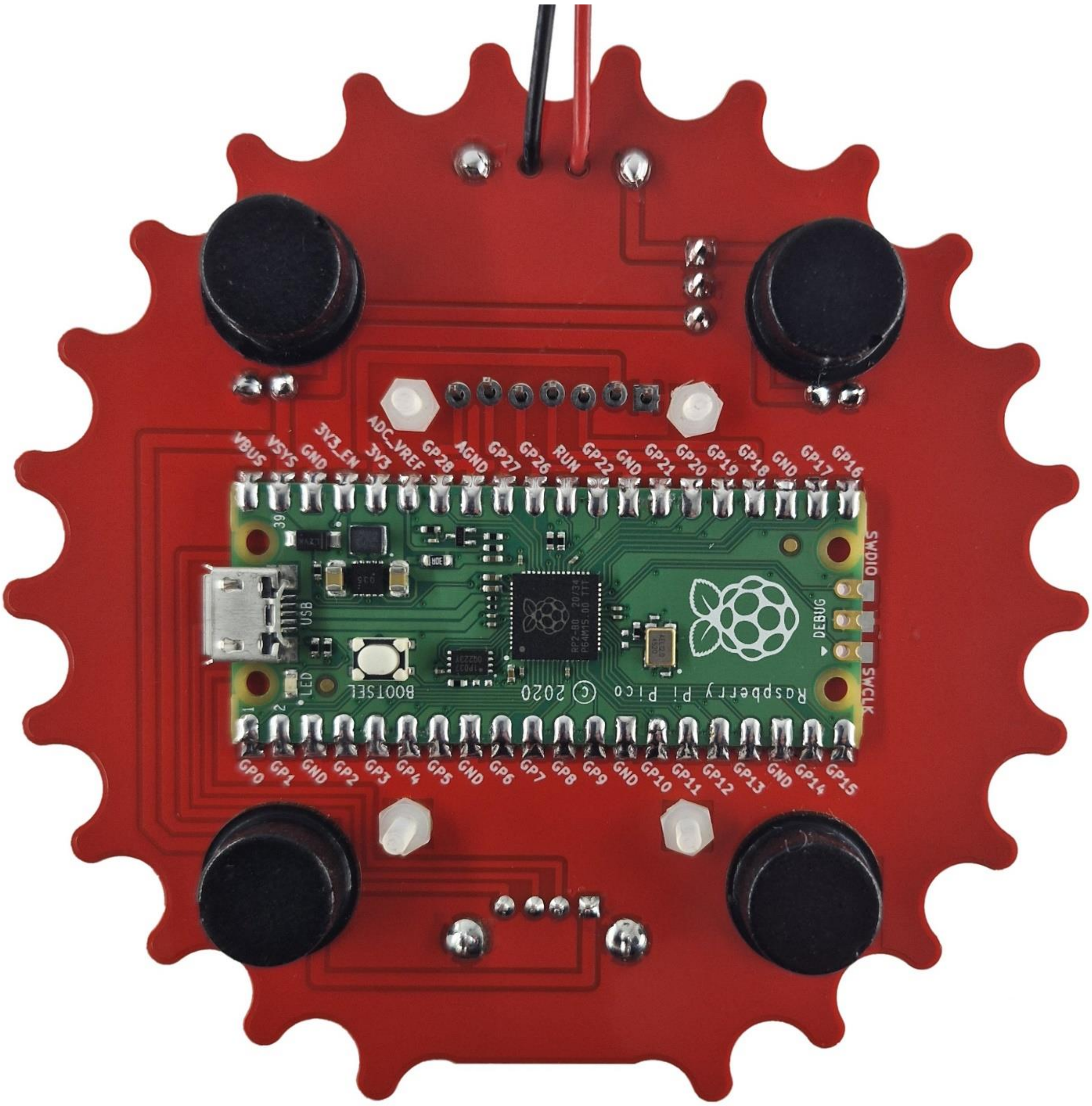
If the board is completely working then the display can be soldered in position or left as a push fit. Use the nylon bolts, nuts and spacers to secure the display in place.

Two alternatives are provided for feet – either self-adhesive rubber ones or PCB pillars that fit in the four large holes.

It is recommended that primary (non-rechargeable) AA cells are used. Secondary (rechargeable) cells such as NiMH, which have a lower voltage of 1.2V as opposed to 1.5V, should also work but that depends on the attached keyboard still functioning when supplied with less than 5V. That may depend on the manufacturer of the keyboard.

If the *Pico* needs to be re-flashed a micro USB cable can still be attached to the *Pico* provided the cable's plug is sufficiently low profile.


BATTERY
REG1
C1
C2
GND VCC SCL SDA RES DC BLK
www.madlab.org
@clubmadlab
The Enigma
Machine v2.0
ENIGMA
240*240 IPS
F1 = help
F2 = rotors
F3 = rings
F4 = reflector
F5 = plugs
F6 = reset


VBUS
VSYS
GND
3V3_EN
3V3
ADC_VREF
GP28
AGND
GP27
GP26
RUN
GP22
GND
GP21
GP20
GP19
GP18
GND
GP17
GP16
SWDIO
DEBUG
SWCLK
USB
LED
BOOTSEL
© 2020
Raspberry Pi Pico
GP0
GP1
GND
GP2
GP3
GP4
GP5
GND
GP6
GP7
GP8
GP9
GND
GP10
GP11
GP12
GP13
GND
GP14
GP15

Component list

Capacitors

C1	100uF electrolytic (blue or black)
C2	10uF electrolytic (blue or black)

Semiconductors

REG1	LM2940 5V 1A LDO regulator (black/silver)
LCD1	1.3” 240 x 240 LCD display + 7-way SIL header
U1	Raspberry Pi Pico single-board computer

Miscellaneous

USB	USB type A keyboard socket
BATTERY	moulded battery snap + 4 x AA battery box

PCB
self-adhesive rubber feet x 4
nylon bolts, nuts, spacers x 4
PCB pillars x 4
SIL alignment pins x 4

Email: info@madlab.org
Web: www.madlab.org
Social: @clubmadlab