

Open Enigma for Dummies

v20140823

BJ Gleason

bjgleas@gmail.com

Making Everything Easier!™

Novelty Edition

Open Enigma

FOR
DUMMIES®

Learn to:

- Encrypt Messages!
- Decrypt Messages!
- Speak with a German Accent!

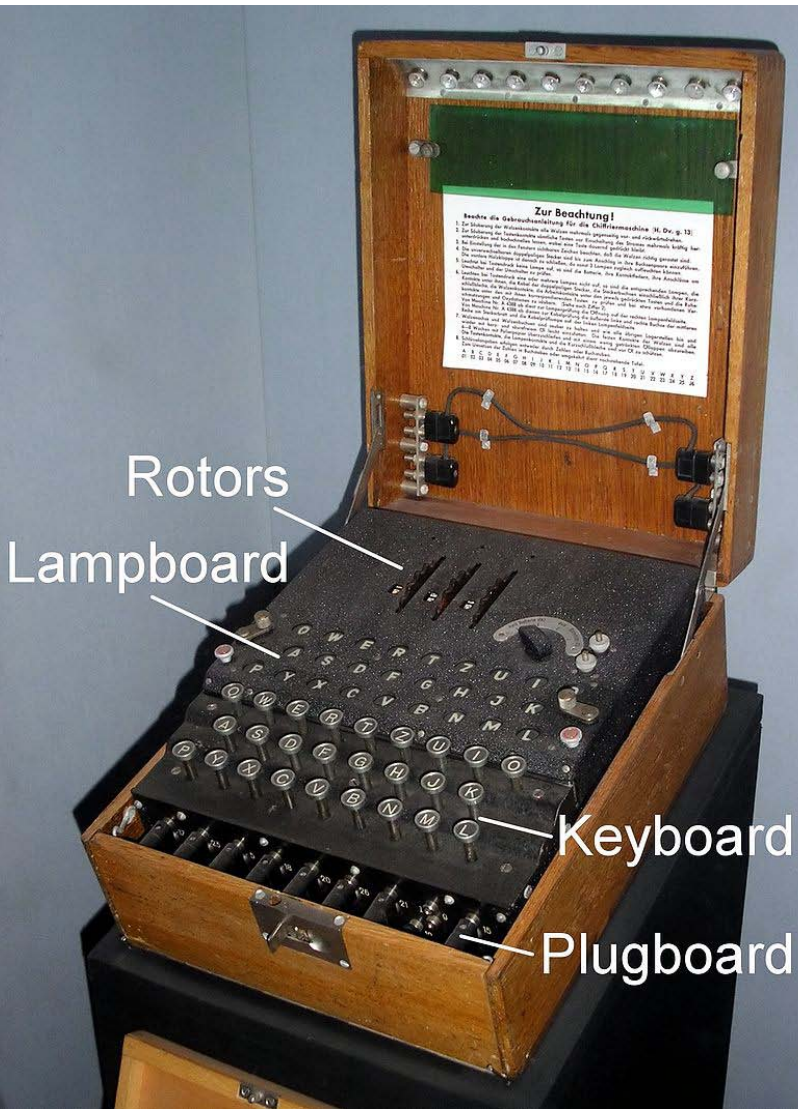
BJ Gleason
S&T GeoTronics



The Open Enigma

- The Open Enigma project was developed by S & T GeoTronics <http://www.stgeotronics.com>
- Emulates a 3 or 4 rotor Enigma machine
- Powered by Arduino Mega computer board
- Software or hardware plugboard emulation
- Funded by hundreds of people via Kickstarter
- Websites:
 - <http://www.openenigma.com/>
 - <http://openenigma.tumblr.com/>
 - <https://www.kickstarter.com/projects/438986934/the-open-enigma-project>

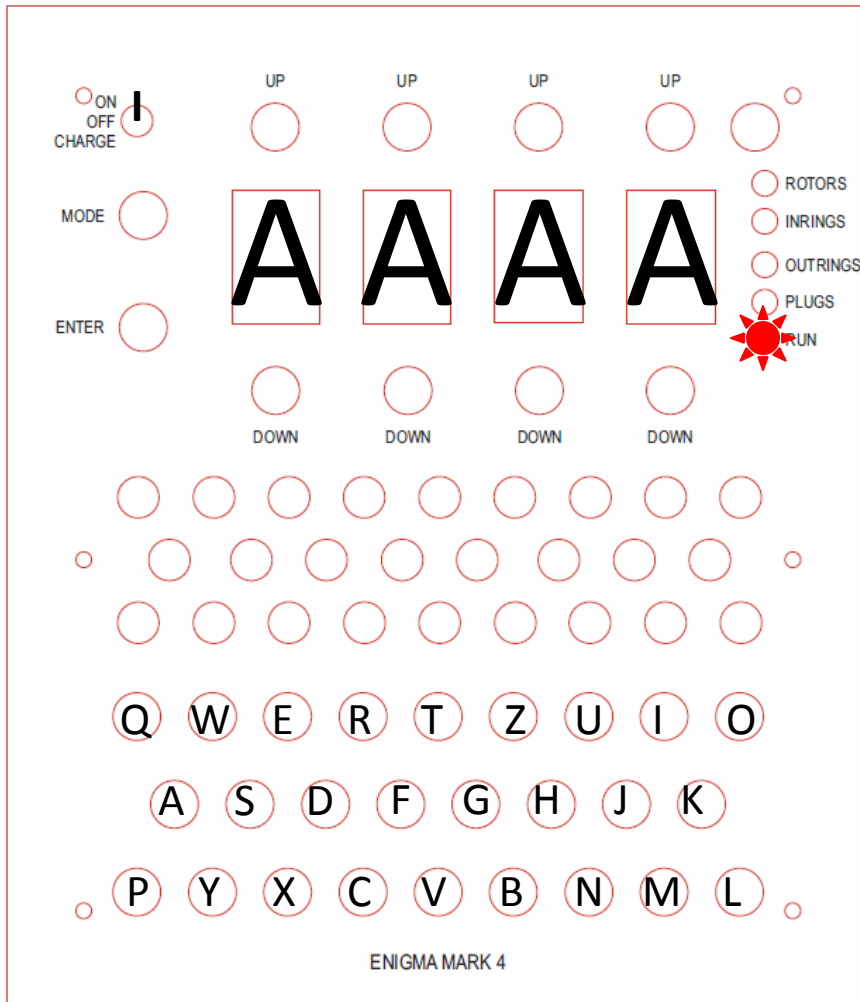
Real vs. Replica



Quick Start

- So you want to encrypt and decrypt a message?
- Turn the machine on, press <Mode> until the Run LED is on.
- Type your message, and record the lamps. That is your encrypted message.
- To decrypt the message, turn off the machine, turn it back on, press <Mode> to get to RUN
- Type in the encrypted message, and record the lamps. This will be your original message.

RUN



- Run LED is lit
- Press a key
- Record the lamps that turn on...
- We press E
- F lights Up
- The Outring Rotor display will now show AAAB

Let's Try It...

- Turn on the Enigma
- <Mode> to Run
- Enter the message: HELLO
- The Encrypted Message is: ILBDA
- Turn off/on the Enigma
- <Mode> to Run
- Enter the encrypted text: ILBDA
- The decrypted message is: HELLO

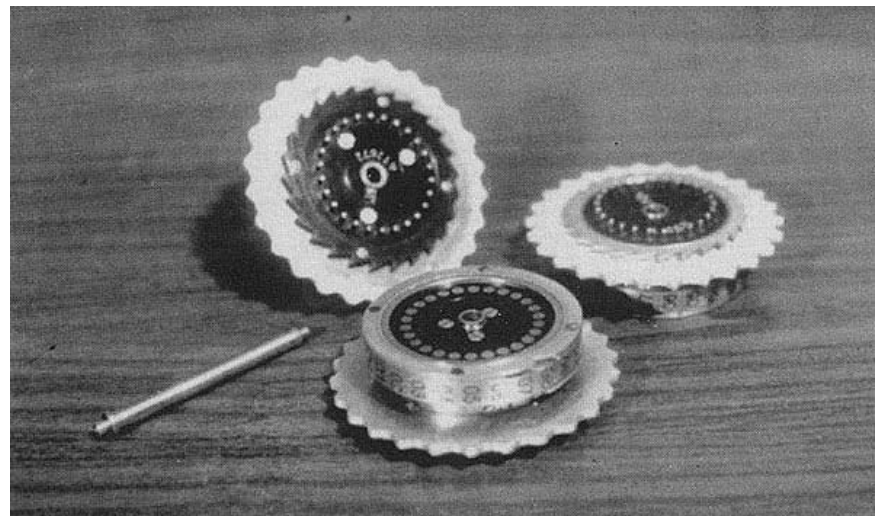
The Setting of the Quick Start

- But if someone else is NOT using the Open Enigma, they won't be able to decrypt the message, since their default settings are different.
- Here are the default setting for the Open Enigma
 - 4 Rotors: B123
 - Reflector: B
 - Internal Settings (Inrings): A A A A
 - External Settings (Outrings): A A A A
 - Plugs: (none)

How Many Rotors?



- Older Enigmas had 3 rotors.
- A 4th rotor was added to make it harder to break the codes.



3 and 4 rotor Compatibility

- The 4-rotor configuration with the B Rotor and the B reflector, with the 4th inring and outring rotors set to A is compatible with a 3-rotor machine, if all the other settings are the same.
- So if a 4 rotor machine wanted to send a message to a 3 rotor machine, here are the setting...

- 4 Rotors: B123
- Reflector: B
- Inrings: A A A A
- Outrings: A A A A
- Plugs: (same)

- 3 Rotors: 123
- Inrings: A A A
- Outrings: A A A
- Plugs: (same)

3 Rotor Enigma Simulator

- Written by Mike Koss
- <http://startpad.googlecode.com/hg/labs/js/enigma/enigma-sim.html>

Enigma Machine Simulator

by Mike Koss

Initialization

Rotors:

Rotor Start:

Rings:

Plugboard:

Encoding

A

A

F


Type Message Here:

HELLO

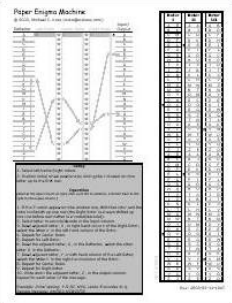

Read Output Here:

ILBDA

☒ **Preserve spacing**

Send to Twitter: 

To learn more about the [Enigma Machine](#), try using the [Paper Enigma](#). You can also read the [source code](#) used by this Enigma Simulator.



Digging Deeper

- We keep talking about
 - Rotors
 - Reflectors
 - Internal Settings (Inrings)
 - External Settings (Outrings)
 - Plugs
- What do they mean?
- How do they change the message?

Rotors

- The rotors were the mechanical wheels with letters or numbers on them.
- Each enigma would have 3 or 4 rotors, but those rotors were selected from many others
- The 4th rotor had 2 selections: Beta and Gamma
- The M4 Naval Enigma had 8 rotors to choose from - so the selection of rotors, and their positions would have an impact on the message.
- Learn more
 - http://en.wikipedia.org/wiki/Enigma_rotor_details

Reflectors

- Called Umkehrwalze in German (UKW)
- During WWII, there were 2 reflectors, B and C
- If B was used with Beta, or C was Gamma, it was compatible with the 3 rotor machines
- This allowed the same settings to be used for encryption and decryption.
- Learn more
 - <http://users.telenet.be/d.rijmenants/en/enigmatech.htm#reflector>
 - http://en.wikipedia.org/wiki/Enigma_machine#Reflector

Rotors and Reflectors



- The gamma reflector and rotors I, II, III, and "beta"
 - <http://w1tp.com/4sale/m18316/18316.htm>

Internal Settings (Inrings)

- The rotors actually had two parts - the external ring where the letters were, and an internal ring where the wiring was.
- The internal ring could be rotated so that it generate a different code.
- Learn more:
 - http://en.wikipedia.org/wiki/Enigma_machine#Rotors
 - <http://users.telenet.be/d.rijmenants/en/enigmatech.htm#wiringtables>
 - <http://users.telenet.be/d.rijmenants/en/enigmatech.htm#rotorencryption>

Internal Settings (Inrings)

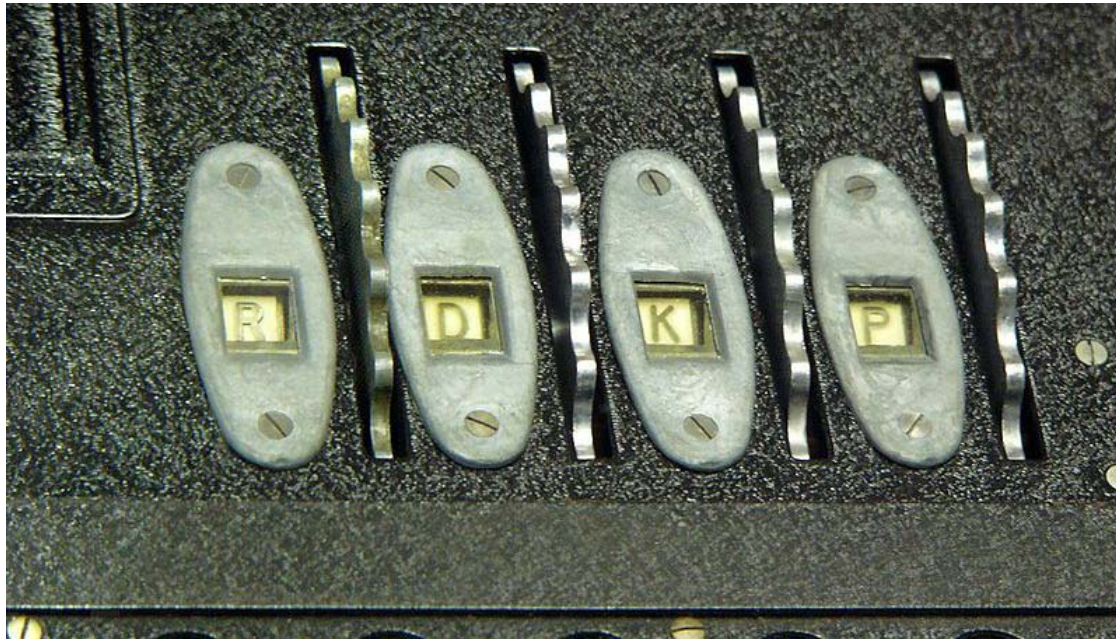


- This photo show the internal working of the rotor
 - http://en.wikipedia.org/wiki/File:Enigma_rotors_and_spindle_showing_contacts_ratchet_and_notch.jpg

External Settings (Outtings)

- This is the initial position of the rotors, set by the operator
- These would also be the setting for the session key
- As the operator typed, the rotors would increment, changing the code after each key.
- Learn more:
 - http://en.wikipedia.org/wiki/Enigma_machine#Rotors

External Settings (Outtrings)

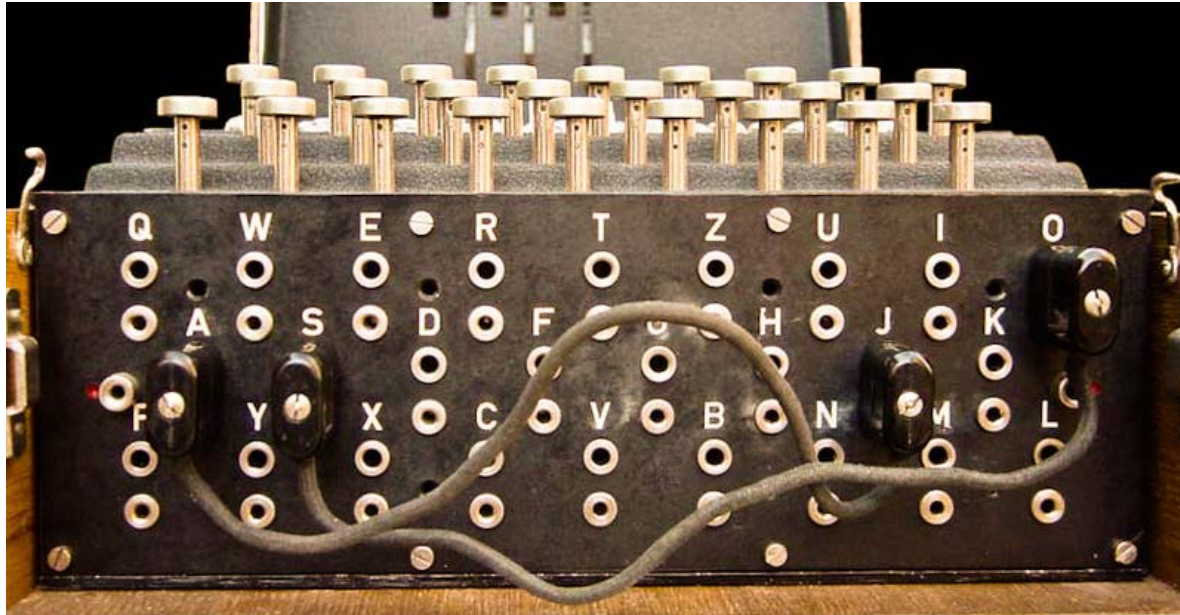


- The Rotors are set by spinning the wheels
 - <http://en.wikipedia.org/wiki/File:Enigma-rotor-windows.jpg>

Plugs

- The plugboard allowed letters to be swapped.
- If A and D are connected, then when A is pressed, a D is sent to the rotors.
- Up to 13 pairs can be swapped.
- The Open Enigma software emulation only allows up to 10 to be swapped.
- Learn more
 - http://en.wikipedia.org/wiki/Enigma_machine#Plugboard

Plugboard



- In this photo, A and J, S and O are swapped.
 - <http://en.wikipedia.org/wiki/File:Enigma-plugboard.jpg>

Summing Up

- By combining all the varying factors - rotor selection, rotor position, number of rotors, internal rotor settings, external rotor position, reflector choice, and plugs, and session key, we get an amazing number of combinations, making it difficult to crack.
- Combining three rotors from a set of five, the rotor settings with 26 positions, and the plugboard with ten pairs of letters connected, the military Enigma has 158,962,555,217,826,360,000 (158 quintillion) different settings.
 - http://en.wikipedia.org/wiki/Enigma_machine#Mathematical_analysis

The Message

- Here is an Enigma encrypted message:
YYW BQZ MOO LDL BXK WSZ XKY
- Can you decrypt it?
- To decrypt it, we will need an Enigma machine, and the settings the message was encrypted with.
- The settings would typically be sent out of band, and closely guarded.
- The message may also include a session key, an extra layer of complexity.

The Settings

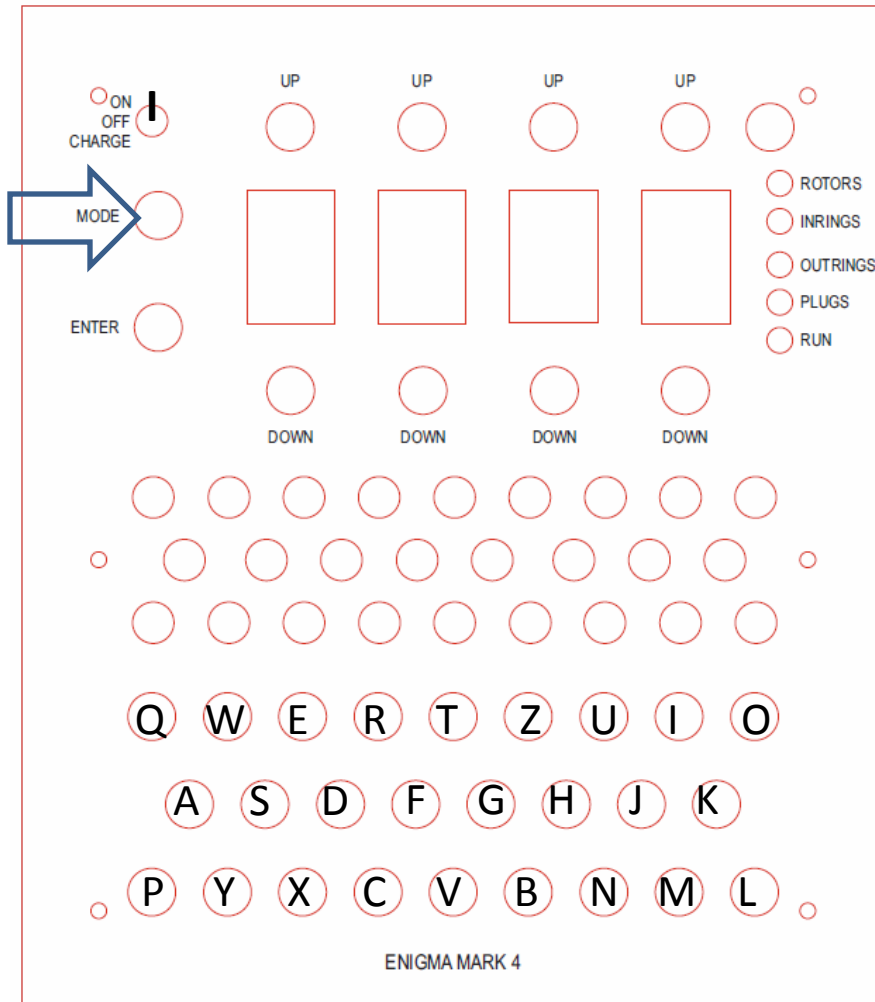
- 4 Rotors: G 4 5 6
 - Reflector: C
 - Internal Settings (Inrings): A B J G
 - External Settings (Outrings): O P E N
 - Plugs: A-Z, B-E, C-D
-
- How do we enter these settings in the Open Enigma?

Plugs

- If you want to use the hardware plugs, insert them BEFORE you turn on the machine.
- Here are the plugs for this message:

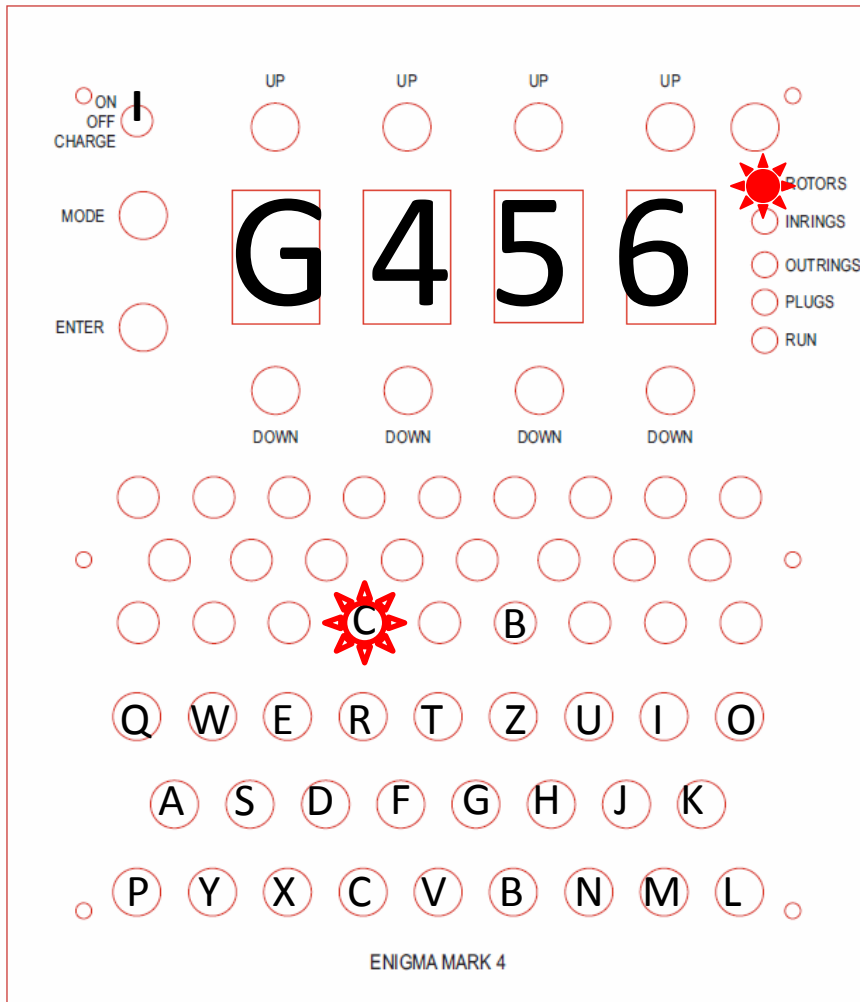


Turn it On



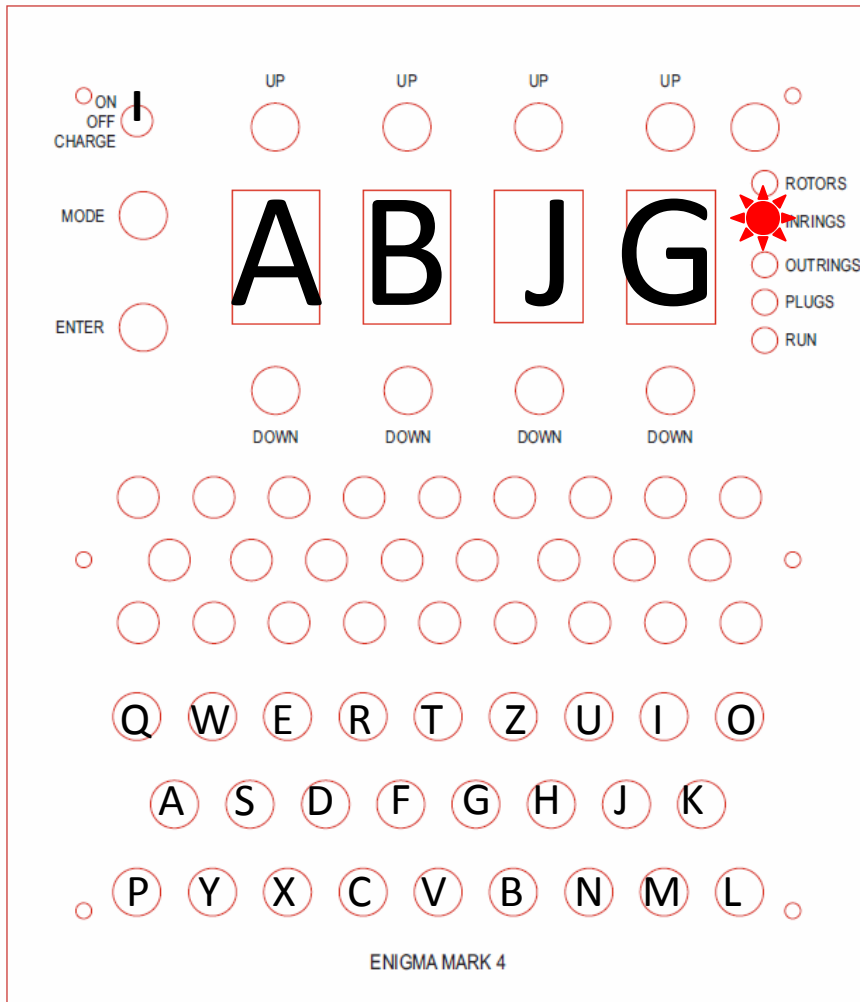
- Turn Power to ON
- Message will scroll
- Press <Mode>

Set Rotors



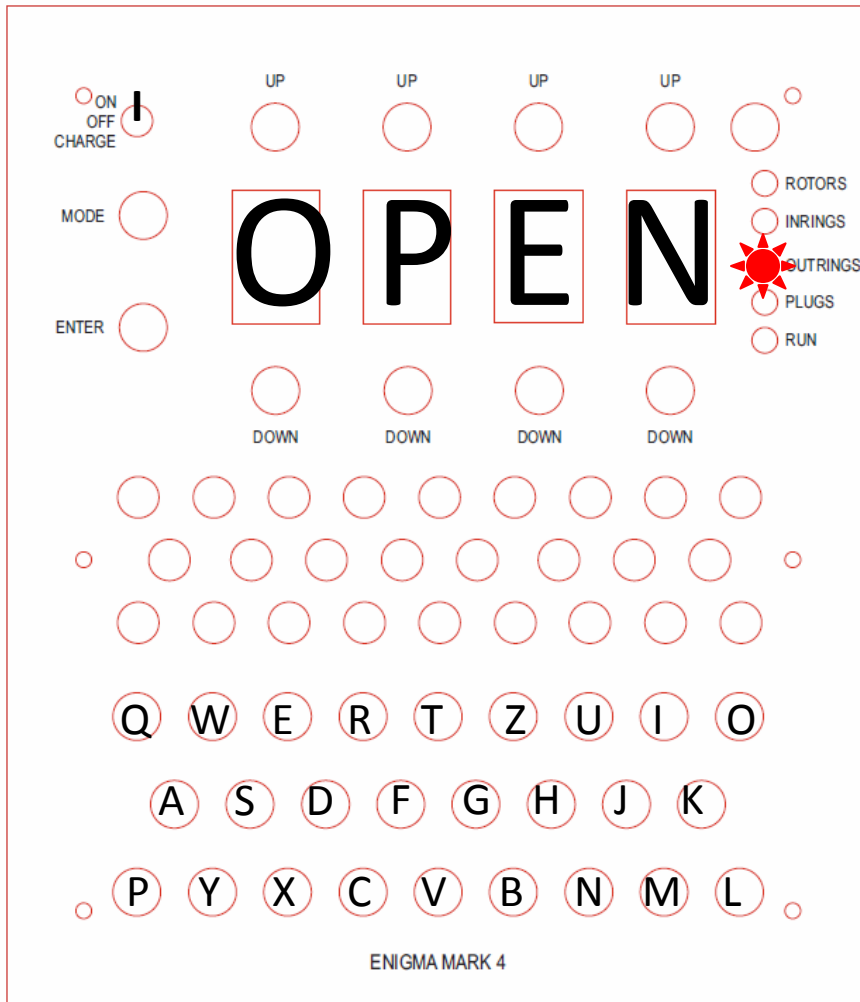
- Rotors LED is on
- Default: B123
- Set to: G456
- Notice B lamp lit up
- When you cycle to select B/G, you will see C/B lamps alternate.
 - That is the reflector
- Use Up/Down to set to G456
- C lamp should be lit
- <Mode>

Set Inrings



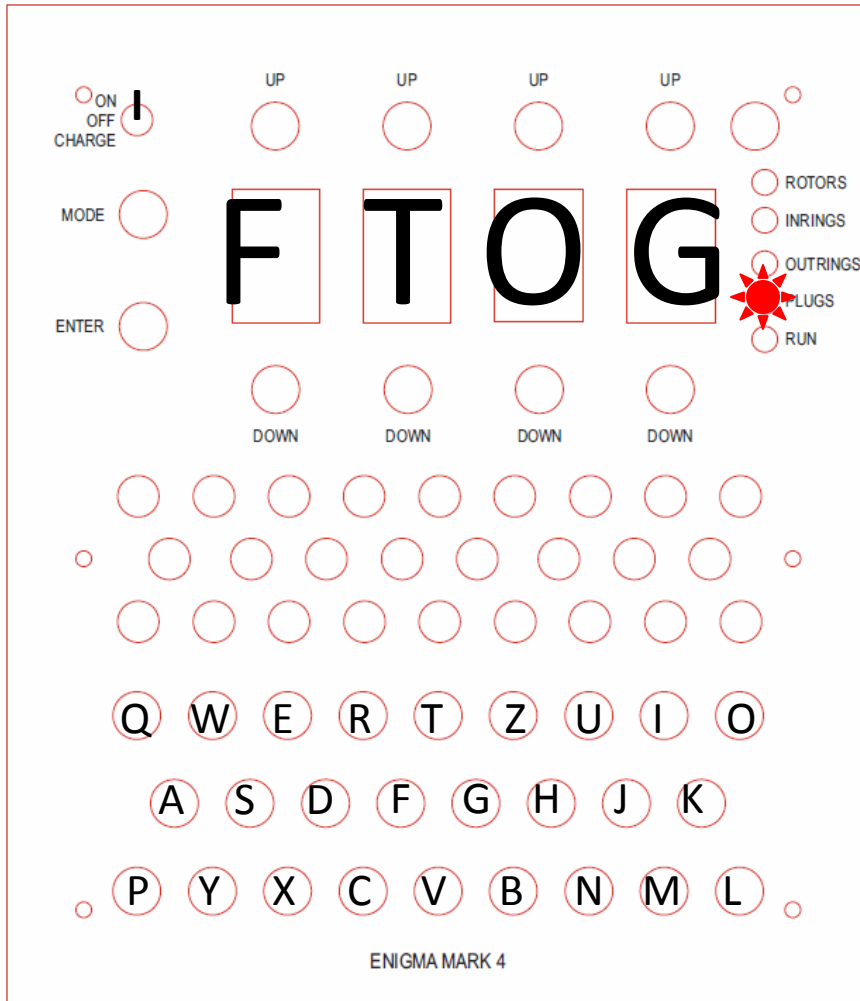
- Inrings LED is on
- Default: AAAA
- Set to: ABJG
- <Mode>

Set Outrings



- Outrings LED is on
- Default: AAAA
- Set to: OPEN
- <Mode>

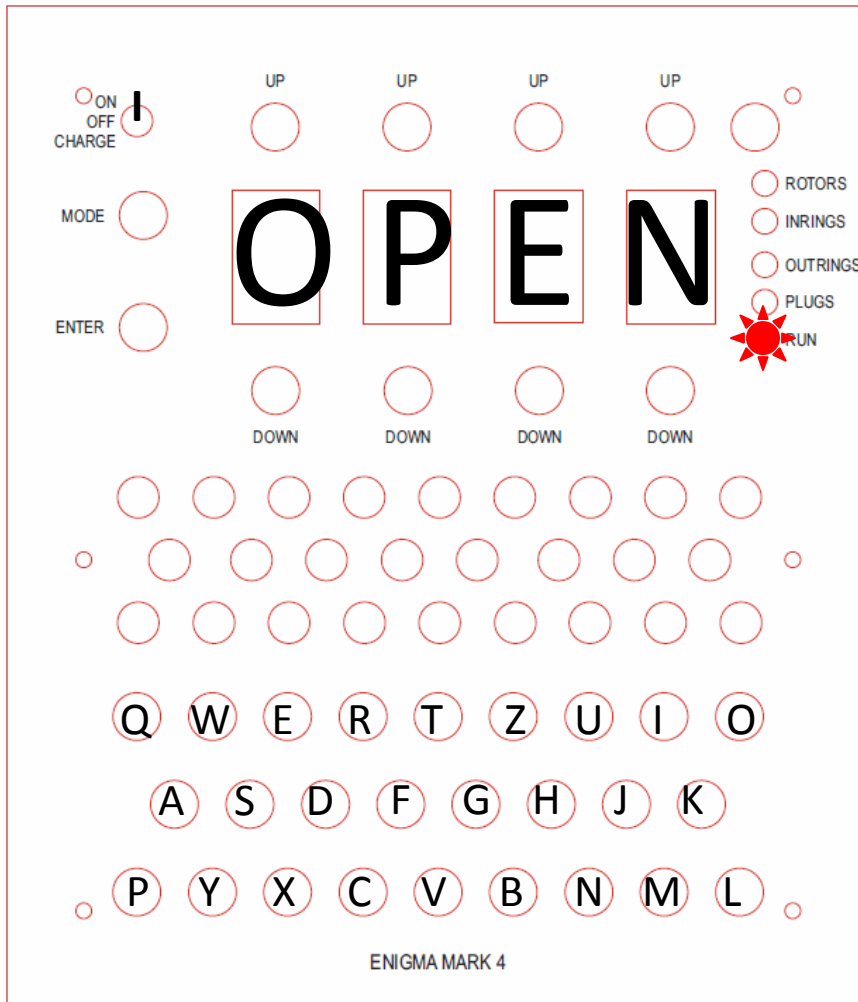
Set Plugs



- *Skip if using hardware plugs! Press <Mode>*
- Plugs LED is on
- Default: ATOB
- Set to:
 - ATOZ<Enter>
 - BTOE<Enter>
 - CTOD<Enter>
- When FTOG appears, press <Mode>

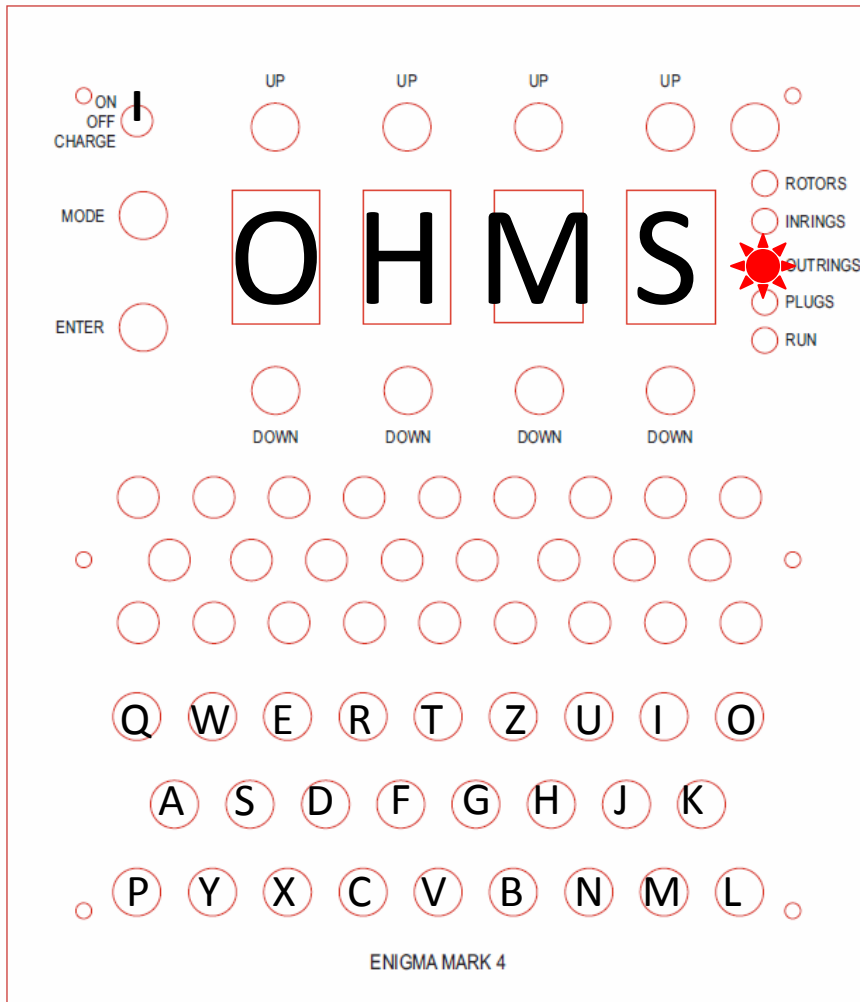
RUN

YYW BQZ MOO LDL BXK WSZ XKY



- Run LED is on
- Type in the first 3 characters to get session key - this is an extra layer of complexity.
- Type in next 3 characters to confirm
- YYW becomes HMS
- BQZ becomes HMS
- HMS is the session key

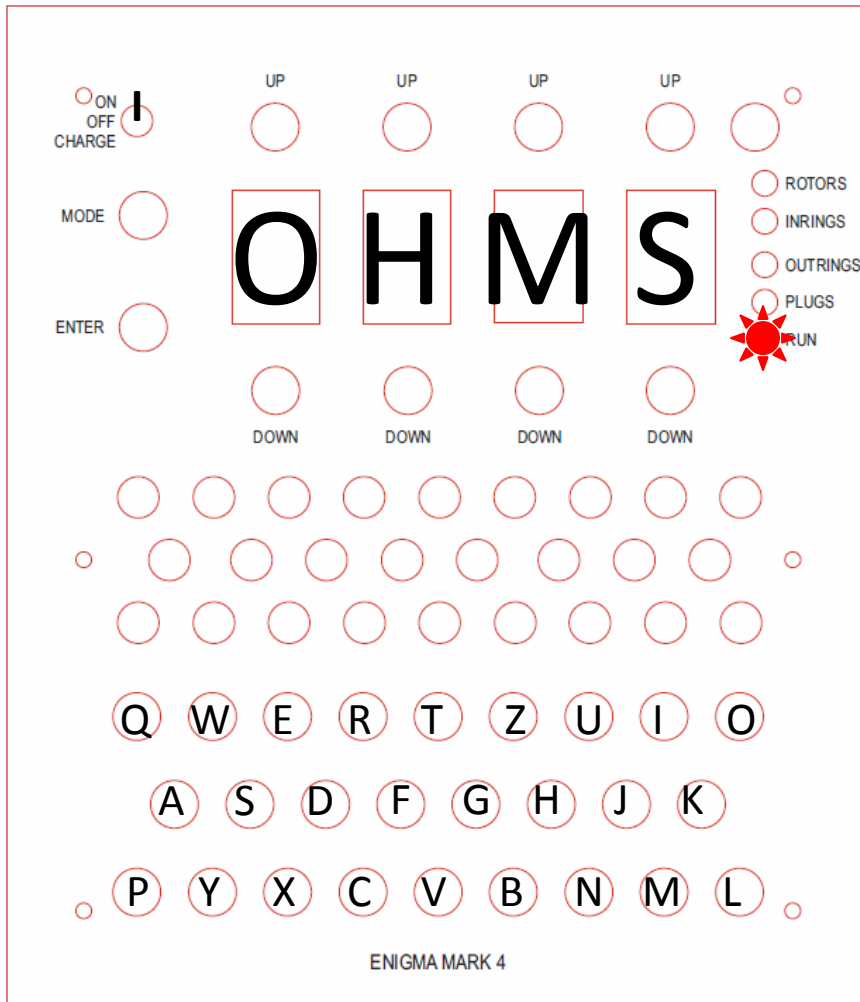
Set Outtings / Session Key



- <Mode> until Outtings LED is on
- Session key is 3 letters, so change last 3 letters to match session key.
- Set to: OHMS
- <Mode> to Run

RUN

~~YYW BQZ~~ MOO LDL BXK WSZ XKY



- Run LED is on
- Skip the session keys and enter the rest of the message: MOO LDL BXK WSZ XKY
- Are you decoding it properly?
- If you enter MOO, you should see LET appear... it is working!

Note on Messages

- Notice there are no numbers, punctuations, and there is no space bar on the machine.
- According to Wikipedia (http://en.wikipedia.org/wiki/Enigma_machine):
 - The Army Enigma machine used only the 26 alphabet characters. Signs were replaced with rare character combinations. A space was omitted or replaced with an X. The X was generally used as point or full-stop.
 - Some signs were different in other parts of the armed forces. The Wehrmacht replaced a comma with ZZ and the question sign with FRAGE or FRAQ.

The Enigma Coin

- From <http://www.geocaching.com/track/details.aspx?id=3334130>
- This coin has a encrypted message on it...



More Complex

- Based on Enigma M2114
- Rotors = G 1 6 3, Reflector = C
- Inner ring = A F U E
- Outer ring = A E G C
- Plugs: WS RF ZH BU DC GN JM AE
- SJDS FTTV WBZX PDUM YUCR NPLN OQDU RZLA
VGXO GURQ IORH NRDK MAIK VUVC XBSH DELV
XIIE HCRM JPQW JIAN TPWN KDRG PBBE KPSP
DCZB NTFK UWBY



Hints

- Open Enigma uses software to emulate the hardware plugs. You can enter the plug codes in any order, and in any direction... ATOZ is the same as ZTOA
- There is a session key in the message... After the session key (remember it is repeated), the next three decoded letters should be CON... if you get that, you are on the right path!

Selecting the Number of Rotors

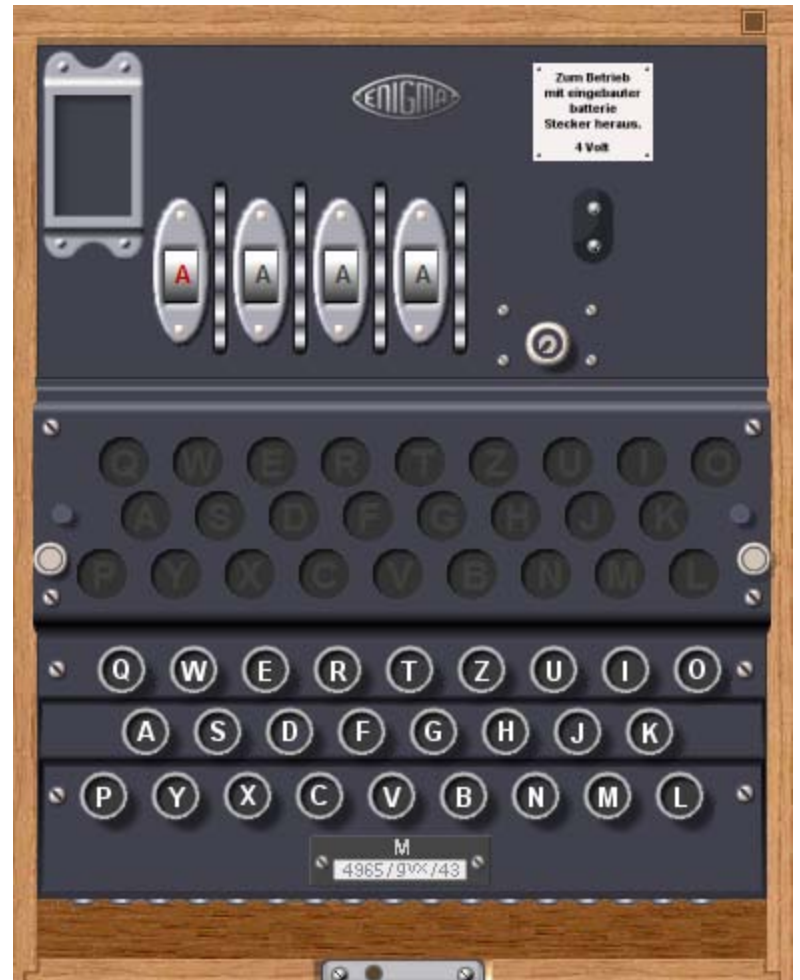
- The Open Enigma can emulate a 3 or 4 rotor machine, as well as a non-double step mode.
- To change modes, turn on the machine. Press the Left UP button.
- You will see the mode at the end of the marquee message, "S & T GeoTronics ENIGMA Mark 3 DT"
- Sequence
 - Mark 4, DT (default)
 - Mark 3, DT (1 press)
 - Mark 4, NDT (2 presses)
 - Mark 4, DT (3 presses)

Software Enigmas

- So your friends don't have an Open Enigma and you want to send secret messages back and forth?
 - Encourage them to get one!
- Or they can use Mike Koss' 3 rotor emulator
 - <http://startpad.googlecode.com/hg/labs/js/enigma/enigma-sim.html>
- Or Dirk Rijmenants' Enigma Simulator v7.0
 - <http://users.telenet.be/d.rijmenants/en/enigmasim.htm>

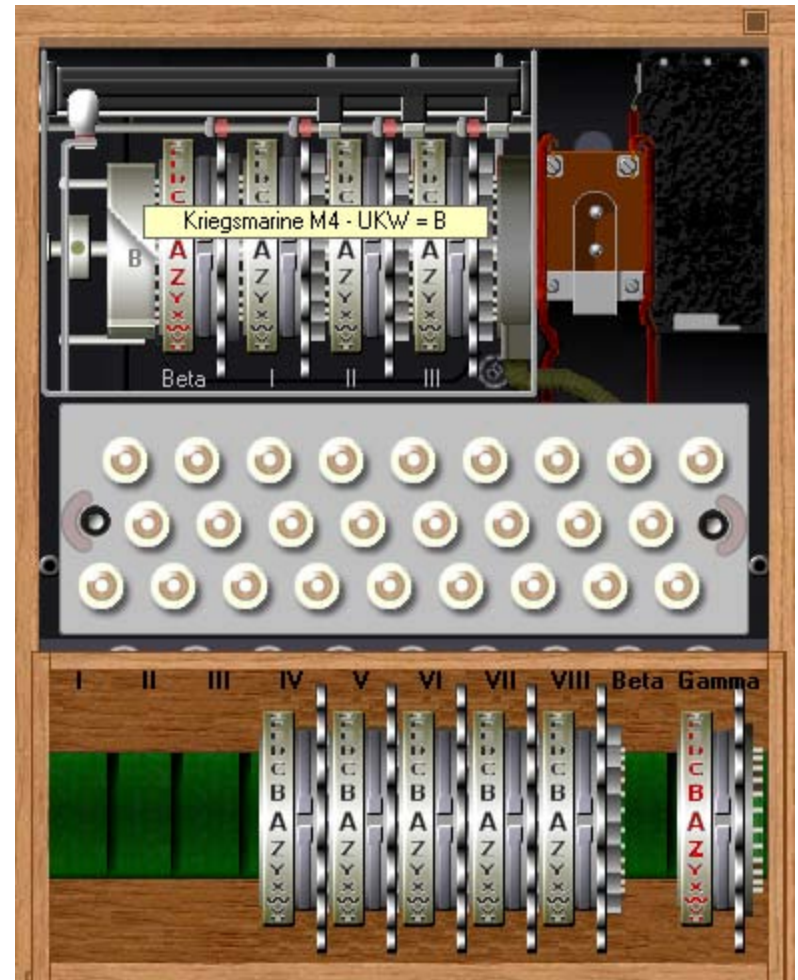
Enigma Simulator v7.0

- It installs locally on a Windows system
- It can emulate many different machines, and the documentation is excellent.
- You can "open" it up to change the rotors...



Setting it Up

- Set this emulator to Kriegsmarine M4 - UKW=B
- It will behave the same as the default setting for the Open Enigma.
- It is an amazing program, with a great set of instructions, and a very nice website.



Care and Feeding

- The Open Enigma is powered by internal Li-Poly rechargeable batteries.
- To recharge, turn the power switch to CHARGE, and plug in the power brick.
- The light on power brick will be **blue** until charge is complete, it will then turn **red**.
- You cannot use the Open Enigma while charging & you cannot charge it while using it.

Thanks

- Thanks to the terrific team at S & T GeoTronics for this great box.
- Thanks to all the great Enigma resources on the web.
- Feel free to distribute this document. If you have any corrections, suggestions, etc... send them to BJ Gleason, bjgleas@gmail.com
- Let's Have Some Fun!