

Created by Ray Alger

May 2015

This program emulates the infamous ENIGMA M4 machine used by German U-Boats to encrypt messages during the Second World War.

There are two versions of the emulator:

1. ENIGMA.bas which runs on a MaxiMite
2. ENIGMAD.bas for DOS MMBasic

Both programs work in the same way and use just the alphabet keys A to Z, the [Space Bar], [Enter] and [Esc] keys.(and of course [Ctrl [C] to stop the program). The screen displays the options available at different points. Both programs write the Text Out string to EnigOut.txt in the current folder.



There are minor differences between the two versions:

ENIGMA

- Pauses for you to write down the encrypted and decrypted text after 60 characters.
- Displays the lamp board

ENIGMAD

- Increases the limit to 200 characters (blocks >200 may have unpredictable results).
- Doesn't display the lamp board
- Supports COPY/PASTE to enter and save text from/to the clipboard.

There is also a program, ENIGMAG.bas, which runs in either environment to suggest a random setup for your emulator. It uses a Seed (any text string) to set the MMBasic random number generator to a repeatable starting point; change the Seed for a different setup.

Further reading

Plenty of information on these machines can be found on the web including authentic WW2 encrypted messages. A good place to start is the description of Enigma in one of these:

How Enigma Machines Work

<http://enigma.louisedade.co.uk/howitworks.html>

The Enigma and the Bombe

<http://www.ellsbury.com/enigmabombe.htm>

In the second one, forget about The Bombe for the moment.

Contents

ENIGMA and ENIGMAD Basic operation.....	2
Setup instructions:-.....	2
Coding and decoding	2
Notes on M3 ENIGMA.....	3
Generating a code book.....	3
ENIGMAG setup suggestion.....	3
German coding procedure	3

ENIGMA and ENIGMAD Basic operation

Setup instructions:-

Note: If you make a mistake during setup, kept going to the end.
Then press [Esc] then [S] to re-do the setup.

- Step 1. Press the letter B or C to select which REFLECTOR to use.
- Step 2. Press the [Space Bar] to select which ROTOR will be used in the position highlighted. Press [Space] again until the required ROTOR shows. Then press [Enter] to accept. Repeat until all ROTORS have been selected.
- Step 3. Adjust the RING SETTING for a ROTOR using the letters A to Z, then press [Enter] to accept. Repeat until all ROTORS are set.
- Step 4. Set up the PLUGBOARD by pressing the required letter pairs one after another, e.g. AI ER DO WF etc. The PLUGBOARD will highlight the connections as you go. If you make a mistake here just press the letter twice to remove the connection. Trying to plug a used letter is not allowed. Press [Enter] after all the connections are made.
- Step 5. The machine is now setup, but before you can start encrypting or decrypting you must set the ROTORS to their start positions. This is done in the same way as the RING SETTING in Step 3.

You are ready to go!

Coding and decoding

Text IN can be PLAIN TEXT to encode or ENCRYPTED TEXT to decode.

Text OUT will be the opposite.

Provided the SETUP and ROTOR start positions are identical, PLAIN TEXT in will produce the ENCRYPTED TEXT and ENCRYPTED TEXT in will produce the same PLAIN TEXT.

Often in operation it was required to change the ROTOR positions without changing the setup, Press [Esc] then [A] then follow Step 5.

Finally.

The LAMPBOARD is provided to give the feel of a real machine. You can type faster than the LAMPBOARD allows; the keyboard buffer will hold the keystrokes (Thanks Geoff!).

Characters typed will be displayed on a Pad 60 characters long (200 characters in the DOS version). If the Pad becomes full no more key presses will be accepted until the Pad is cleared by pressing [Enter] (write down the message first!). The last 5 characters will remain so you can find your place.

Notes on M3 ENIGMA

The M4 machines were so designed that messages sent and received on the 3 ROTOR M3 machines could also be accommodated. To do this on the M4 machine used "B" REFLECTOR with "beta" ROTOR or "C" REFLECTOR with "gamma" ROTOR, in both cases the left hand RING SETTING and ROTOR position must be set to "A", the remaining 3 ROTORS are set the same way as required by the M3 machine.

Generating a code book

There are a number of web sites that will generate a code book for you. One such is <http://enigma.louisedade.co.uk/dailykeys.html> .

ENIGMAG setup suggestion

Alternatively you can use the MMBasic program ENIGMAG.bas to generate a unique pseudo-random setup based upon a Seed. Use the same Seed, and you get the same setup. The Seed can be any text string, such as the 1 across clue in today's newspaper cryptic crossword or the first two words in the headline on the front page, thus it is very easy to come up with a varying key that both sender and recipient can know without communicating it.

For example, run ENIGMAG.bas and enter seed "e" (lower case and without the quotes).

You should get:

```
Reflector      = C
Rotor order    = beta VI IV I
Ring setup     = R Y Q Z
Plug board     = BU SK ZD OG AX PJ TF EV YQ IC
Rotor setting  = N P K J
Message key    = ADUE ZYJI
```

Set up Enigma with everything down to and including the Rotor setting.

Type the first 4 letters of the Message key in Text In.

Press [Esc] followed by [A] and reset the rotors with the result from Text Out.

Now paste in the following encrypted code as Text In.

UOGR GYRSK MFQIA BHSUU JMPJY UMGNU UKOCD NUDLK OBWPR ILOWS
VPZA

You should get the second part of the Message key followed by X and the message.

German coding procedure

Generally, the Germans followed the following procedure but there were variations. The above example follows this procedure.

1. Set up the machine from the code book for their area of operation and the date (Reflector, Rotor order, Ring setup, Plug board setup, initial Rotor setting).
2. Choose a Message Key (3 or 4 characters) and encode it.
3. Adjust the rotors to the encoded Message Key.
4. Type the message and write down the resultant encoded text on a message pad.
5. Messages were limited to 256 characters to make them more difficult to break. Continue in another message using the same setup but a different Message Key.