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 a 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 photocopies 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 a help message.

F2 – selects the rotors. Type **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 the rotors automatically resets all the ring and start positions to **A**.

shift F2 – displays the current rotor selection (**1** to **8** for each of the left, centre and right rotors).

F3 – sets the ring positions for the rotors. Type **A** to **Z** for each of the left, centre and right rotors.

shift F3 – displays the current ring positions (**A** to **Z** for each of the left, centre and right rotors).

F4 – sets the rotor start positions. Type **A** to **Z** for each of the left, centre and right rotors.

shift F4 – displays the rotor start positions (**A** to **Z** for each of the left, centre and right rotors).

shift F5 – displays the current rotor positions (**A** to **Z** for each of the left, centre and right rotors). 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.

F6 – sets the current reflector. Type **B** or **C**.

shift F6 – displays the current reflector (**B** or **C**).

F7 – sets the plug board. Type up to 13 pairs of letters **A** to **Z**. Press the **ENTER** or 'return' key after the last pair. Note that you can't connect a letter to itself, nor use the same letter more than once. **F7** followed immediately by **ENTER** will clear all the plugs.

shift F7 – displays the plug board (up to 13 pairs **A** to **Z**).

ESC or **HOME** – resets all the rotors to their start positions (i.e. clears the message). The display flashes twice to acknowledge.

DELETE or 'backspace' – deletes the last letter entered (i.e. steps the rotors back one position). The keyboard LED's flash twice to acknowledge. Note that there is only a single level of delete (the real Enigmas didn't have a delete key at all!).

While waiting for a setting to be entered *The Enigma Machine* displays '?'. If an invalid key is pressed it will display '!'.

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