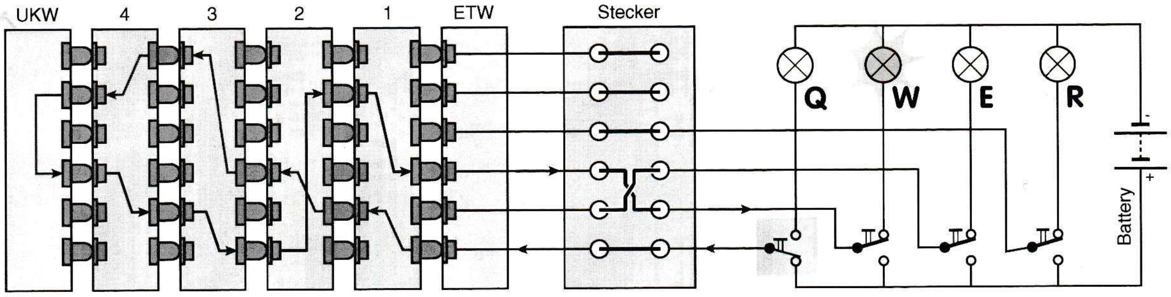
6. Working Principle of the Enigma

This is an attempt to describe the working principle of the Enigma. When developing our Enigma Simulator for RISC OS, we've searched the Internet and read many articles and books. Most articles give a rough description of the machine, but many important details, necessary to deduce the algorithm, are missing. This chapter describes the working principle of the Enigma machine in an easy to read manner. Any suggestions, that may help to clarify this matter further are most welcome. Please contact the authors at the address given on page 2.

6.1 Working Principle

When studying the working principle of the Enigma, we have to consider that there are in fact many different variants of this machine. Some of the differences make it impossible to decrypt a message that was encoded on another model. That does however not affect the working principle as explained here. For this we study the circuit diagram of an M4 Enigma.



ETW = STATIC WHEEL

Letters are 'scrambled' by a set of rotatable wheels each with 26 contacts on either side. Each contact on one side is connected (wired) to a contact on the other side in some random fashion. Some models, like the M3 have 3 such rotating wheels, but the M4 model, used later in the war during the U-boat war, has 4 wheels. Each time a key is pressed, the right most wheel is rotated by one step, resulting in a different mapping of the internal wires. A wheel has one or more notches that may cause the next wheel to be moved by one position too. This will result in a different encoding for each letter entered on the keyboard!

The keyboard consists of 26 keys, marked A-Z. Whenever a key, say '**Q**', is pressed the wheels will be moved into a new position and a contact is closed. As a result a current will flow. The wires from the 26 keys are connected to the Steckerbrett. The Steckerbrett may cause the letter to be swapped with another letter. The wires from the Steckerbrett are connected to a static wheel called the Stator or Eintrittswalze (ETW). The order in which the keys are connected to the 26 contacts on the ETW varies between the different Enigma models. In the diagram they are mapped in a linear fashion (i.e. A, B, C, etc.).

Leaving the ETW, the current enters the right most wheel (1) at the right hand side. The internal wiring of that wheel 'translates' this to one of the contacts of its left hand side, where it enters the next wheel, etc. Left of the rotating wheels is the Reflector, or Umkehrwalze (UKW). This wheel sends the current back into the rotating wheels, but this time the current flows from left to right, until it reaches the ETW again. From the ETW the current goes to the lamp board where the corresponding letter ('**W**' in the example) will be lit. It is inherent to this design, that a letter can never be encoded into itself.

Before starting the ciphering process, the Enigma needs to be setup in a way known by both sides. This means the wheel order (Walzenlage) needs to be known as well as the starting position of each wheel (Grundstellung). In order to further complicate things, each wheel has a settable index ring that moves the contacts independant of the wheel's alphabet. This is called the ring setting (Ringstellung).

Due to the fact that the current flows through the wheels twice (once from right to left, then from left to right), the cipher process is reversable. This means that encoding a letter is exacly the same as decoding. In other words: if '**Q**' becomes '**W**', then '**W**' would become '**Q**' (with the same Enigma settings).

(UKW)

UMKEHRWALZE = REFLECTOR

WAZENLAGE = "WHEEL ORDER"

GRUNDSTELLUNG = "STARTING POSITION"

RINGSTELLUNG = "RING SETTINGS"