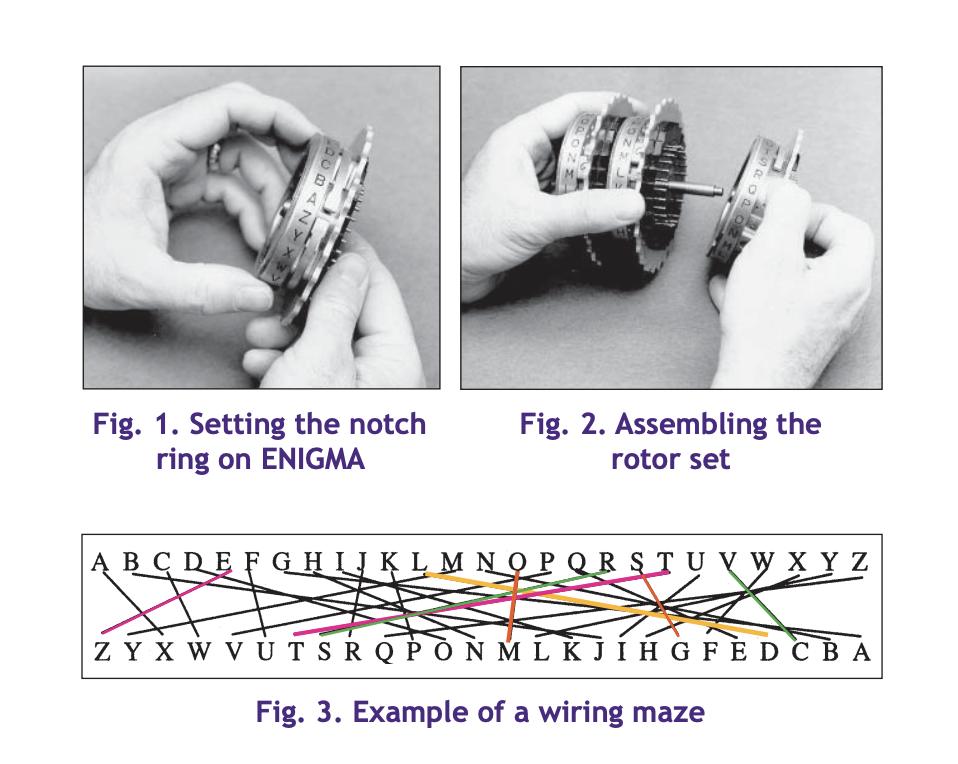
CPS485 Projects

Enigma Research



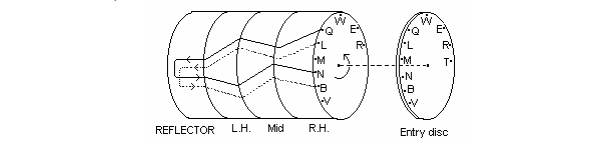
The rotors in the avware had five to eight rotors with 26 settings or letters to set up and each turn would cause the next rotor to turn selecting a different letter each time. Each rotor had a maze-like setup in order to make sure that when rotated it would have a different letter this would be changed daily.

<https://www.codesandciphers.org.uk/enigma/enigma3.htm>

<https://www.nsa.gov/portals/75/documents/about/cryptologic-heritage/historical-figures-publications/publications/wwii/german_cipher.pdf>

<https://cryptocellar.org/files/web+abwehr2.pdf>

According to one of the articles it was common that one message can be enciphered twice. Dilly Knox, a codebreaker who helped during World War 2 came up with the name “Crab” that described how the machine worked. Essentially once the you press a button it says that when enciphering a letter the three rotors and the reflector all happen to move one position



(i) The machine had a reflector which could be turned by hand like the commercial machine but which also moved during operation. (In contrast to the standard service Enigma for which there was a fixed reflector.)

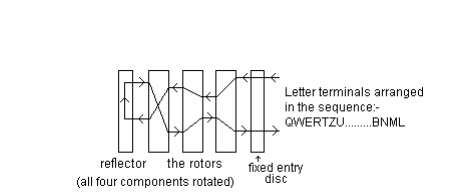
(ii) The machine had an entry disc on which the letter terminals were arranged in a circular pattern in the order QWERTZU…….BNML (clockwise when viewed from the right-hand side).

(iii) The rotors had a large number of turn-over positions, as otherwise “crabs” would be very rare. This was a feature not previously encountered (the standard service rotors had only one or two turn-over positions).

(iv) That there would be other positions at which all the rotors and the reflector turned over simultaneously, but without it happening again four positions later, as it did for a “crab”; Dilly Knox called this a “lobster”, claiming that it was half a “crab”. A lobster could be of assistance in the decipherment of the indicators, as will be shown later, and Knox immediately organised a “lobster hunt”.

The procedure used by the Abwehr operators was basically the same as that used before the war for the standard service version of the Enigma. The operator first adjusted all the ring settings and then set up the machine, locating the three rotors in a particular order. Both of these operations were carried out according to the instructions he had been given for the day. Then the reflector and three rotors were turned to the positions prescribed for the base setting (Grundstellung) for that day, so that the designated letter on each ring appeared in the corresponding window on the machine.

The operator then decided on the starting positions for the reflector and rotors that he intended to use (i.e. the message setting), and enciphered this four-letter sequence twice in succession on the machine, to produce the eight letters that made up the indicator. He then turned the reflector and rotors to the positions of his chosen message setting and proceeded to encipher the message.



<https://cryptocellar.org/files/web+abwehr2.pdf>