The Mathematics of the Enigma Machine

Student: Emily Yale **Supervisor: Dr Tariq Jarad**

The Enigma Machine is a mechanical encryption device used mainly by the German Forces during WWII to turn plaintext into complex ciphertext, the same machine could be used to do the reverse (Trappe and Washington, 2006). Invented by the German engineer Arthur Scherbius at the end of World War I the cipher it produced was marketed as 'unbreakable' (Trappe and Washington, 2006). Adopted by the German military forces, it worked by layering a number of substitution ciphers that were decided by an excess of 1.589×10^{21} machine settings. With help from Polish and French mathematicians, the cryptographer named Alan Turing created a machine known as the 'Bombe' which helped to reduce the time taken to 'break' an Enigma cipher (Imperial War Museums, 2015). The report this poster is based on focuses on the mathematics of the Enigma machine as well as the methods used to find the settings for a piece of ciphertext. Advantages and disadvantages of the Enigma code will be explored, alternative cipher machines are considered.

Aims and Objective

- A brief insight into Cryptography
- The history of the Enigma Machine
- The mechanism of the Enigma Machine
- The mathematics of the Bombe
- Understanding Group Theory

Cryptography

Although modern cryptography has many uses, Arthur Scherbius used classic cryptography to create the Enigma Machine and produce a method of secure communication. Classic Cryptography can be described as the science of encrypting and decrypting messages to ensure secure communication, it should be noted that this requires a key or a method of retrieving the key (Turing and Copeland, 2004).

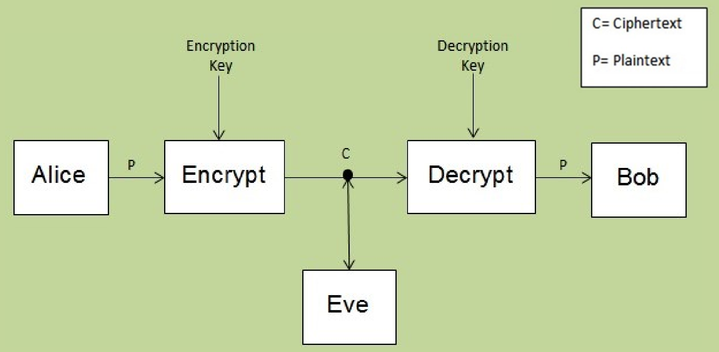


Figure 1: Basic Communication Scenario

A simple way of explaining cryptography when used for secure communication can be explain by the "Basic Communication Scenario" model above (Trappe and Washington, 2006) this can be seen in Figure 1. It should be noted that plaintext is a message that is easily read whereas ciphertext is text that cannot be read without the key.

References

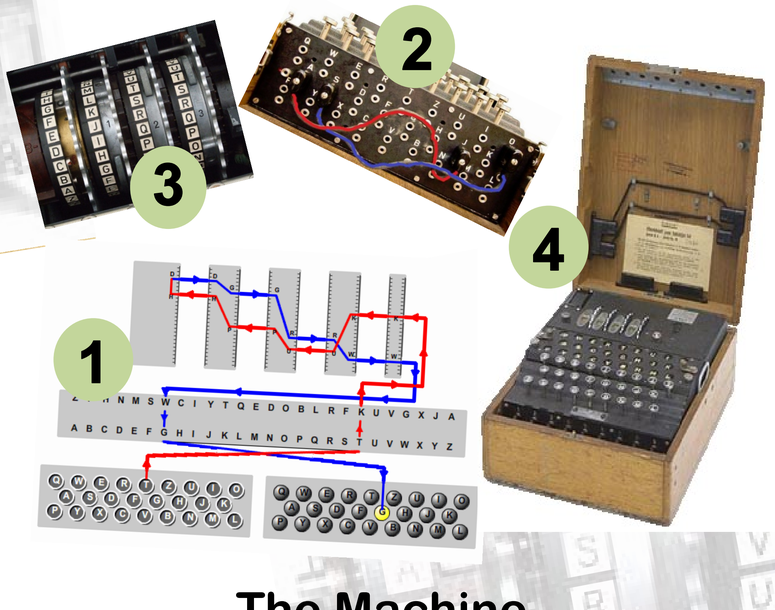
Oxforddictionaries.com, (2015) cipher - definition of cipher in English from the *Oxford dictionary*. [Online] [Accessed on 16 November 2015] http://www.oxforddictionaries.com/definition/english/cipher.

Imperial War Museums, (2015) *How Alan Turing Cracked The Enigma Code*. [Online] [Accessed on 20 October 2015] http://www.iwm.org.uk/history/how-alan-turing-cracked-the-enigma-code.

Trappe, W. and Washington, L. (2006) *Introduction to cryptography.* Upper Saddle River, N.J.: Pearson Prentice Hall.

Turing, A. and Copeland, B. (2004) *The essential Turing*. Oxford: Clarendon Press.

Images obtained from Google images



The Machine

1) **The Electrical Pathway -** The Enigma Machine has the appearance of an old fashioned type writer with a simple battery powered mechanism. Given that the settings are known, a person can input a letter on the keyboard , this triggers an electrical impulse to go through the machine, the machine uses 9 layers of encryption and then lights up a new letter on the lampboard .
2) **The Plugboard** - The plugboard takes the 26 letters of the alphabet and sorts them into 5-10 pairs, not that not all letters are affected. When a letter is inputted it is swapped to the other letter in the pair, the plugboard is used twice, once at beginning of the process and then at the end.
3) **The Rotors** - The rotors consist of a stationary rotor which does not change the letter the plugboard outputs and three rotors which each encrypt the letter once. After the forth rotor the letter is reflected, whilst encrypting the letter again, sending the electrical impulse back through the rotors and then onto the plugboard.
4) **The System -** An operator inputs a letter into the keyboards, the letter goes through the electrical pathway which sends an electrical impulse to the plugboard then the rotors and then back through the plugboard, this happens instantaneously to light up the encrypted letter on the lampboard (Turing and Copeland, 2004). .

Bombe (Group Theory)

The Bombe was a machine that could be used to find the key to an Enigma cipher. It was modelled on the Polish machine, Bomba, which could also do same before Enigma was enhanced. Bombe could find the settings on an Enigma machine that had been used to encrypt a ciphertext. Both Bombe and Bomba used trial and error along with a specific input to try the many possible settings until the correct settings were found. Bomba used the Germans' indicator system which could be used to find difference between rotor settings. The Germans saw the flaw in the indicator system so it was discarded so instead Bombe used a piece of known plaintext, called a crib, and the fact that Enigma could never encrypt a letter to itself (Turing and Copeland, 2004). To try every possible setting both machines would have taken a very long time, as the settings were changed daily and towards the war every 8 hours, this would have often been too long, i.e. with help from 'intelligence'. Group theory was used to limit the number of settings the machines had to test. Group theory worked by finding a fingerprint (pattern) given by the settings. Using the crib the operator would make a list of what the letters in the plaintext encrypted to in the ciphertext to , this could then be used to find the fingerprint. i.e.

$$\begin{array}{lcccccccc} & 1 & 3 & 5 & 6 & 2 & 8 & 4 & 7 \\ \text{Input} & A & B & C & D & E & F & G & H \\ \text{Output} & E & G & A & H & B & D & C & F \end{array}$$

$$\text{Fingerprint } (A\ E\ B\ G\ C)(D\ H\ F)$$

This fingerprint could be assigned to a certain number of possible settings, a list of possible settings was given in a catalogue made by the cryptographers (Trappe and Washington, 2006) .

Conclusion

The Report this poster is based on compares the Enigma machine to alternative cipher machines used by the Germans at around the same time in history (1939-1941). Advantages and disadvantages of the machine itself were found as well as the method of the applying the code produced by Enigma. The advantages of the machine include the fact that the ciphers it uses were that of random substitution making them unpredictable and without formula. Although it can be simple to find a key to a single random substitution ciphers the Enigma machine makes it much harder by using 9 layers of encryption meaning that frequency analysis is rendered useless. The disadvantages found include the main flaw of the machine itself, that the machine never encrypted a letter to itself, meaning that the use of cribs was possible and furthermore group theory. As well as this, the report exposes the operator errors that led to Enigma being broken.