Final Report

Abstract

*Enigma Machines were used in the main during World War II by the German military. It was a device which scrambled plain text into ciphered text. This project demonstrates both the enciphering and deciphering of the Enigma machine in a graphical simulation. The simulation demonstrates the movement of the rotors, within the machine, which presents a 3D graphical visualisation of the process of encrypting plain text into cipher text.*

Intro

With the outbreak of wireless communication in the early 1900s, there was a necessity for secure communication, particularly for military. With this came the invention of a Enigma machine in 1918, invented by a German engineer, Arthur Schebius, later the enigma machine patented in 1919. In the 1920s early models were used commercially, and later adopted by Nazi Germany before and during World War II. The Enigma machine was an electro-mechanical device which scrambled a plain text message into ciphered text using a letter substitution systen. This enabled the military forces to communicate using coded messages.

In this project a graphical Enigma simulator was developed, which represented the inner working of the process of encryption, plain text to cipher text, as well as the process of decryption, ciphered text to plain text. The simulator will provide a greater detail of the processes in a 3-Dimensional graphical format. The simulation, developed by C++ language, also allowing users to encrypt their own text. In the background section, some historical information about the Enigma machine are presented, which enhance the understanding of Enigma machines.

Background

History

The Enigma machine was invented by a German engineer in 1918 and later adopted by Nazi Germany before and during World War II. The Enigma was a device used by the Germans to communicate with their allies using encrypted messages. The enigma consisted of a keyboard of 26 letters in the pattern of the normal German typewriter, but with no keys for numeric or punctuation characters. Behind the keyboard was a lamp board made up of 26 small circular windows, each bearing a letter in the same pattern as the keyboard, which could light up one at a time. Behind the lamp board was the scrambler unit consisting of a fixed wheel at each end, and a central space for three rotation wheels. Message were limited to a maximum of 250 letters to avoid the inner mechanism returning to the same position because the sequence would repeat itself after 17,576 (26x26x26) key rings. Had the messages not been limited then British code-breakers may have been able to break the encrypted messages. Thus potentially the number of cipher text alphabets was vast and this led German military authorities to believe in the absolute security of this cipher system [1]. The first Enigma machine was heavy and bulky.

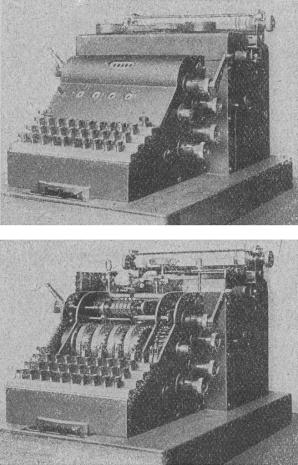


Figure 1 – Enigma A (Crypto Museum, 2008)

Various versions of the Enigma machine were developed, each with varying rotors. In 1926, a commercial version of the Enigma machine was purchased by the German Navy and adapted for military use. A special Enigma was developed by Chiffriermaschinen-AG, which had rotors that have the same contact alignment as the D rotors, but with teeth, multiple notches and are advanced cog wheels instead of pawls and ratchets. This model lead to the Enigma G. The Enigma G had different rotors with a zigzag pin placement and the counter on its right. Its rotors, which also had multiple notches, were moved by a system of gears.

The German forces, the Wehrmacht, in 1932, revised the commercial Enigma D and added the plugboard at the front of the machine. This version, known as Enigma I, became known as the Wehrmacht Enigma and was introduced on a large scale in the Army and public authorities. Initially this enigma came with three rotors, however from 1939 onwards they were equipped with five rotors. The Wehrmacht model was later adopted by the German Navy, with its securer plugboard and the extended set of rotors of eight. [2]

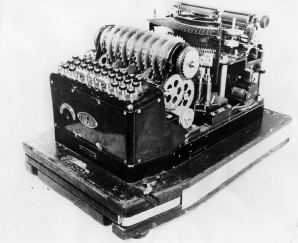


Figure 1-1 – The Wehrmacht Model (Crypto Museum, 2009)

Breaking the code

The Germans believed that the messages being sent to their allies were not breakable. However, the code breakers based at Bletchley Park cracked the secret messages being broadcasted, which played a crucial role in the defeat of Germany.

The Polish were the first people to come close to cracking the Enigma code. Marian Rejewski, Henryk Zygalski and Jerzy Rozicki were three mathematicians who successfully cracked the Enigma. They also developed an electro-mechanical machine, called the Bomba, to speed up the code breaking processing. [2] With the invasion of Poland looming, the Poles shared their information with the British, who in turn established the Government Code and Cipher School at Bletchley Park, however it was only in 1941 where their work began to pay off meaningfully when they were able to gather evidence of the planned invasion of Greece. [3]

Bletchley Park

Previous Work

Specification

Design

Implementation and Testing

Evaluation

Usability

Other Criteria

Summary and Conclusions

Acknowledgment

References

[1] **Royal Naval Museum**. ‘The Enigma Machine’ [Online].

Available at:

http://www.royalnavalmuseum.org/info\_sheets\_enigma.htm

(Accessed at: 27/10/2014)

[2] **Rijmenants D.** ‘The German Enigma Cipher Machine’ [Online].

Available at:

http://users.telenet.be/d.rijmenants/en/enigma.htm

(Accessed at: 27/10/2014)

[3] **History** ‘Code Breaking’ [Online].

Available at:

http://www.history.co.uk/study-topics/history-of-ww2/code-breaking

(Accessed at: 11/11/2014)