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. 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 allows users to encrypt their own text.

Background

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 16,900 (26x25x26) 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 ciphertext alphabets was vast and this led German military authorities to believe in the absolute security of this cipher system.

Specification

Design

Implementation and Testing

Evaluation

Usability

Other Criteria

Summary and Conclusions

Acknowledgments