Enigma Simulation Proposal

By Cryptopher Columbus

This Project will to simulate the historic Enigma machine encryption scheme. The project will be divided into three different sections: encryption, decryption and exploration of the enigma system.

First, this project will implement the enigma machine in software, coding its encryption algorithm to simulate encrypting a plain text message and getting a ciphertext back. This will simulate traditional enigma configuration and settings.

Secondly, this project will implement decryption strategies used by the British in the Second World War to crack the keys for various messages.

Finally this project will describe the cryptographic nature of the enigma machine, how the machine works, and what the strategies were used to break the machine.

The Presentation will focus on the encryption and decryption software to simulate the enigma machine and the paper will study the crypt used and what was done to crack it.