CSC 592 Cryptography

Proposal for Project – Digital Enigma

The Enigma was a pivotal WW2 German code machine. It used three to seven mechanical rotors to produce a product cipher with a key that changed for each character encoded. We propose to create a digital version of the Enigma that runs on a standard windows or Linux PC. The implementation language will be C++. This product includes three deliverables:

(1) A digital simulation of an enigma machine (the model).

2 weeks – on schedule

(2) An openGL interface that reflects the machine operation, including rotor positions, cyphertext, plugboard state, and keyboard. An additional Enigma may be rendered to display the plaintext coming out of an equivalently configured machine.

4 weeks – not yet started

(3) A separate stand-alone application that configures an Enigma machine via a series of questions, then writes it into a file. This text file can be edited, or loaded directly into the Digital Enigma. It includes any number of custom rotors (permutations) and an optional key (rotor starting position).

Deliverable complete.

Please consider this proposal for the CSC 592 project.
Mike Johnson
Matthew Bennett