Project Specification Document **Alex Gillies, LLLL76**
Project Title: Engima and BOMBE simulation
Supervisor: Matthew Johnson
Degree: Computer Science

Description: The Enigma is a electro-mechanical rotor cipher machine used to protect commercial, diplomatic and military communication by encrypting it. The BOMBE is an electomechanical device used by British Codebreakers during World War Two to break the Enigma-Encoded messages used by the German millitary. This project will aim to simulate both the Engima and BOMBE; it further aims to have the BOMBE show its effectiveness by running on and breaking some of the Enigma simulations encoded messages. The advanced aims are to expand the scope of the BOMBE to incorperate modern computational power. This will be done by utilizing the power of parallel computing.

Preliminary Preparations

- A thorough undertanding of the functioning of the Enigma Machine.
- A thorough undertanding of the functioning of the BOMBE.
- A thorough understanding of parallel programming.
- A survery of parallel programming techniques.

Minimum Objectives

- Simulate Enigma and show its correctness, by encrypting plaintext and comparing this to its known ciphertext to show this correctness, this should be done over a significant database of plaintext and ciphertext.
- Simulate BOMBE and show its correctness, taking some of the aformentioned stock ciphertext and running the BOMBE on this input such that the plaintext is output as the result.

Intermediate Objectives

- Prove the correctness of the Enigma simulation by encrypting plaintext and comparing this to its known ciphertext to show this correctness. This should be done over a significant database of plaintext and corresponding ciphertext.
- Prove that the BOMBE simulation is correct by taking all of the aformentioned stock ciphertext and running the BOMBE on this input such that the plaintext is output as the result.
- Both simulations should also be proved to be effective on random inputs and also in relation to one another; the Enigma machine should be run on a random input and the output should then be used as the input on the BOMBE which should in turn return the random plaintext.
- Evaluate average computational time on inputs of a set size.

Advanced Objectives

- Increase the scope of the BOMBE simuation by running the simulation in parallel. This means that different parts of the ciphertext could be run in parallel or the whole cipher text being run with each parallel part testing different configurations of the Engima machine.

References

- https://en.wikipedia.org/wiki/Parallel_computing
- https://en.wikipedia.org/wiki/Enigma_machine
- https://en.wikipedia.org/wiki/Bombe