# Enigma and BOMBE simulation

Student Name: A.L. Gillies

Supervisor Name: M. Johnson

Submitted as part of the degree of MEng Computer Science to the

Board of Examiners in the School of Engineering and Computing Sciences, Durham University

***Abstract —***

**Context/Background** - Can antiquated ideas and designs be brought up to speed in the modern day? The aim of this paper is to show the plausibility of this using the Enigma and the BOMBE, two cryptographic devices from the second world war, these will be modernised and tested to prove this hypothesis.

**Aims** - Using the known execution speed of the antique Enigma and BOMBE, the aim of this paper is to show, through implementation and testing of a modern interpretation of the Enigma and BOMBE, the speed up that has occurred since the inception of both.

**Method** - After both the Enigma and BOMBE are implemented the BOMBE will then be improved on using parallelisation techniques. Each will then be tested. The time taken for a standard Enigma machine to encrypt, the computerised version to encrypt and the parallelised version to encrypt will be compared to one another to give a good indication of the improvements over time. Another comparison will be made between the standard Enigma, the computerised Enigma and the parallelised Enigma, this should re-enforce the indication of computer improvements.

**Proposed Solution** - The Enigma machine will be implemented through C++ code, this will form the baseline for a modern interpretation of the machine as it will not run anything in parallel. This code will then be parallelised using different standardised tools and techniques, these will then be used as the final comparison to show the significant increases in performance that this seemingly antiquated idea can expect across different inputs.

***Keywords —*** Enigma, BOMBE, Parallel, Modern, Computation, Evaluation, Reinterpretation, Comparison, C++, Antiquated.

## I INTRODUCTION

What the project is about - talk through the motivations and a rough outline of the project
Context of the project - what are some real world things that need to be taken into account
Research question -
What was achieved - go through deliverables and then go through issues and counter
2-3 pages

## II RELATED WORK

Survey relevant literature
Relate to your own project

May be able to reuse parts of the literature survey
2 pages

## III SOLUTION

Overview of architecture and design - use parts from the design report
Description of tools used - design report
Outline of algorithms to be used - design report
Features of the implementation process - issues and struggles with the implementation, how they were overcome
Testing - validation and all other testing done
Verification and validation
Stages of the life cycle undertaken - software engineering
4-7 pages

## IV RESULTS

Evaluation method description
Experimental settings (if experiments are carried out) - no experiments were carried out
Results generated by the software
2-3 pages

## V EVALUATION

Discussion of strengths and weaknesses of solution and of lessons learnt - evaluate issues
Limitations of the solution - given more time...
Critical appraisal of the way the project was organised - critique my own organization
2-3 pages

## VI CONCLUSION

An overview of the project
Brief description of the main findings
Discussion on how the project can be extended
1-2 pages

## *A References*

### References

*Enigma – Britannica Academic* (n.d.).
**URL:** *http://academic.eb.com.ezphost.dur.ac.uk/levels/collegiate/article/32677*

*Navy M3/M4 Enigma Machine Emulator* (n.d.).
**URL:** *http://enigma.louisedade.co.uk/enigma.html*

Stoler, M. S. (2007), 'Re-engineering the Enigma Cipher'.

*The Turing Bombe - Cribs and Menus* (n.d.).
**URL:** *http://www.ellsbury.com/%5C/bombe1.htm*