Enigma and BOMBE simulation

Student Name: A.L. Gillies

Supervisor Name: M. Johnson

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

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

Abstract — These instructions give you guidelines for preparing the design paper. DO NOT change any settings, such as margins and font sizes. Just use this as a template and modify the contents into your design paper. Do not cite references in the abstract.

The abstract must be a Structured Abstract with the headings **Context/Background**, **Aims**, **Method**, and **Proposed Solution**. This section should not be no longer than a page, and having no more than two or three sentences under each heading is advised.

Context/Background - The world has changed significantly in the last fifty years. Ideas that were had before modern computing was fully realised need to be re-evaluated with a modern perspective. One such example is the Engima machine and it's counterpart, the BOMBE. What is the computational speed up from 1940 to now?
talk about the background and why the project is being done.

Aims - The aim of this paper is to show the improvements of modern computing using the comparison of an antiquated design against several modern re-interpretations.
what are the end goals?

Method - After both the engima and BOMBE are implemented they will then be improved on using modern techniques. Each will then be tested. The time taken for a standard engima 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
how will we reach the end goals?

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 modern techniques, these will then be used as the final comparison to show the significant increases in performance that any antiquated idea can expect.
what is the system?

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

I INTRODUCTION

This section briefly introduces the project, the research question you are addressing. Do not change the font sizes or line spacing in order to put in more text.

Note that the whole report, including the references, should not be longer than 12 pages in length (there is no penalty for short papers if the required content is included). There should be at least 5 referenced papers.

II DESIGN

This section presents the proposed solutions of the problems in detail. The design details should all be placed in this section. You may create a number of subsections, each focusing on one issue.

This section should be up to 8 pages in length. The rest of this section shows the formats of subsections as well as some general formatting information. You should also consult the Word template.

A Main Text

The font used for the main text should be Times New Roman (Times) and the font size should be 12. The first line of all paragraphs should be indented by 0.25in, except for the first paragraph of each section, subsection, subsubsection etc. (the paragraph immediately after the header) where no indentation is needed.

B Figures and Tables

In general, figures and tables should not appear before they are cited. Place figure captions below the figures; place table titles above the tables. If your figure has two parts, for example, include the labels "(a)" and "(b)" as part of the artwork. Please verify that figures and tables you mention in the text actually exist. make sure that all tables and figures are numbered as shown in Table 1 and Figure 1.

Table 1: UNITS FOR MAGNETIC PROPERTIES

Symbol	Quantity	Conversion from Gaussian

C References

The list of cited references should appear at the end of the report, ordered alphabetically by the surnames of the first authors. The default style for references cited in the main text is the Harvard (author, date) format. When citing a section in a book, please give the relevant page numbers, as in (**?**, p293). When citing, where there are either one or two authors, use the names, but if there are more than two, give the first one and use "et al." as in , except where this would be ambiguous, in which case use all author names.

You need to give all authors' names in each reference. Do not use "et al." unless there are more than five authors. Papers that have not been published should be cited as "unpublished"

(**?**). Papers that have been submitted or accepted for publication should be cited as "submitted for publication" as in (**?**) . You can also cite using just the year when the author's name appears in the text, as in "but according to Futher (**?**), we . . . ". Where an authors has more than one publication in a year, add 'a', 'b' etc. after the year.