Project Proposal

by Robert Biedron

Enigma Emulator

Project Proposal

B00030071 – Robert Biedron

10/13/2011

Contents

1. Abstract

This project proposal document describies development of Enigma emulator software. This project would attempt to emulate the original Enigma machine from the Second World War and be used to encode and decode messages. This document includes Project Scope, Work Breakdown Structure and Gantt-Chart.

2. Project Scope

2.1 Problem / opportunity

With Enigma Emulator it will be possible to to encrypt and decrypt messages including some of the original copied German messages.

2.2 Background

"An Enigma machine is any of a family of related electro-mechanical rotor cipher machines used for the encryption and decryption of secret messages. Enigma was invented by German engineer Arthur Scherbius at the end of World War I. The early models were used commercially from the early 1920s, and adopted by military and government services of several countries — most notably by Nazi Germany before and during World War II. Several different Enigma models were produced, but the German military models are the ones most commonly discussed.

In December 1932, the Polish Cipher Bureau first broke Germany's military Enigma ciphers. Five weeks before the outbreak of World War II, on 25 July 1939, in Warsaw, they presented their Enigma-decryption techniques and equipment to French and British military intelligence. Thanks to this, during the war, Allied codebreakers were able to decrypt a vast number of messages that had been enciphered using the Enigma. The intelligence gleaned from this source, codenamed "Ultra" by the British, was a substantial aid to the Allied war effort."[1]

2.3 Project name, supervisor and manager

Name – Enigma Emulator

Supervisor – Aoife Fox, Luke Raeside

Manager – Robert Biedron

2.4 Project goal

The research, planning and development of a software called Enigma Emulator.

2.5 Objectives

1. Research the original Enigma machine, how it worked.
2. Research how Enigma code was broken.
3. Perform a literary review of the project research.
4. Develop a project design and analysis document.
5. Build and test the project according to the chosen SDLC (Software Development Life Cycle).
6. Finalise program and submit.

2.6 Success criteria

1. The finished program should be able to encode messages in the same way as original Enigma machine.
2. The program should be able to decode original German messages from the Second World War.
3. The program User Interface should be "User Friendly".

2.7 Assumptions, risks and obstacles

The main assumptions associated with this project are;

- Access to a modern PC/laptop.
- Ability of project members to uderstand how Enigma machine worked.
- Ability of project members to understand how to decrypt Enigma's encryption.
- Ability of project members to implement Enigma's mechanism into Java code.

Possible risks and obstacles to the project include;

- An individual project could be too difficult for one person to acomplish.
- Feature creep and scope creep can delay the deployment of the finished software.

3. Methodology

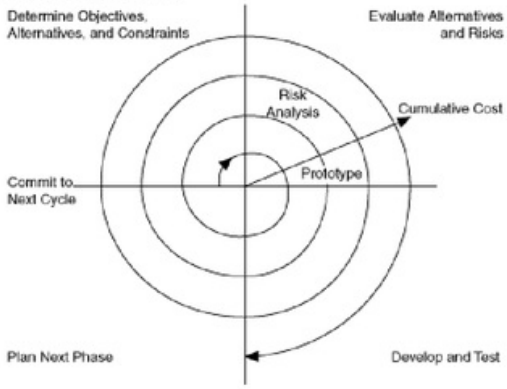
Software Development Life Cycle that suits best for this project is Spiral Model. The reason for this is because it provides a lot of teasting, wich lead to better final product.

Spiral model

The main feature of this model is to analyze the risks present in each loop (iteration). First task is an analysis of preliminary requirements. If the requirements seem to be feasible within a given time, budget and with the available resources, the project can go to the palnning stage and first iteration. Each iteration looks like small waterfall model, and after each one the full system is reviewed. If the project needs further work, then there is need to plan next iteration, and then conduct risk analisis for it. Spiral model is therefore an upgraded version of waterfall model with current risk analysis. This model can be viewed as cyclic repeating of four steps:

- Planning – based on requirements and objectives set by the customer.
- Risk analisis – evaluation of alternatives and attempts to identify and analize the risks associated with each of the possible design alternatives of the product.
- Construction – has a form of a "little waterfall", and aims to produce next edition of the software.
- Evaluation – validation of the product and its evaluation with the possibility of modifications.

The main advantage of the spiral model is an attempt to minimalize the risk of the project failure and continuous verification of the product by the user, which is to produce fully satisfactory software for the customer.



4. Work Breakdown Structure (WBS)

1. Complete project proposal.
2. Research original Enigma machine mechanism.
3. Research deryption techiques used to break the Enigma.
4. Perform literary review.
5. Risk analysis.
6. Development plan.
7. Build prototype.
8. Second risk analysis.

9. Validation and verification.
10. Operational prototype.
11. Validation and verification.
12. Final development.
13. Implementation.
14. Teasting and quality control.
15. Release.

5. Gantt chart

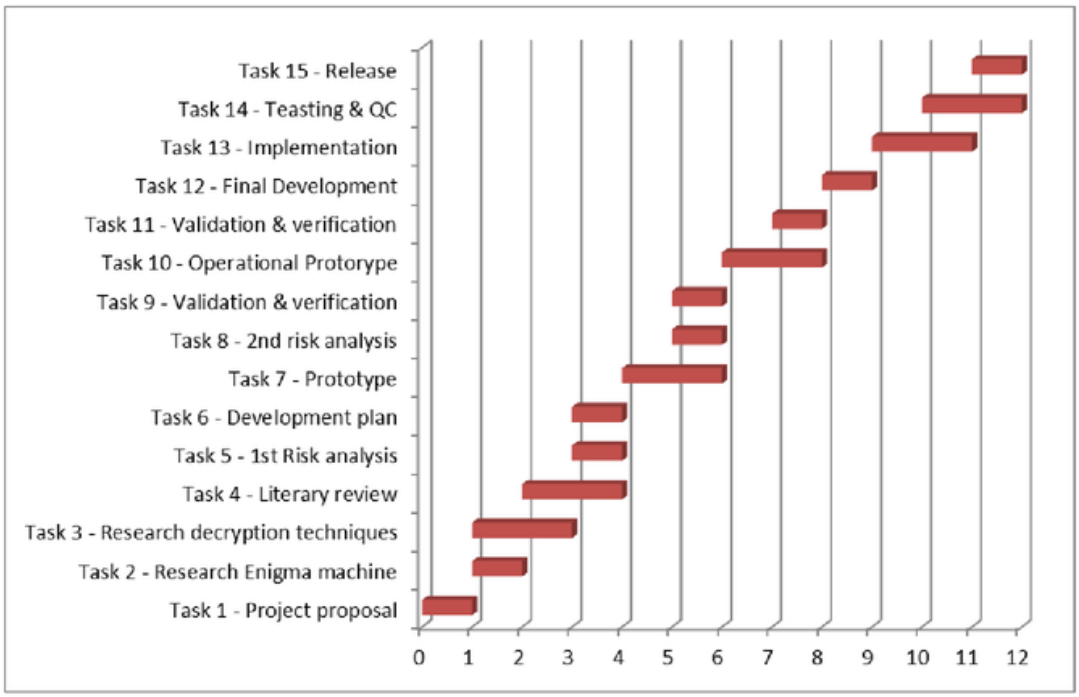


Figure 1 Gantt chart

6. Conclusion

This project is ready to start, some changes may occur later during new iterations. Next stage of the project is to research available resources. Finished project is scheduled for the end of the semester.

7. References

[1] – World Wide Web: Enigma Machine

http://en.wikipedia.org/wiki/Enigma_machine

GRADEMARK REPORT

FINAL GRADE
/ 10

GENERAL COMMENTS

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6