Enigma: Encryption & Decryption Methods

**October 2019**

**By**

**James Duncan**

**Student number 201709001**

**Word count: 2371**

Contents

[1. Project background and purpose 3](#_Toc22399309)

[1.1. Background 3](#_Toc22399310)

[1.2. Objectives 3](#_Toc22399311)

[Primary Objectives 3](#_Toc22399312)

[Secondary Objectives 3](#_Toc22399313)

[Tertiary Objectives 4](#_Toc22399314)

[1.3. Scope 4](#_Toc22399315)

[Encryption Methods 4](#_Toc22399316)

[Alan Turing & The World Wars 4](#_Toc22399317)

[1.4. Deliverables 4](#_Toc22399318)

[1.5. Constraints & Assumptions 5](#_Toc22399319)

[2. Project rationale and operation 6](#_Toc22399320)

[2.1. Project benefits 6](#_Toc22399321)

[2.2. Project operation 6](#_Toc22399322)

[2.3. Options 6](#_Toc22399323)

[Programming languages 6](#_Toc22399324)

[2.4. Risk analysis 7](#_Toc22399325)

[2.5. Resources required 10](#_Toc22399326)

[Project methodology and outcomes 11](#_Toc22399327)

[2.6. Initial project plan 11](#_Toc22399328)

[2.6.1. Tasks and milestones 11](#_Toc22399329)

[2.6.2. Schedule Gantt chart 11](#_Toc22399330)

[2.7. Project control 15](#_Toc22399331)

[3. Appendix a (Bibliography) 16](#_Toc22399332)

[4. Appendix b 17](#_Toc22399333)

[4.1. Determining Key Tasks 17](#_Toc22399334)

[4.2. Task Breakdown 18](#_Toc22399335)

[4.3. Gantt Chart Full 18](#_Toc22399336)

[4.4. Gantt Chart Compressed 20](#_Toc22399337)

# Project background and purpose

## Background

Computer Science is continuingly advancing and so is the need to protect user’s data particularly as we move towards the cloud as a service for large businesses. Losing customer data to Malicious hackers is one of the worst things that can happen to a company and we have seen the ramifications of what happens when a company is lacking in security. Facebook is one of the biggest examples of this as we saw with their connections to “Cambridge Analytica” (Kleinman, 2018) and their recent “admission to storing user passwords in plain text” (KrebsonSecurity, 2019) . You would think by 2019 we would have understood the need for keeping data safe however, this year we had “Collection 1” (Hunt, 2019) release which is the largest dump of emails and passwords in the History of the Internet

In World War 2 the Germans understood the need to keep all their communications secret and adopted the Enigma Machine to encode all their messages so that the allied forces could not understand the messages sent through Morse code. This was eventually broken by the British during the war and “many flaws in Enigma helped the British crack it” (Numberphile, 2013).

So why can’t modern businesses keep their user’s data safe? Is encryption hard to implement? Are there major flaws that make the encrypted text easy to decrypt? Or are hackers just finding ways round?

In this analysis the project will take a detailed look at the Enigma machine and compare it to modern encryption methods whilst highlighting key advancements and weaknesses. The development and analysis will attempt to improve on the key weaknesses that the Enigma machine had in order to resemble that of the “Typex machine” (Computerphile, 2015).

This analysis will answer some of the above questions whilst at the same time gather a detailed understanding on different encryption and decryption methods used in the present by testing and studying modern encryption and historical encryption methods .

## Objectives

### Primary Objectives

The primary objectives for this project are as follows. Firstly, to create an Enigma machine and decoder (Similar to the Bombe) to aid in analysis of encryption methods and decryption methods. To research and build modern encryption methods to understand modern advancements, modern uses and ease of implementation in comparison to Enigma.

Once development is complete, there will be a deeper analysis of encryption methods and Enigma comparing them against each other. The comparison will be completed both practically using developed methods and theoretically underpinning the key the advancements made in the industry.

During the analysis, businesses will be recommend a method they should take to keep their data safe whilst answering the questions stated in the introduction and any relevant additional questions, including how may be able to understand and protect against “cryptographic attacks” (Herzog, 2019).

### Secondary Objectives

A machine with enhanced security was initially developed by the British. The “Typex used more rotors and fixed the issue where a character couldn’t be encrypted as itself” (Computerphile, 2015). This machine was used this to communicate with the Americans during the war.

If there is extra time, development will start to improve on the developed Enigma machine to make it like a Typex machine solving the key weakness and adding extra characters. This is possible and maybe easier on modern computers as the original machine used electrical current to encrypt the messages where as we now we have access to programming languages and much faster computers.

### Tertiary Objectives

To stick close to the history of the Enigma, building a “Morse code” (The British Museum, n.d.)translator would be a nice addition to the machine considering that this was the method used the Germans and the British to send the encrypted messages as the internet had not been invented yet.

## Scope

This project will contain developed Encryption and decryption methods like the Enigma and Bombe. This project will also contain a report with clear examples of how encryption methods have advanced in the industry, and how they can be used to helps businesses understand what they can actively do to prevent data breaches. This includes “other types of cryptographic attack designed to steal customer data” (Herzog, 2019).

By researching the Enigma machine there is a lot of data that will not be part of the analysis as stated below.

### Encryption Methods

In this project there will be a focus on modern encryption methods and the Enigma Machine and not on every single encryption method through history as some are completely irrelevant (Hieroglyphics) and some made little advancement to the previous version. Instead research will be focussed on looking at methods that we use today and methods such as Enigma that made advancements to the methods used.

### Alan Turing & The World Wars

Although reference to Alan Turing will be made in the full report/findings there will not be research into Alan’s personal life, however more focus will be put on how the Enigma was broken and his contributions to It. Similarly, although reference to the world wars will be made the focus will be on encryption used at the time.

## Deliverables

This project will deliver multiple coded encryption methods specifically the Enigma Machine and some select modern encryption techniques. There will also be a developed Bombe (Enigma decryption Machine) to showcase how the encryption was broken.

The report will deliver on a range of tested and developed methods in order to answer questions, underline technical advancements and make a recommendation on what businesses should be doing to protect user’s data.

This project will be successful if the coded methods and the analysis meets the primary objectives. Specifically, The Enigma Machine and Bombe must function, The analysis must come to a conclusion for to the stated questions whilst making a recommendation about what a business should do to protect their user’s data.

## Constraints & Assumptions

At one point a lot of the Enigma material was classified and some of this information could have been lost during the time. A lot of this information is now unclassified however, although unlikely there might be some that is still classified.

Fortunately, there is a lot of information on the Enigma machine including the museum at Bletchley Park, as a result the project will continue assuming that all the information has been already released allowing for analysis to progress.

# Project rationale and operation

## Project benefits

This project will benefit businesses, specifically start-ups that might not know what or how implement encryption and how they can keep their data safe. This is especially relevant in the environment we are in today where Cyber is becoming a major area of development with “cyber-attacks costing small companies and average of $200,000” (Steinberg, 2019).

Hopefully by researching encryption and decryption methods the report may suggest how a business can avoid encryption-based attacks such as ransomware. This form of attack is becoming an increasing large way that a malicious actor may try to exploit money out of their victims. When ransomware hits a business, it can be devastating as we saw with “WannaCry when the NHS was affected costing them £92 Million” (Field, 2018).

I personally will benefit from the project learning a lot about the Enigma machine, Encryption/Decryption methods and programming languages.

## Project operation

This project will mostly be using the iterative methodology for development where prototypes will be delivered at intervals in the development to adjust for any change that may be required. This allows focus to be on tasks and features based on what is important for the project completion.

Agile is not being used as it is more focused on the user and the interactions that a user might have in order to have a smoother experience. Since the development is only to assist with the analysis, having the development be focussed on user interaction/user stories may be a waste of time.

Prototypes will be used to develop to compare them against objectives to measure progress on the project achieving various milestones with each feature that is implemented. Once the objectives have been met it will be possible to assess that part of the project has been a success. During development Trello will be used to keep track of all independent tasks. This will act as a Kanban board allowing me to keep track of progress at each stage of development.

For more flexibility GitHub will be used as version control software allowing control of development with functions included such as being able to revert to previous versions when required.

## Options

### Programming languages

There is a wide range of different programming languages available to complete the development implementations in however for this project It would be beneficial to choose a web language as the internet is the area where most breaches happen in business.

That still leaves the project with a wide selection of different languages to consider including whether to complete the implementations using server-side code or Client-side code.

Evaluations of which language is the best to use will be on a case to case basis, for example here might not be any need for server-side connections for the Enigma machine so It could be coded in client-side languages such as JavaScript.

## Risk analysis

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Risk | Likelihood | Severity | Impact | Controls | Adjusted Likelihood | Adjusted Severity | Adjusted Impact |
| Corruption of Data | Medium (3) | High (4) | 12 | Store data on the cloud.  Have a backup | Very Low (1) | N/A | 4 |
| Project delay due to Illness (1 Week or less) | Medium (3) | Medium (3) | 9 | Keep a week available in planning to ensure recovery time | Low (2) | N/A | 6 |
| Project Delay due to illness (Greater than 1 Week) | Low (2) | High (4) | 8 | Keep healthy | Low (2) | N/A | 8 |
| Supervisor Leaving University | Very High (5) | High (4) | 20 | Schedule meetings with new Supervisor as soon as possible to keep up to date.  Schedule meetings with current supervisor and gain any knowledge he has before leaving the University  Accept the risk | Very high (5) | Low (2) | 10 |
| Repetitive Strain Injury | Low (2) | Medium (3) | 6 | Take Regular breaks | Very Low (1) | N/A | 3 |
| Sleep Deprivation | Low (2) | Medium (3) | 6 | Plan the project well  Ensure I sleep for a healthy amount of time and don’t stay up for too long | Very Low (1) | N/A | 3 |
| Looming Assignment Deadlines affect time allocated to Dissertation causing delays | High (4) | Medium (3) | 12 | Ensure I plan time for other assignments/Modules | Medium (3) | N/A | 9 |
| Encryption Methods Fails to correctly Encrypt data | Medium (3) | Medium (3) | 9 | Test a set of data through development of the methods to test encryption | Very Low (1) | N/A | 3 |
| Possibility of learning a new language causes delay | Medium (3) | Medium (3) | 9 | Use a language similar to languages I already know. | Medium (3) | Low (2) | 6 |
| Scope changes by new emerging technologies causing delay | Low (2) | High (4) | 8 | Do some research into upcoming products.  Consider not including in scope and continuing the project as normal | N/A | Medium (3) | 6 |

## Resources required

This project requires access to standard resources such as a computer to code and research on and a stable internet connection to research with. If unable to access a computer or a stable internet connection this may lead to delay in the project fortunately, both a stable connection and computers are available at the University.

No non-standard resources will be needed for this project however, the project will be using a set of open source programs (IDE’s etc..) to code the project in.

There may be a requirement to execute server-side code at some point during development meaning access to a server may be required to run the program. This will probably require a localhost program like WAMP for PHP or a server. If a server is unavailable, development will change language and try to implement the program client side.

# Project methodology and outcomes

## Initial project plan

## Tasks and milestones

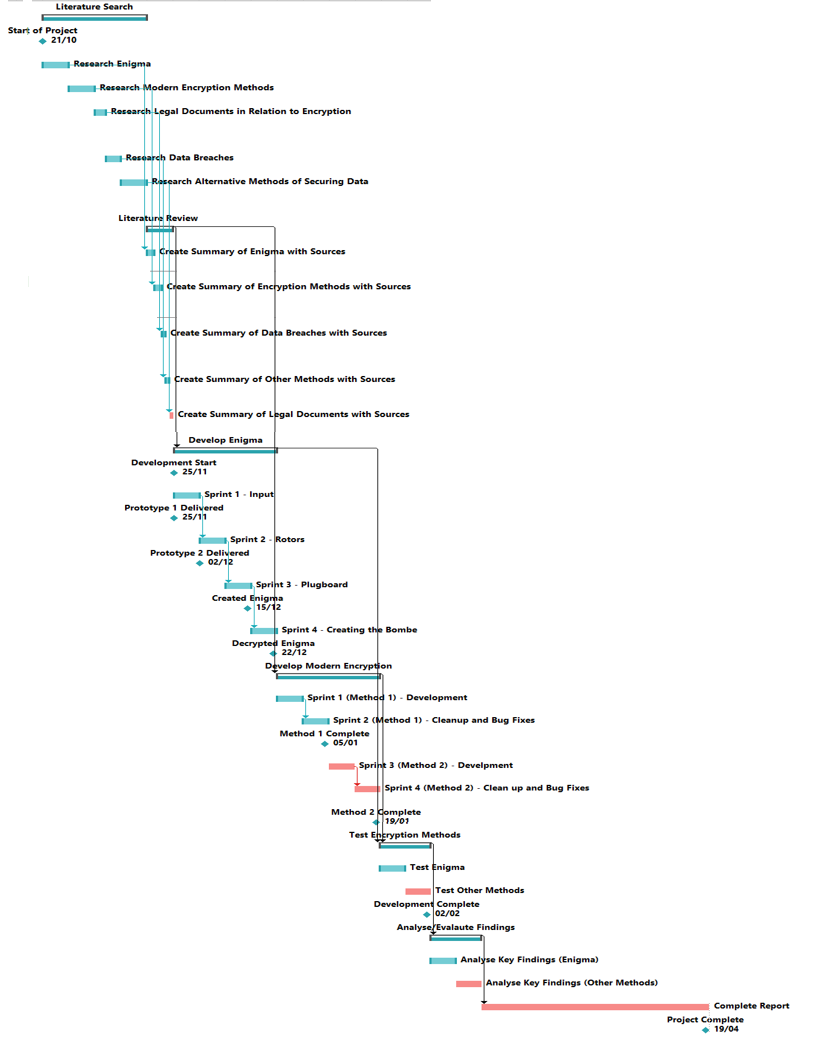
Below is a compressed task sheet that describes the biggest tasks in the project. The Gantt chart which can be found in 3.1.2 has further broken these tasks down.

26 Weeks (21/08/2019 – 23/04/2019)

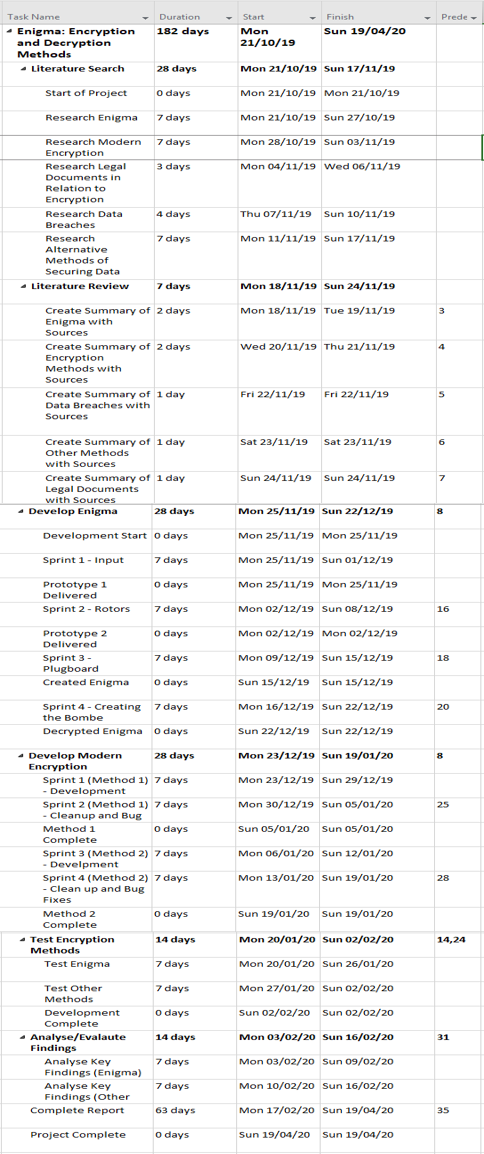
|  |  |  |
| --- | --- | --- |
| Task | Contents | Time for completion (Weeks) |
| Literature Search | Search for relevant books, Articles and sites about encryption methods gathering important information required for development of the project and future analysis. | 4 |
| Literature Review | Review the literature found and compile the important information. | 1 |
| Develop Enigma | Develop Enigma in chosen language. Broken down into developmental sprints and key tasks. | 4 |
| Develop Modern Encryption | Develop Modern Encryption in chosen languages and chosen methods. Progress measured by developmental milestones and key tasks. | 4 |
| Test Encryption Methods | Ensure all methods are correctly working fixing any bugs in the code. | 2 |
| Analyse/Evaluate Findings | Analyse my findings on encryptions against found literature and research. | 2 |
| Complete Report | Complete my analysis of encryption methods answering required questions and recommending how a business might be able to protect their data. | 9 |

## Schedule Gantt chart

This view of the Gantt chart shows each task broken down with milestones (represented by diamonds ) set at periods where a something important happens which helps to measure progress throughout the project. All tasks have their own completion time within the bounds of the simplified project plan found in 3.1.1. the compressed version of the Gantt chart can be found in appendix 5.4.

Any task in red means that it’s a critical task and if it was delayed at any point it could delay the entire project.

This Task breakdown shows when each part of the project is expected to start and finish along with its dependencies that a task requires to be completed in order to start. The project in total will take 182 days.

****

## Project control

The project will be monitored through the Gantt Chart where each task has a deadline. If each tasks deadline is met the project will be complete in time. If tasks finish early the project will be completed faster or allowing extra time to be spent on key tasks without delaying the project.

Development will be monitored through Trello where tasks will be tracked and managed. Progress with be measured through the release of new features and prototypes until the final version where the program is fully implemented.

Time will be set aside each day in order to work on the project and ensure movement towards completion. Development will be a success if all features are implemented without any bugs and the encryption works as required.

The project will be a success if the report/analysis underlines the key advancements made and the development of Enigma and other techniques clearly demonstrates how the encryption of data works.

# Appendix a (Bibliography)

Computerphile. (2015, January 7). *Enigma, TypeX and Dad - Computerphile*. Retrieved from Youtube: https://www.youtube.com/watch?v=jvKdOEHkrJc

Field, M. (2018, October 11). *WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled* . Retrieved from The Telegraph: https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/

Herzog, B. (2019, July 29). *Crytographic Attacks: A Guide for the Perplexed*. Retrieved from Check Point Research: https://research.checkpoint.com/cryptographic-attacks-a-guide-for-the-perplexed/

Hunt, T. (2019, January 17th). *The 773 Million Record Data Breach*. Retrieved from troyhunt: https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

Kleinman, Z. (2018, March 21). *Cambridge Analytica: The story so far*. Retrieved from BBC News: https://www.bbc.co.uk/news/technology-43465968

KrebsonSecurity. (2019, March 19). *Facebook Stored Hundreds of Millions of User Passwords in Plain Text for Years*. Retrieved from Krebsonsecurity: https://krebsonsecurity.com/2019/03/facebook-stored-hundreds-of-millions-of-user-passwords-in-plain-text-for-years/

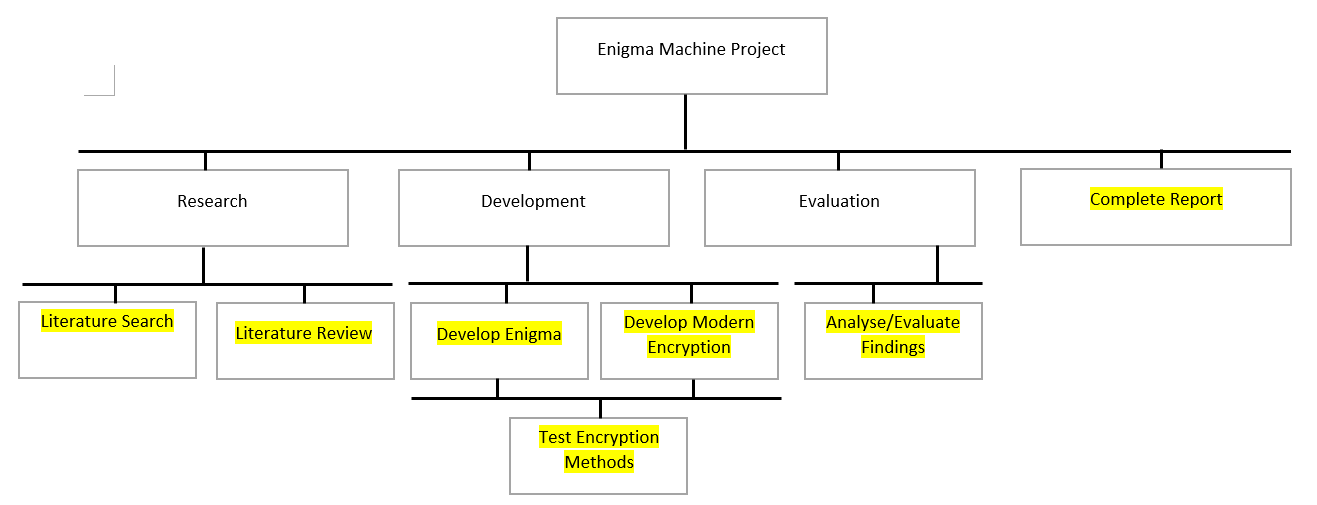
Numberphile. (2013, January 14). *Flaw in the Enigma Code - Numberphile*. Retrieved from Numberphile (Youtube) : https://www.youtube.com/watch?v=V4V2bpZlqx8

Steinberg, S. (2019, October 13). *Cyberattacks now cost small companies $200,000 on average, putting many out of business*. Retrieved from CNBC: https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html

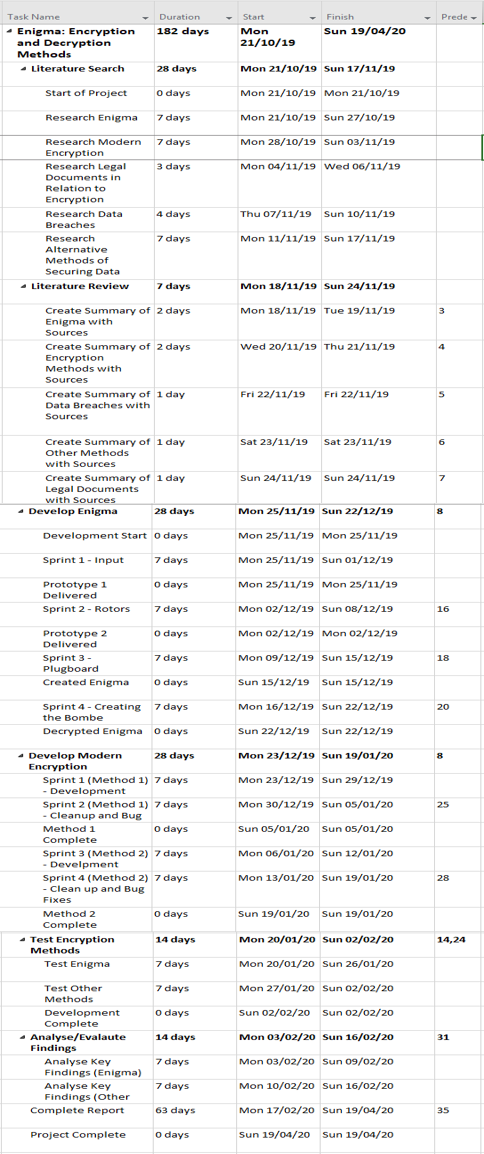
The British Museum. (n.d.). *Teaching History with 100 Objects: Enigma*. Retrieved from TeachingHistory: http://www.teachinghistory100.org/objects/about\_the\_object/enigma\_cipher\_machine

# Appendix b

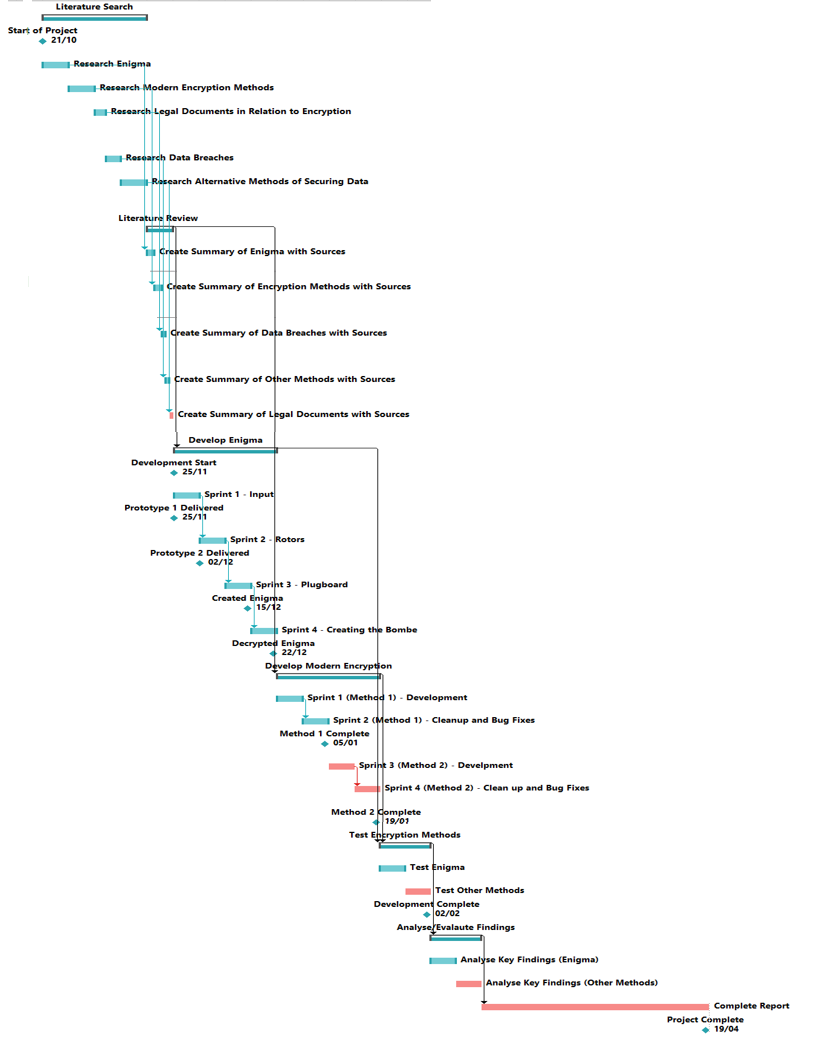
## Determining Key Tasks



## Task Breakdown

****

## Gantt Chart Full



## Gantt Chart Compressed

