Enigma Machine Simulator

Elliot Brooks

Supervisors:

April 2024

# Abstract

Contents

[1 Abstract 2](#_Toc158033956)

[2 Introduction 4](#_Toc158033957)

[2.1 Aims and Objectives 4](#_Toc158033958)

[3 History & Background 5](#_Toc158033959)

[3.1 History of the Machine 5](#_Toc158033960)

[3.2 Design of the Machine 5](#_Toc158033961)

[3.2.1 Keyboard & Lampboard 6](#_Toc158033962)

[3.2.2 Rotors 6](#_Toc158033963)

[3.2.3 Reflector 7](#_Toc158033964)

[3.2.4 Plugboard 7](#_Toc158033965)

[3.3 Enigma Machine and Abstraction 7](#_Toc158033966)

[3.3.1 Enigma’s Encryption 7](#_Toc158033967)

[3.3.2 Abstractions 8](#_Toc158033968)

[3.4 Design Flaws 11](#_Toc158033969)

[3.5 Possible Solutions 11](#_Toc158033970)

[3.6 Similar Products 11](#_Toc158033971)

[4 Design & Implementation 11](#_Toc158033972)

[4.1 Tools and Technologies 11](#_Toc158033973)

[4.2 Enigma Model Design 12](#_Toc158033974)

[4.2.1 Keyboard & Lamp board 12](#_Toc158033975)

[4.2.2 Reflector 12](#_Toc158033976)

[4.2.3 Rotors 12](#_Toc158033977)

[4.2.4 Enigma 12](#_Toc158033978)

[4.3 Design of the Application 12](#_Toc158033979)

[4.3.1 Command Line Interface 12](#_Toc158033980)

[4.3.2 GUI 12](#_Toc158033981)

[4.3.3 Visualization 12](#_Toc158033982)

[5 Results 12](#_Toc158033983)

[6 Evaluation 12](#_Toc158033984)

[6.1 Model Evaluations 12](#_Toc158033985)

[6.2 GUI Evaluation 12](#_Toc158033986)

[7 Conclusion 13](#_Toc158033987)

[8 References 13](#_Toc158033988)

[9 Table of Figures 13](#_Toc158033989)

[10 Tables of Tables 13](#_Toc158033990)

[11 Table of Equations 14](#_Toc158033991)

# Introduction

The Enigma Cypher Machine (*Enigma I)* is most well-known for its usage and eventual breaking, during World War 2 (WW2). The machine used several mechanical rotors, a reflect and a plugboard to redirect electrical signals, scrambling a plaintext message into cyphertext. Whilst most have heard of the machine, either from a study of cryptography or through history, many do not understand how the machine functions and its significance in cryptography. By creating a visual tool to demonstrate the inner workings of the Enigma, the aim of the project was to offer a deeper insight into the functionality, significance, but also the weaknesses of the machine.

There already exists a handful of examples of Enigma simulations which tend to offer a skeuomorphic approach to modelling the machine. The challenge I wanted to overcome was to create a tool that teaches the user how the machine functions logically. I began my project by thoroughly researching *Enigma I* to understand the inner workings of the machine and to compile this research into a simpler, abstracted model using Java. I created both a multi-platform command line interface (CLI) and a multi-platform graphical user interface (GUI) to allow the user to interact with the model, the former offering a step-by-step visualisation of the encryption of a message. To complete the project, I developed a second “Enhanced Enigma” model which aims to correct the two key cryptographic weaknesses of the machine. I identified the accuracy of my model by comparing with similar products as well as some real-world messages found amongst the German forces during WW2. I also identified the effectiveness of the two Enigma models by using some basic cryptoanalysis.

## Aims and Objectives

The following list adapted from the original project description, however there are some additional objectives I have included myself. For each task I set my own criteria to assess the success of each task’s implementation.

|  |  |
| --- | --- |
| Aim / Objective | Criteria for Success |
| Create a standalone package that simulates the Enigma Machine | The package should simulate only the Enigma machine and should be able to be used in different applications. It should also produce the correct output for a given input. The package should allow the Enigma Machine to be fully configurable as the ‘Enigma I’ |
| Create a new “Enhanced Enigma” machine with an aim of fixing cryptographic weaknesses | The enhanced machine should function similarly to the original Enigma and should be more secure cryptographically |
| Create a basic command line interface | The CLI should be allow full configuration of the machine and allow the user to enter a plaintext message |
| Create a GUI with a visualisation tool | The GUI should have the same capabilities, if not more than the CLI. In addition, it should aim to visually reflect the machine.  The visualisation tool should provide a simplified and informative representation of the encryption steps |
| Support multiple platforms | The application should be compatible with Windows/MacOS/Linux |

# History & Background

## History of the Machine

The Enigma cypher is one of the most famous cipher machines (Enigma n.d.) due to its role in WW2 and the work undertaken at Bletchley Park to crack the code. The Enigma was used extensively by the German forces to transmit coded messages for more secure communication. Whilst most people refer to this machine as “The Enigma”, Enigma is a brand name for a series of cypher machines (Enigma n.d.). The one used most in WW2 was *Enigma I* and was the key focus of this project.

To use the Enigma machine, it had to be configured to an exact setting so that the machine could be correctly decoded by the intended parties. These settings were distributed to the German forces each month in a code book, containing each day’s settings.

TODO : Add more history here

## Design of the Machine

The Enigma Machine was a rotor-based machine and worked with a hybrid of mechanics and electrical signals. *Enigma I* contained 5 key components that worked together to produce cyphertext which were: the keyboard and lampboard, the rotors, the reflector, and the plugboard. The inclusion of all these components aimed to make the machine as unpredictable as possible as well as generating a large key-length of roughly 67 bits (nearly 159 quintillion different settings see Equation 6) (van Manen and Robertsson 2016).

The use of the machine was a simple process. A user would receive a message along with a key denoting the choice of rotors and their respective settings, the plugboard settings and a reflector choice. Each time a key was pressed on the keyboard, a light on the lampboard would emit light as demonstrated in Owen’s animation (Owen 2021) and the user would write down the corresponding letter. Due to the symmetric design of the Enigma machine, as long as two people had the same settings then they could simply input the cyphertext into the machine and receive the plaintext and vice versa. However, this design choice was overlooked and compromised the Enigma’s security (See 3.4) (Thimbleby 2016).



Figure 1 A photo of Enigma I showing the plugboard, keyboard and lampboard. Only a small portion of the rotors are visible, and the reflector is hidden (Enigma n.d.).

### Keyboard & Lampboard

The keyboard and lampboard were the interface which the user could encode/decode messages. The former was comprised of the 26-letter alphabet omitting any special or numeric characters. Each key on the keyboard could be pressed which would cause a ratchet mechanism to move a lever (pawl) to step the rotors (Hamer 1997). The lampboard was a copy of the keyboard but instead of keys, there were small glass panels which would allow the bulbs underneath to shine through. These panels were also printed with the 26-letter alphabet and upon a keypress, any given lamp could light up to show the plaintext character’s corresponding cyphertext.

### Rotors

The rotors were the heart of the Enigma machine and were responsible for most of its unique properties. They were metal ratchet discs with 26 different positions representing each letter of the alphabet. Each position had a corresponding metal contact (Owen 2021) on both sides of the disk to allow electrical current to flow through the rotor. Inside the rotor, fixed wires were implemented which directed the current from one contact to another, encoding the input.

Rotors also exhibited another property; each rotor had a notch at a fixed position on the ratchet which would allow the levers (pawls) mentioned earlier to ‘step’ the rotor (Hamer 1997). This stepping caused the rotor to rotate by one position. In the machine, three rotors were placed in series to allow current to pass through all three, causing a letter to be scrambled 3 times from one key press. Once a rotor would reach its turnover position (the character shown to the user once the notch position is lined up to the pawl, the latter is not seen by the user of the machine), the rotor to left of the turnover rotor would be stepped as well. The right-most rotor would step every key press, the middle rotor would step with a period of 25 (Grime 2013) (Smart 2016) (one might expect 26, however due to a quirk of the machine known as double stepping, the middle rotor could step twice in a row). The left-most rotor would step with a period of 262. This rotational property of the machine allowed for the encoding for a given letter to change each keypress.

The Enigma rotors could be swapped around and placed in any order in the three slots available. Usually, users were given a box containing 5 different rotors (although later models had more and could place them in a choice of 4 slots), [CITE] the choice of which to use formed part of the Enigma’s key. Table 1 depicts the 5 rotors that were included with *Enigma I* demonstrating their internal wiring as well as the location of the notch. For example, rotor I will map A to E and B to K provided the rotor is in rest position (Position A and Ring setting A).

|  |  |  |  |
| --- | --- | --- | --- |
| Rotor | Encoding (Position A - Ring setting A) ABCDEFGHIJKLMNOPQRSTUVWXYZ | Notch | Turnover |
| I | EKMFLGDQVZNTOWYHXUSPAIBRCJ | Y | Q |
| II | AJDKSIRUXBLHWTMCQGZNPYFVOE | M | E |
| III | BDFHJLCPRTXVZNYEIWGAKMUSQO | D | V |
| IV | ESOVPZJAYQUIRHXLNFTGKDCMWB | R | J |
| V | VZBRGITYUPSDNHLXAWMJQOFECK | H | Z |

Table 1 "Enigma I" rotor encodings (Enigma wiring n.d.)

Finally, the rotors had an additional setting known as the ring setting. This allowed the internal wires and ratchet to be shifted independently from the letter ring. This allowed the notch position to move relative to the letter ring. Whilst generally, the ring setting formed part of the key, it is important to note that the effect of the ring setting did not contribute much to the strength of the cypher [CITE].

Much of the complexity of the Enigma was due to these rotors. Alone, with an *Enigma I* model, there were 1054560 different ways to configure the rotors (See Equation 1)

Equation 1 Permutations for rotors (excluding ring setting)

### Reflector

The reflector was a similar component to that of the rotors and together formed the subsystem that does most of the scrambling. The main differences regarding the reflector are that it does not rotate, and the current does not pass through but rather is ‘reflected’, travelling back in the opposite direction. This reflection allows the reflector to act as a similar substitution cypher akin to the rotors.

The design of the reflector was to enable whole machine to be reciprocal, combining encryption and decryption into one operation. This, along with the fact that the reflector could not encode a letter to itself (the design of the rotor prevented the current being passed back through the same metal contact) were crucial flaws exploited (Thimbleby 2016) by the team at Bletchley Park to crack the code during WW2.

The Enigma machine came with a reflector which could be replaced with another but generally remained the same. The three that were available with the *Enigma I* were UKW-A, UKW-B and UKW-C as shown in Table 2. The encodings demonstrate the inner wiring of each reflector, for example UKW-A maps A to the letter E as they have matching indexes.

|  |  |
| --- | --- |
| Reflector | Encoding ABCDEFGHIJKLMNOPQRSTUVWXYZ |
| UKW-A | EJMZALYXVBWFCRQUONTSPIKHGD |
| UKW-B | YRUHQSLDPXNGOKMIEBFZCWVJAT |
| UKW-C | FVPJIAOYEDRZXWGCTKUQSBNMHL |

Table 2 "Enigma I" reflector encodings (Enigma wiring n.d.)

### Plugboard

The plugboard formed the final part of the Enigma’s encryption key and was located at the front of the machine. It displayed another representation of the 26-letter alphabet, each of which had a plug socket. These sockets, and the cables that came with the machine allowed two letters to be connected to each other on the plugboard. This created yet another scrambling of the letter, such that if socket A and socket E were connected then any current passing through the plugboard in wire A, would be directed to wire E and vice versa. Any letter left unconnected to another would result in the plugboard having no effect. The plugboards letter swapping effect only occurred twice in each encryption, once at the start of the encryption (after the keypress) and once at the end (before the lamp on the lampboard lights up).



Figure 2 A front-facing photo of the Enigma I plugboard with cables in place (Enigma n.d.)

## Enigma Machine and Abstraction

### Enigma’s Encryption

Often the best way to understand the mechanisms of the machine is to focus on a single letter’s encryption. As mentioned in 3.2, the user begins with defining the machine’s key. Upon a keypress on the keyboard, the first notable event is that the rightmost rotor will rotate. Depending on the current rotation, the other rotors may also rotate but only ever by one position. Once this step is completed, an electrical signal will be induced passing through the plugboard towards the rotors. Depending on the plugboard settings, this input signal may be scrambled. This electrical signal then passes through rotors right-to-left with the signal being redirected at each rotor. The output of the three rotor redirections is then transmitted to the reflector where the signal’s direction is reversed and redirected to a different letter’s contact. The signal then passes through all three rotors for a final time, this time from left-to-right, before passing through the plugboard again. Finally, the signal is transmitted to the lampboard where the cyphertext is displayed. Any plaintext letter can be scrambled up to nine times before the cyphertext is displayed.

By representing each of the components of the Enigma as a transformation as demonstrated by Rejewski (Rejewski 1980), such that represents the plugboard, represents the rotor in the left, middle or right position and represents the reflector, an equation, such as Equation 2, can be formulated to describe Enigma’s encryption steps. It is important to note that due to the plugboard’s symmetry, .

Equation 2 The encryption steps of Enigma I

### Abstractions

The Enigma machine is a complex machine. With numerous components working together in both mechanical and electrical forms, it can prove difficult to predict the outcome of an encryption. This section aims to abstract each component into a logical model to help demonstrate the behaviour and weaknesses of the machine. The diagrams provided are inspired by work from Smart (Smart 2016) and Thimbleby (Thimbleby 2016).

The plugboard acts as a simple cypher, which aims to swap two letters. This means that letters connected by a cable on the physical machine are encoded to each other; in absence of a cable, no letter scrambling takes place. As shown in Figure 3, sockets on the machine that connected are represented with a connection between nodes such as A and D. Due to the plugboard symmetry, these such diagrams exhibit this ‘X’ shapes.

A diagram of lines and dots

Description automatically generated

Figure 3 A wiring diagram to show a plugboards potential encoding

The reflector acts as a substitution cypher with additional constraints being self-coding and reciprocal coding (See Equation 3). Like other components this can be represented using a wiring diagram such as Figure 4 which demonstrates an example of a reflector. In the diagram, A is shown to be connected to F and vice versa such that any input into the reflector will output the letter at the connected node.

TODO : Check this function

Equation 3 An equation and additional constraints to describe the behaviour of an Enigma Reflector

A diagram of a diagram

Description automatically generated

Figure 4 A wiring diagram to show a potential encoding for a reflector

The rotors of the machine are substitution cyphers with no additional constraints. They take an input letter and produce either the same or a different letter. A rotor can be represented using a wiring diagram, however multiple diagrams are needed to convey the rotor’s rotational effects. As demonstrated in Figure 5, the image on the right depicts the same rotor displayed on the left but with a rotation of one. This leads to the connections between nodes to move upwards whereas the ring setting will cause them to move downwards. This effect is easily seen with the horizontal connection between F. Once the rotor is rotated the same connection is moved upwards in the diagram to become a horizontal connection between E. This effect can be generalised such that any input letter will be mapped to the input letter . In addition, the output of the letter will be shifted by (See Equation 4). It is clear from these generalisations that if the rotation setting was ten and the ring setting was 10, then there would be no effect on a letter’s encryption as mentioned in 3.2.2.

TODO : Check this function, is it well defined? Define map(x)?

Equation 4 A function to represent the encoding behaviour of the rotor where x and x` are letters, represents the rotor’s rotation and represents the ring setting. The map function returns the input letter’s mapping as if no rotational effects have taken place e.g. in Figure 5,

A diagram of lines and dots

Description automatically generatedA diagram of lines and dots

Description automatically generated

Figure 5 Two wiring diagrams to show a potential rotor encoding. The diagram on the right shows the same rotor as on the left, but with a rotation of one

By abstracting all the electrical and mechanical features of the machine, logical diagrams demonstrating the letter scrambling that takes place in the Enigma machine can be created with more ease. The diagrams from Figures 3-5 represent each component of the machine and can be combined to create a representation of the entire Enigma machine (See Figures 6-7). These diagrams depict an Enigma machine and demonstrate how the machine works in full. It is important to note that these diagrams only show a single state, upon each key press the rotor wirings will change leading to a potentially different output for the same input.

A diagram of a network

Description automatically generated

Figure 6 A wiring diagram representing a single state of an Enigma I machine. Input is received on the right-hand side before being scrambled by components performing a loop. The electrical signal received back from the plugboard represents the encoded letter. The names of each rotor/reflector do not match the encodings but are given as an example.

A diagram of a network

Description automatically generated

Figure 7 An example of an encryption/decryption taking place in an Enigma I machine. In this case A is encoded to C.

## Design Flaws

At a first glance, it may seem like the Enigma machine is unbreakable and indeed the Germans shared this over-confidence (Thimbleby 2016). The Germans were lazy when operating the machine often opting to use the same 3 rotors and neglecting to use more than one reflector (Tang, Lee and Russo 2018). This led to a to a large reduction in the security of communication amongst the Germans due to factors that could have been largely avoided (Thimbleby 2016).

Whilst the Enigma machine had a large key space (see Equation 6), it is not the only factor that contributes to a cypher’s strength (How does the Enigma machine work? n.d.). In fact, work from Tang, Lee and Russo (Tang, Lee and Russo 2018) suggests that the Enigma had a theoretical key space of . As suggested by Thimbleby (Thimbleby 2016), by imagining the Enigma machine without its internal components, it can be viewed a substitution cypher with different mappings from keyboard to lamp board. However, this assumes that there are no restrictions with how the mappings can be wired. As mentioned earlier in 3.2, this was not the case for *Enigma I*. The actual number of permutations for the Enigma machine was (See Equation 5). The reduction in permutations by a factor of roughly is due to two features of the machine being self-coding and reciprocal coding (see Equation 3) (Ostwald 2023) (Thimbleby 2016).

Equation 5 Definition of double factorial [CITE]

Equation 6 The number of settings (key space) of Enigma I assuming 10 plugboard cables are used. Ring setting is omitted as it was not changed by the Germans. Based on work from Tang, Lee and Russo (Tang, Lee and Russo 2018).

## Possible Solutions

## Similar Products

A section to show the other types of enigma simulators that can be found on the internet which form the inspiration for my project. Explain how I would like to take this further.

# Design & Implementation

## Tools and Technologies

Description and list of tools used within this project.

* Java to create the application and the model.
* JavaFX – graphics package used to create the GUI + Visualizations.
* GitHub – version control and development tasks
* Maven – build project across multiple platforms.
* XML – Custom component definitions
* Gluon Scene Builder – Used for UI building and FXML creation.

## Enigma Model Design

Talk about the idea of the package, this would be a good place for UML diagrams and a description of how this model is going to work.

### Keyboard & Lamp board

Explanation of how this part does not really need to be modelled, and instead can be represented as input and output.

### Reflector

Description of how this will be modelled.

### Rotors

Description of how this will be modelled.

### Enigma

Description of how this will be modelled.

## Design of the Application

Explain how the application will work, show diagrams in order to show how the interfaces will interact with the model.

### Command Line Interface

A fairly short section, just explain how the interface works and what information will be shown.

### GUI

Larger section explaining the various design stages of the GUI, as well as explaining the MVC implementation. Important to talk about design choices in this section as this is the bulk of the project.

### Visualization

A second part to the GUI, explain the design choices and implementation as well as a section “interpreting the diagram.”

# Results

# Evaluation

## Model Evaluations

* Test Coverage
* Actual German messages
* Permutations compared with improved model.

## GUI Evaluation

* Usability
* Cross-platform

# Conclusion

# References

n.d. “Enigma.” *Crypto Museum.* Accessed 2024. https://www.cryptomuseum.com/crypto/enigma/.

n.d. “Enigma wiring.” *Crypto Museum.* Accessed 2024. https://www.cryptomuseum.com/crypto/enigma/wiring.htm.

Grime, J. 2013. “Maths from the talk "Alan Turing and the Enigma Machine".”

Hamer, David H. 1997. “Enigma: Actions involved in the ‘double stepping’of the middle rotor.” *Cryptologia 21, no. 1* 47-50.

n.d. “How does the Enigma machine work?” *Crypto Museum.* Accessed 2024. https://www.cryptomuseum.com/crypto/enigma/working.htm.

Ostwald, Olaf. 2023. “Cryptographic design flaws of early Enigma.”

Owen, Jaren. 2021. “How did the Enigma Machine work?” *Youtube.*

Rejewski, Marian. 1980. “An application of the theory of permutations in breaking the Enigma cipher.” *Applicationes Mathematicae. 16, No. 4,* 543-559.

Smart, Nigel P. 2016. “The enigma machine.” *Cryptography Made Simple* 133-161.

Tang, Lynda, Nayoung Lee, and Sophie Russo. 2018. “Breaking Enigma.”

Thimbleby, Harold. 2016. “Human factors and missed solutions to Enigma design weaknesses.” *Cryptologia 40, no. 2* 177-202.

van Manen, Dirk Jan, and Johan O.A. Robertsson. 2016. “Codes and ciphers.” *Part I: Decoding nature’s disorder: GeoExpro 13* 38-41.

# Table of Figures

[Figure 1 A photo of Enigma I showing the plugboard, keyboard and lampboard. Only a small portion of the rotors are visible, and the reflector is hidden (Enigma n.d.). 5](#_Toc158033854)

[Figure 2 A front-facing photo of the Enigma I plugboard with cables in place (Enigma n.d.) 7](#_Toc158033855)

[Figure 3 Wiring diagram to show a plugboard's potential encoding for a reduced alphabet size e.g. A encodes to D and vice versa. Notice the plugboard wiring diagrams tend to create X shapes. 8](#_Toc158033856)

[Figure 4 Wiring diagram to show an example reflector encoding for a reduced alphabet size e.g. A encodes to F and vice versa. 9](#_Toc158033857)

[Figure 5 Two Wiring diagrams to show an example rotor encoding. The diagram on the right shows the same rotor as on the left, but with a rotation of one. The left diagram shows F encoded to F and the diagram on the right shows E encoded to E. The “wire” is still the same, but the rotation of the rotor will lead to an F input/output, interpreted as E input/output. 10](#_Toc158033858)

[Figure 6 A wiring diagram representing a single state of an Enigma I machine. Input is received on the right-hand side before being scrambled by components in the following order: plugboard, rotor III, rotor II, rotor I, reflector UKW-B, rotor I, rotor II, rotor III, plugboard. The electrical signal received back from the plugboard represents the encoded letter. The names of each rotor/reflector do not match the encodings but are given as an example. 11](#_Toc158033859)

[Figure 7 An example of an encryption/decryption taking place in an Enigma I machine. In this case A is encoded to C. 11](#_Toc158033860)

# Tables of Tables

[Table 1 "Enigma I" rotor encodings (Enigma wiring n.d.) 6](#_Toc158033861)

[Table 2 "Enigma I" reflector encodings (Enigma wiring n.d.) 7](#_Toc158033862)

# Table of Equations

[Equation 1 Permutations for rotors (excluding ring setting) 7](#_Toc158213184)

[Equation 2 The encryption steps of Enigma I 9](#_Toc158213185)

[Equation 3 An equation and additional constraints to describe the behaviour of an Enigma Reflector 10](#_Toc158213186)

[Equation 4 A function to represent the encoding behaviour of the rotor where x and x` are letters, represents the rotor’s rotation and represents the ring setting. The map function returns the input letter’s mapping as if no rotational effects have taken place e.g. in Figure 5, 11](#_Toc158213187)

[Equation 5 Definition of double factorial [CITE] 13](#_Toc158213188)

[Equation 6 The number of settings (key space) of Enigma I assuming 10 plugboard cables are used. Ring setting is omitted as it was not changed by the Germans. Based on work from Tang, Lee and Russo (Tang, Lee and Russo 2018). 13](#_Toc158213189)