Enigma Machine Simulator

Elliot Brooks

Supervisors:

April 2024

# Abstract

Contents

[1 Abstract 2](#_Toc160610271)

[2 Introduction 5](#_Toc160610272)

[2.1 Aims and Objectives 5](#_Toc160610273)

[3 History & Background 6](#_Toc160610274)

[3.1 History of the Machine 6](#_Toc160610275)

[3.2 Design of the Machine 6](#_Toc160610276)

[3.2.1 Keyboard & Lampboard 6](#_Toc160610277)

[3.2.2 Rotors 7](#_Toc160610278)

[3.2.3 Reflector 7](#_Toc160610279)

[3.2.4 Plugboard 8](#_Toc160610280)

[3.3 Enigma Machine and Abstraction 8](#_Toc160610281)

[3.3.1 Enigma’s Encryption 8](#_Toc160610282)

[3.3.2 Abstractions 9](#_Toc160610283)

[3.4 Design Flaws & Remedies 12](#_Toc160610284)

[3.4.1 Cypher Strength 12](#_Toc160610285)

[3.4.2 Improving the Machine 12](#_Toc160610286)

[3.5 Related work 13](#_Toc160610287)

[4 Design & Implementation 15](#_Toc160610288)

[4.1 Tools and Technologies 15](#_Toc160610289)

[4.2 Enigma Model Design 15](#_Toc160610290)

[4.2.1 Keyboard & Lamp board 16](#_Toc160610291)

[4.2.2 Reflector 16](#_Toc160610292)

[4.2.3 Plugboard 17](#_Toc160610293)

[4.2.4 Rotors 17](#_Toc160610294)

[4.2.5 Enigma 19](#_Toc160610295)

[4.2.6 EnigmaPlus 20](#_Toc160610296)

[4.2.7 Additional Features 21](#_Toc160610297)

[4.3 Design of the Applications 21](#_Toc160610298)

[4.3.1 Command Line Interface 23](#_Toc160610299)

[4.3.2 GUI 24](#_Toc160610300)

[4.3.3 Visualization 24](#_Toc160610301)

[5 Results 24](#_Toc160610302)

[6 Evaluation 24](#_Toc160610303)

[6.1 Model Evaluations 24](#_Toc160610304)

[6.2 GUI Evaluation 24](#_Toc160610305)

[7 Conclusion 24](#_Toc160610306)

[8 References 24](#_Toc160610307)

[9 Table of Figures 25](#_Toc160610308)

[10 Tables of Tables 25](#_Toc160610309)

[11 Table of Equations 25](#_Toc160610310)

[12 Table of Code Blocks 26](#_Toc160610311)

# 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 “EnimgaPlus” 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 *Enigma I* | 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 “EnigmaPlus” machine with an aim of fixing cryptographic weaknesses of *Enigma I* | The “EnigmaPlus” 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.

## 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).

An old machine on a glass table

Description automatically generated

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. Photo taken by author at Science Museum London (Science Museum 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, thereby 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 reached 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 and the middle rotor would step with a period of 25 (Grime 2013) (Smart 2016) due to a quirk of the machine known as double stepping, where the middle rotor would also step when it reached its own turnover position as demonstrated by Hamer (Hamer 1997). 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 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, allowing 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 it had marginal impact on the strength of the cypher, only affecting the turnover position of the adjacent rotor (How does the Enigma machine work? n.d.).

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 the 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 others 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 for that letter. 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 the contact of a different letter. 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 complex. 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.

Firstly, The diagrams provided (Figures 3-7) are inspired by work from Smart (Smart 2016) and Thimbleby (Thimbleby 2016) and depict rectangles with nodes on each side to represent each letter in a truncated alphabet (A-F). The connections between these nodes represent the internal wiring of each component or, in a more logical sense, the letter-to-letter mappings of each component. These diagrams are designed such that the any letter is **input on the right** and the **output on the left** is map(x). Consequently, the left can also represent and the right-hand side represents . For example, Figure 3 shows the plugboard in which if the input on the right is “A” then the output will be map(“A”) which is “D”. The reason for representing input on the right-hand side is to better reflect the physical layout of the Enigma machine. It is important to note that, in the case of rotors, the function refers to the component with no rotational effects.

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 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.

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 causes 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 on the left image. Once the rotor is rotated the same connection is moved upwards in the diagram to become a horizontal connection between E as shown by the image on the right. 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 ten, then there would be no effect on a letter’s encryption as mentioned in 3.2.2.

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

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 greater 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 & Remedies

### Cypher Strength

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 became complacent when operating the machine often opting to use the same 3 rotors and neglecting to change the reflector (Tang, Lee and Russo 2018). This led to a to a large reduction in the security of communication between operators by 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 on how the mappings can be configured. 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 approximately is due to two features of the machine: self-coding and reciprocal coding (see Equation 3) (Ostwald 2023) (Thimbleby 2016).

Equation 5 Definition of double factorial

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).

### Improving the Machine

Clearly, the most obvious solution to improve the *Enigma I* is to increase its key space with more rotors. This can be done by adding an additional slot to the machine to allow for 4 or more rotors to be in use at any one time, or even using the usual 3 rotor slots but having a larger collection to choose from. In fact, rotor IV and V were introduced later in 1932 (Ostwald 2023) in order to increase the key space. Other machines inspired by Enigma, such as the British Typex, were developed to utilise more than 3 rotors at a time, thus increasing combinatorial complexity (Ostwald 2023). Ostwald’s study (Ostwald 2023) shows numerous additional improvements that either were implemented or could have been implemented to improve the cypher key space.

Thimbleby (Thimbleby 2016) gives examples of multiple circuits that aimed to fix the Enigma’s two main weaknesses mentioned in 3.4.1 demonstrating that the technology at the time period was capable of creating a much stronger cypher. In particular, Figure 8 demonstrates a circuit that only uses 3 rotors omitting both the reflector and the plugboard. By removing these two components, it avoids both self-coding and reciprocal coding by separating encoding and decoding into two distinct functions. For encoding, the current would pass from right to left, and vice versa for decoding. Whilst this model does not include the plugboard, so long as it is only applied once in an encryption, it can still be included so that both weaknesses are avoided. The removal of the reflector does reduce the key space however, this can be mitigated by simply adding another rotor.

A diagram of a machine

Description automatically generated

Figure 8 A circuit showing an Enigma style machine avoiding both self-coding and reciprocal coding. Taken from Figure 6 (Thimbleby 2016)

The design in Figure 8 mainly focusses on the electrical behaviour of the hypothetical machine however it acted as the main inspiration for “EnigmaPlus”. By representing this circuit as a wiring diagram similar to Figures 6-7, a logical model for this machine can be inferred as shown in Figure 9.



Figure 9 A wiring diagram depicting "EnigmaPlus". Note that there is no reflector as well as encoding and decoding take place in opposing directions.

## Related work

Before conducting the research to this product, several similar products were found that simulated the Enigma machine. This project and much of the work done around *Enigma I*were inspired by these products. In addition to this, the paper written by Thimbleby (Thimbleby 2016) gave direct inspiration into the creation of “EnigmaPlus”.

“Enigma Machine Emulator” (Enigma Machine Emulator n.d.) is a webpage consisting of a short description about the Enigma machine as well as offering an interactive emulator for the Enigma machine. The emulator follows a skeuomorphic design aiming to present a flat image that resembles the real machine.

“The Enigma Machine” (Enigma Machine n.d.) presents a sleeker UI allowing the user to configure the machine as well as encode/decode their messages. The design of this webpage strays from the original look and feel of the machine, offering a new and simpler way to interact with it. Much of the design points for my project were inspired by this page.

“Virtual Enigma” (Virtual Enigma n.d.) offers extremely interactive 3D simulation of the Enigma machine. This simulation allows full control of the machine down to each minute detail. Users can open different parts of the machine with their mouse and drag and drop rotors into place on a virtual model of the machine. The level of detail in this simulation offers an authentic experience for the user and is highly recommended for those who would like to experience the machine as a whole.

“The Enigma Machine” (MacWright n.d.) is the only similar product that I came across that offers a form of visualization to the inner workings of the machine. It represents the Enigma’s encodings as a circular wiring diagram analogous to Figures 3-7. This particular page was the inspiration for the visualiser functionality for this project.

# Design & Implementation

The key goal of this project was to create an exact simulation of the Enigma machine and provide both a command line interface and a graphical user interface to interact with it, focussing on educating the user on the machine’s functionality. Also, an additional model named EnigmaPlus was to be developed maintaining compatibility with the GUI and CLI as well as providing a stronger cypher than the original machine. Figure 10 provides an overview of the underlying system developed throughout this project. The subsequent sections provide a detailed account of each package; however, an overview will be given in this section.

A diagram of a computer

Description automatically generated

Figure 10 A diagram depicting the underlying system of this project

The Enigma package contains all the necessary backend functionality to accurately model and simulate the Enigma machine and EnigmaPlus. These models are designed to reflect the real-world machines (or hypothetical machine for EnigmaPlus), encrypting any plaintext message into cyphertext and vice versa. In addition, the package also provides pre-built rotor and reflector configurations to the Parsers package. The Parsers package and Config package both aim to provide custom component creation for both the CLI and GUI. They also provide a means of configuring the Enigma machine exclusively for the CLI. The CLI package contains a small demo application allowing the user to quickly configure and operate the model of the Enigma machine. Independently, the GUI package provides the user with a Model-View-Controller (MVC) based graphical application allowing the user to configure and operate the machine. In addition, the GUI provides numerous additional tools aimed towards providing an informative representation of the encryption process.

## Tools & Technology

TODO : Give description of all tools and technologies used in this project, focus more on existing packages such as JavaFX. Justify Choices

## Enigma and EnigmaPlus

### Enigma

After conducting research on the Enigma machine, which is explained in the previous chapter, it was clear that the most elegant solution to simulating the machine was by adopting object-oriented programming. By doing so, each class can reflect the core definition of each physical component therefore creating an accurate encryption process. Consequently, the Enigma package was created, and its UML diagram is demonstrated within Figure 11. This diagram does not include EnigmaPlus, as this was an additional requirement that was accommodated much later in the development process. The diagram shows the classes for each component of the Enigma which hold a composite relationship with the Enigma class, such that it cannot exist without these components. Interestingly, the UML diagram does not include any mention of the keyboard or lampboard that were covered in the background section. This is because whilst they were significant components for the physical machine, in a logical sense, they are nothing more than input and output.

A diagram of a computer program

Description automatically generated

Figure 11 UML diagram depicting the Enigma package, omitting EnigmaPlus

The majority of the components within enigma are some form of substitution cypher therefore a common representation was needed to represent this. At first, it was thought the best way to represent the substitution cypher encodings would be with the use of hash-maps. Whilst this representation would have worked, there would have needed to be 52 key-value pairs in the hash-map to represent this. In addition, hash-maps would have brought unnecessary complexity into the representation. Therefore, it was decided that a simple array for each component depicted as wiring, of length 26 integers, would be used for the representation. In such an array, each index represents the positional encoding of a letter and the value at that index would represent the positional encoding of the paired letter. This method offers much more simplicity as well as maintaining fast index speeds such as the hash-map, a process that will be abundant in an encryption. For most of the components, this representation was enough, however the rotor required a more complex representation requiring a representation for its inverse wiring, rotation, turnover position and ring setting. Therefore, the Rotor class exhibits additional attributes: reverseWiring, currentRotation, turnoverPosition and ringSetting to represent these.

In addition to the components and the machine, the Enigma package contains two factory classes. These were implemented to encapsulate all rotor and reflector creation. This includes creation of pre-set components as shown in Table 1 and Table 2 which were hard coded into these factory classes, as well as creation of custom components. By encapsulating this functionality, it also allows for a clean and concise method for checking additional constraints on the component’s encodings. This is especially important for the reflector which, as previously mentioned in section 3.2.3, cannot contain self-coding and must abide by reciprocal coding.

With the representation of each component complete, the core Enigma model could be created. The attributes for this model are a list of rotors, a plugboard and a reflector. This properly reflects the components of the physical machine. In order to accurately recreate the encryption process, two key functions were developed, encode and rotate. The former takes a plaintext character as input and returns a cyphertext character as output whilst following the encryption steps formulated previously in Equation 2. This function only encodes one character; however, this can be simply extended using iteration. A flowchart depicting the developed encryption process can be seen in Figure 12. The flowchart shows a call to the rotate function which is presented as pseudocode in Code Block 1, before subsequently calling each components encode function (scrambling the letter) in the following order: plugboard, right rotor, middle rotor, left rotor, reflector, left rotor, middle rotor, right rotor, plugboard.

A diagram of a character

Description automatically generated

Figure 12 A flowchart depicting the Enigma models encryption/decryption steps

FUNCTION rotate() {

doubleStepped = false

// The rare case of double stepping (the left and middle rotor rotate when the middle is at a turnover)

IF (rotors[MIDDLE\_ROTOR].isAtTurnoverPosition()) {

rotors[MIDDLE\_ROTOR].rotate()

rotors[LEFT\_ROTOR].rotate()

doubleStepped = true

}

// Rotate middle rotor if right-most rotor is at turnover

IF (rotors[RIGHT\_ROTOR].isAtTurnoverPosition() AND NOT doubleStepped) {

rotors[MIDDLE\_ROTOR].rotate()

}

// Right-most rotor rotates every key press

rotors[RIGHT\_ROTOR].rotate()

}

Code Block 1 The Enigma's rotation mechanism demonstrated by pseudocode

### EnigmaPlus

At a later point in the design and implementation process, it was decided that the EnigmaPlus model would be developed alongside the original machine. As such a readjustment was made to the structure of the Enigma package as demonstrated in [Figure]. This new UML diagram shows both EnigmaPlus and Enigma inheriting from a base class called RotorMachineBase. This class was included to help reduce the amount of duplicated code within the package as well as ensure the two models work in similar fashions.

A diagram of a computer program

Description automatically generated

Figure 13 A UML diagram showing both Enigma and EnigmaPlus

The differences between Enigma and EnigmaPlus are small but important. The encryption process of EnigmaPlus worked differently, in which encoding and decoding are two distinct operations. Consequently, both an encode and decode function were developed in which one is the inverse of the other. Figure 14 shows a flowchart depicting both the encode and decode function for EnigmaPlus. By observing the steps of these algorithms carefully, the inverse relationship becomes clear.

A diagram of a character

Description automatically generated

Figure 14 EnigmaPlus encryption and decryption flowcharts

### Additional Features

In addition to the models developed in this project, numerous classes were added to the Enigma package to create ease-of-use. Whilst these features are not core components of Enigma, they were included in this section as they are useful to have whilst developing applications by offering interesting information regarding the model. Some of these features are not present in previous UML diagrams and they were added much later in the design process and are less noteworthy.

Two logger classes were implemented that log both Enigma and EnigmaPlus. These loggers are static classes which are utilized by both models so that they can provide a step-by-step outline of the encryption/decryption process. The loggers also provide information such as the current rotation at any given frame in the encryption, the effect that each component has on an input letter and all other information regarding the state of the model.

Whilst developing the GUI for this project, it was decided that additional functionality was needed for each model. This new functionality generates a list of all wiring connections in the model at any given frame by using enumeration, in which each letter of the alphabet is encrypted (without rotation applied in this case) and the scrambling of the letter is recorded at each component. This addition allowed for a complete picture of the model to be generated at any time and was used extensively in the GUI development.

## Config and Parsers

The Config and Parsers packages were implemented to create an XML based miniature database within the application. The Config package contained three files, rotor\_bank.xml, reflector\_bank.xml and enigma\_settings.xml which allowed the user to configure the settings for the Enigma machine. The Parsers package contained several XML parser files to parse and store the contents of the files stored within the Config package. As per the requirements of this project, the machine needed to be fully configurable. However, during the implementation of the Enigma package it was decided that a system allowing the user to configure the machine beyond the capabilities of the original machine would be beneficial.

Both rotor\_bank.xml and reflector\_bank.xml were created to allow the user to create their own definitions of the corresponding components much like the ones shown in Table 1 and Table 2. Code Block 2 shows an example of an entry a user could create in rotor\_bank.xml, creating a new rotor called “MyCustomRotor”. Once this has been done, at runtime of either the CLI or GUI application, the Parsers package will create rotor objects based on the contents of this file and store it in ComponentCache along with pre-configured components. This cache is then used in both the CLI and GUI for configuration.

<rotor\_bank>

<rotor>

<name>MyCustomRotor</name>

<encoding>ZYXWVUTSRQPONMLKJIHGFEDCBA</encoding>

<turnover\_position>E</turnover\_position>

</rotor>

...

</rotor\_bank>

Code Block 2 rotor\_bank.xml contents showing an example custom rotor called "MyCustomRotor"

The enigma\_settings.xml file was created exclusively for the CLI for a simpler configuration experience. In addition, it also allows the use of any custom components that are stored within ComponentCache at runtime. Code Block 3 shows an example configuration of the Enigma using the custom component shown in Code Block 2

<enigma>

<plugboard encoding="AM FI NV PS TU WZ"></plugboard>

<rotor>

<name>MyCustomRotor</name>

<ring\_setting>22</ring\_setting>

<start\_position>L</start\_position>

</rotor>

<rotor>

<name>I</name>

<ring\_setting>13</ring\_setting>

<start\_position>B</start\_position>

</rotor>

<rotor>

<name>II</name>

<ring\_setting>24</ring\_setting>

<start\_position>A</start\_position>

</rotor>

<reflector>

<name>UKW-A</name>

</reflector>

</enigma>

Code Block 3 enigma\_settings.xml contents depicting the start settings of the machine

## CLI

As per the requirements, the CLI was to be developed as a basic and simple application which acts more like a tool than an educational experience. Consequently, the code that underpins this application is relatively short and simple. As previously mentioned, when using the CLI the configuration of the Enigma model takes place within the Config package, specifically enigma\_settings.xml as demonstrated in Code Block 3. Originally, a multi-faced menu approach was experimented with to allow for the user to configure the machine. However, due to the complexity of the Enigma’s key, this led to a tiresome and confusing experience during the setup of the model. The Config package approach allowed for easier editing as well as enabling the settings of the Enigma to be stored.

With the configuration mechanism developed, design regarding what information the user should be provided with in the CLI could begin. Firstly, it was decided that the starting settings of the Enigma should be displayed to the user, to ensure that they understand the settings that were used to encrypt their message. Secondly, the user should be prompted to enter a message before the correct cyphertext (or plaintext if this is a decryption) is displayed. Code Block 4 shown an example of the expected interaction with the CLI, showing the chosen settings for most of the figure, and showing the encryption process of the message “HELLO WORLD”. The same output would be expected if the user intended to decode a message, however the input “HELLO WORLD” would be replaced with “JCUGQ KVBVF” and vice versa

Plugboard : [AM FI NV PS TU WZ]

Reflector : UKW-A (EJMZALYXVBWFCRQUONTSPIKHGD)

Right Rotor : III

Rotation : L

Ring Setting : 22

Encoding : BDFHJLCPRTXVZNYEIWGAKMUSQO

Middle Rotor : I

Rotation : B

Ring Setting : 13

Encoding : EKMFLGDQVZNTOWYHXUSPAIBRCJ

Left Rotor : II

Rotation : A

Ring Setting : 24

Encoding : AJDKSIRUXBLHWTMCQGZNPYFVOE

Enter plaintext message:

HELLO WORLD

Cyphertext

JCUGQ KVBVF

Code Block 4 An example of the expected interaction with the CLI

The functionality to accomplish the requirements of the CLI was achieved by creating the EnigmaSimulatorCLI class, which acted as a runnable file.

## GUI

# Results

# Evaluation

## Model Evaluations

* Test Coverage
* Actual German messages
* Permutations compared with improved model.
* Compare to other products.

## GUI Evaluation

* Usability?
* Cross-platform?

# Conclusion

# References

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

n.d. *Enigma Machine.* https://cryptii.com/pipes/enigma-machine.

n.d. *Enigma Machine Emulator.* Accessed 2024. https://www.101computing.net/enigma-machine-emulator/.

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.

MacWright, Tom. n.d. *Enigma Machine.* Accessed 2024. https://observablehq.com/@tmcw/enigma-machine.

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.

n.d. *Science Museum.* Accessed 2024. https://www.sciencemuseum.org.uk/home.

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.

n.d. *Virtual Enigma.* Accessed 2024. https://enigma.virtualcolossus.co.uk/VirtualEnigma/.

# List 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. Photo taken by author at Science Museum London (Science Museum n.d.) 6](#_Toc160964780)

[Figure 2 A front-facing photo of the Enigma I plugboard with cables in place (Enigma n.d.) 8](#_Toc160964781)

[Figure 3 A wiring diagram to show a plugboards potential encoding 9](#_Toc160964782)

[Figure 4 A wiring diagram to show a potential encoding for a reflector 10](#_Toc160964783)

[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 11](#_Toc160964784)

[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. 11](#_Toc160964785)

[Figure 7 An example of an encryption/decryption taking place in an Enigma I machine. In this case A is encoded to C. 11](#_Toc160964786)

[Figure 8 A circuit showing an Enigma style machine avoiding both self-coding and reciprocal coding. Taken from Figure 6 (Thimbleby 2016) 13](#_Toc160964787)

[Figure 9 A wiring diagram depicting "EnigmaPlus". Note that there is no reflector as well as encoding and decoding take place in opposing directions. 13](#_Toc160964788)

[Figure 10 A diagram depicting the underlying system of this project 15](#_Toc160964789)

[Figure 11 UML diagram depicting the Enigma package, omitting EnigmaPlus 16](#_Toc160964790)

[Figure 12 A flowchart depicting the Enigma models encryption/decryption steps 17](#_Toc160964791)

[Figure 13 A UML diagram showing both Enigma and EnigmaPlus 18](#_Toc160964792)

[Figure 14 EnigmaPlus encryption and decryption flowcharts 19](#_Toc160964793)

# List of Tables

[Table 1 "Enigma I" rotor encodings (Enigma wiring n.d.) 7](#_Toc160964776)

[Table 2 "Enigma I" reflector encodings (Enigma wiring n.d.) 8](#_Toc160964777)

# List of Equations

[Equation 1 Permutations for rotors (excluding ring setting) 7](#_Toc160964763)

[Equation 2 The encryption steps of Enigma I 9](#_Toc160964764)

[Equation 3 An equation and additional constraints to describe the behaviour of an Enigma reflector 10](#_Toc160964765)

[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 10](#_Toc160964766)

[Equation 5 Definition of double factorial 12](#_Toc160964767)

[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). 12](#_Toc160964768)

# List of Code Blocks

[Code Block 1 The Enigma's rotation mechanism demonstrated by pseudocode 18](#_Toc160964756)

[Code Block 2 rotor\_bank.xml contents showing an example custom rotor called "MyCustomRotor" 20](#_Toc160964757)

[Code Block 3 enigma\_settings.xml contents depicting the start settings of the machine 20](#_Toc160964758)