

**“Software Approach To Enigma Machine”**

PROJECT REPORT



April-23-2022

****

GROUP MEMBERS-

**Group-6**

20MEI10033 SOURABH SAHU

20MEI10010 M.PON DINESH KUMAR

20MEI10026 YOGESH PANCHAL

20MEI10078 DEBROOP SARKAR

**“Software Approach To Enigma Machine”**

**A PROJECT REPORT**

###### ***Submitted by***

20MEI10033 - SOURABH SAHU

20MEI10010 - M.PON DINESH KUMAR

20MEI10026 - YOGESH PANCHAL

20MEI10078 - DEBROOP SARKAR

*in partial fulfillment for the award of the degree*

*of*

##### INTEGRATED MASTER OF TECHNOLOGY

*in*

**COMPUTER SCIENCE AND ENGINEERING SPECIALIZATION IN CYBER SECURITY**

****

**SCHOOL OF COMPUTING SCIENCE AND ENGINEERING**

**VIT BHOPAL UNIVERSITY**

**KOTHRIKALAN, SEHORE**

**MADHYA PRADESH - 466114**

April-2022

(A typical specimen of Bonafide Certificate)

**VIT BHOPAL UNIVERSITY, KOTHRIKALAN, SEHORE**

**MADHYA PRADESH – 466114**

**BONAFIDE CERTIFICATE**

Certified that this project report titled **“Software Approach To Enigma Machine”** is the bonafide work of “**Sourabh Sahu (20MEI10033) , M. Pon Dinesh kumar (20MEI10010) , Yogesh Panchal (20MEI10026) , Debroop Sarkar (20MEI10078) ”** who carried out the project work under my supervision. Certified further that to the best of my knowledge the work reported at this time does not form part of any other project/research work based on which a degree or award was conferred on an earlier occasion on this or any other candidate.

**PROGRAM CHAIR PROJECT GUIDE**

Dr. H Azath sir, Dr.S.Rajasoundaran,

Assistance professor (senior) Grade 2 Assistance professor

Head of the Department

School of Computer Science and Engineering School of Computer Science and Engineering

VIT BHOPAL UNIVERSITY VIT BHOPAL UNIVERSITY

**ACKNOWLEDGEMENT**

First and foremost, I would like to thank the Lord Almighty for His presence and immense blessings throughout the project work.

I wish to express my heartfelt gratitude to Dr. H AZATH sir Head of the Department, School of computer Science for much of his valuable support encouragement in carrying out this work.

I would like to thank my internal guide Mr./Ms. Dr.S.Rajasoundaran sir, for continually guiding and actively participating in my project, giving valuable suggestions to complete the project work.

I would like to thank all the technical and teaching staff of the School of Aeronautical Science, who extended directly or indirectly all support.

Last, but not least, I am deeply indebted to my parents who have been the greatest support while I worked day and night for the project to make it a success.

**LIST OF ABBREVIATIONS**

**LIST OF TABLE**

|  |  |  |
| --- | --- | --- |
| **TABLE NO.** | **TITLE** | **PAGE NO.** |
| **1** | **LIST OF ABBREVIATIONS** | **5** |
| **2** | **LIST OF FIGURES AND GRAPHS** | **6** |
| **3** | **TABLE OF CONTENTS** | **8** |

**ABSTRACT**

The Enigma machine is a cipher device developed and used in the early- to mid-20th century to protect commercial, diplomatic, and military communication.

In this project we are trying to show how the actually Enigma machine work based on Software Approachs.

We want to write a program to simulate the Enigma machine to decrypt the secret code produced by the Enigma machine. And also we try to write a program to decrypt the secret code produced by Enigma machine.

An Enigma machine is a electro mechanical rotor cipher machines used for the encryption and decryption of secret massages.

Enigma Machine has played an important role in the history of computing, from motivating the development of the first electronic computer to enabling secure Web-based communication and commerce. This program enable us to know the role of encryption in military and computing history, and have a deep look into the mechanism of Enigma machine.

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| **CHAPTER NO.** | **TITLE** | **PAGE NO.** |
|  | List of Abbreviations  List of Figures and Graphs  List of Tables  Abstract | **v**  iv  vi  viii |
| 1 | **CHAPTER-1:**  **PROJECT DESCRIPTION AND OUTLINE** **Introduction**  1.2 Motivation for the work  1.3 [About Introduction to the project  including techniques]  1.5 Problem Statement  1.6 Objective of the work  1.7 Organization of the project  1.8 Summary | 12-15 |
| 2 | **CHAPTER-2:**  **RELATED WORK INVESTIGATION**  2.1 Introduction | 16 |
| 3 | **CHAPTER-3:**  **REQUIREMENT ARTIFACTS**  3.1 Introduction  3.2 Hardware and Software requirements  3.3 Algorithm | 17-19 |
| 4 | **CHAPTER-4:**  **DESIGN METHODOLOGY AND ITS NOVELTY**  4.1 Introduction  4.2 Methodology and goal  4.3 Functional modules design and analysis  4.4 User Interface designs  4.5 Software Architectural designs | 20-26 |
| 5 | **CHAPTER-5:**  **TECHNICAL IMPLEMENTATION & ANALYSIS**  5.1Outline  5.2 Technical coding and code solutions  5.3 Testing and validation  5.4 Enigma circuit | 26-31 |
| 6 | **CHAPTER-6:**  **PROJECT OUTCOME AND APPLICABILITY**  6.1Outline  6.2 Significant project outcomes  6.3 Project applicability on Real-world applications  6.4 Conclusion  6.5 Inference | 32-33 |
| 7 | **CHAPTER-7:**  **CONCLUSIONS AND RECOMMENDATION**  7.1Outline  7.2 Limitation/Constraints of the System  7.3 Future Enhancements  7.4 Inference | 34 |
|  | Appendix A  Appendix B  References  ***Note: List of References should be written as per IEEE/Springer reference format. (Specimen attached)*** | 35 |

**RELATED WORK INVESTIGATION**

The Enigma machine was invented by German engineer [Arthur Scherbius](https://en.wikipedia.org/wiki/Arthur_Scherbius) at the end of [World War I](https://en.wikipedia.org/wiki/World_War_I). This was unknown until 2003 when a paper by Karl de Leeuw was found that described in detail Scherbius' changes. The German firm Scherbius & Ritter, co-founded by Scherbius, patented ideas for a cipher machine in 1918 and began marketing the finished product under the brand name *Enigma* in 1923, initially targeted at commercial markets. Early models were used commercially from the early 1920s, and adopted by military and government services of several countries, most notably [Nazi Germany](https://en.wikipedia.org/wiki/Nazi_Germany) before and during [World War II](https://en.wikipedia.org/wiki/World_War_II).

Several different Enigma models were produced, but the [German military](https://en.wikipedia.org/wiki/Wehrmacht) models, having a [plugboard](https://en.wikipedia.org/wiki/Plugboard), were the most complex. Japanese and Italian models were also in use. With its adoption (in slightly modified form) by the German Navy in 1926 and the German Army and Air Force soon after, the name *Enigma* became widely known in military circles. Pre-war German military planning emphasized fast, mobile forces and tactics, later known as [blitzkrieg](https://en.wikipedia.org/wiki/Blitzkrieg), which depend on radio communication for command and coordination. Since adversaries would likely intercept radio signals, messages had to be protected with secure encipherment. Compact and easily portable, the Enigma machine filled that need.

**CHAPTER-1**

1. **PROJECT DESCRIPTION AND OUTLINE**
2. **Introduction**

An Enigma machine is a electro mechanical rotor cipher machines used for the encryption and decryption of secret massages.

computing history, and have a deep look into the mechanEnigma Machine has played an important role in the history of computing, from motivating the development of the first electronic computer to enabling secure Web-based communication and commerce. This program enable us to know the role of encryption in military and ism of Enigma machine.

The needs of data protection.

Using computers, the Allies were eventually able to break the Enigma code, giving them an intelligence edge that changed the balance of the war.

We want to write a program to simulate the Enigma machine to decrypt the secret code produced by the Enigma machine.

In this project we have operate the software processing-4 and write the separate program for each part of Enigma machine like as rotor , reflector.

In World War II, the Nazi military employed an encryption scheme that addressed the weakness of substitution ciphers. The scheme, implemented by typewriter sized devices known as Enigma machines, gave the Nazis a tactical advantage that greatly contributed to their early success in the war.

Using computers, the Allies were eventually able to break the Enigma code, giving them an intelligence edge that changed the balance of the war.

* 1. **Motivation for the work**

Firstly, we started doing basic thing like layout of our project we are simulate the enigma machine hardware to software enigma machine then we have implemented the code for each and part for write the code like for rotor , enigma , simaultor , plug , and reflecter like then we implemented by processing 4 software .then run the successfully execute then the GUI based interface open using we have implement using app development .

* 1. **[About Introduction to the project including techniques]**

The Enigma required a list of daily key settings and auxiliary documents. In German military practice, communications were divided into separate networks, each using different settings. These communication nets were termed *keys* at [Bletchley Park](https://en.wikipedia.org/wiki/Bletchley_Park), and were assigned [code names](https://en.wikipedia.org/wiki/Code_name), such as *Red*, *Chaffinch*, and *Shark*. Each unit operating in a network was given the same settings list for its Enigma, valid for a period of time. The procedures for German Naval Enigma were more elaborate and more secure than those in other services and employed auxiliary [codebooks](https://en.wikipedia.org/wiki/Codebook). Navy codebooks were printed in red, water-soluble ink on pink paper so that they could easily be destroyed if they were endangered or if the vessel was sunk.

**1.4 Problem Statement**

**What do we want to do?**

We want to write a program to simulate the Enigma machine to decrypt the secret code produced by the Enigma machine.

There is no weighting factor associated with different plaintext letters. Checking all 159 X 10^18 possible letter substitutions, even by machine, was clearly impractical and that's just for one message. The security and intelligence services however had to decrypt several thousand messages every day. The machine settings were also changed daily so that any minor decryption discoveries would have a very limited useful lifetime.

The Enigma Code was therefore thought to be unbreakable.

* 1. **Objective of the work**

In this project, the team will create a Java program which will emulate an Enigma Machine and produce accurately encrypted or decrypted results from a given input. This software can be used as an educational device, as a historical piece, or as a tool for puzzle creation and decryption in intellectual social gatherings. The team will also spend a portion of the project researching and implementing possible algorithms for decrypting communications

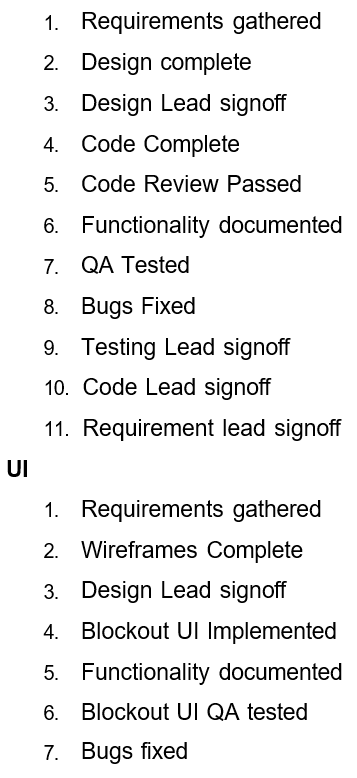
In this project we are trying to show how the actually Enigma machine work based on Software Approachs.

This project is very capable to secure the information .

And as you know the Enigma machine is used in world war II so it also use to for our military base where they can use software approach method and communicate with each other.

* 1. **Organization of the project**

The end product of this project will be divided into smaller demonstrable milestones (See Project Deliverables). Each component must go through the following checklist before it is considered “complete”.



* 1. **Summary**

Overall we here present the great project software approach to enigma machine.

And show the how to actuall work enigma machine in software approach to enigma machine.

**CHAPTER-2**

1. **RELATED WORK INVESTIGATION**

The Enigma machine was invented by German engineer [Arthur Scherbius](https://en.wikipedia.org/wiki/Arthur_Scherbius) at the end of [World War I](https://en.wikipedia.org/wiki/World_War_I). This was unknown until 2003 when a paper by Karl de Leeuw was found that described in detail Scherbius' changes. The German firm Scherbius & Ritter, co-founded by Scherbius, patented ideas for a cipher machine in 1918 and began marketing the finished product under the brand name *Enigma* in 1923, initially targeted at commercial markets. Early models were used commercially from the early 1920s, and adopted by military and government services of several countries, most notably [Nazi Germany](https://en.wikipedia.org/wiki/Nazi_Germany) before and during [World War II](https://en.wikipedia.org/wiki/World_War_II).

Several different Enigma models were produced, but the [German military](https://en.wikipedia.org/wiki/Wehrmacht) models, having a [plugboard](https://en.wikipedia.org/wiki/Plugboard), were the most complex. Japanese and Italian models were also in use. With its adoption (in slightly modified form) by the German Navy in 1926 and the German Army and Air Force soon after, the name *Enigma* became widely known in military circles. Pre-war German military planning emphasized fast, mobile forces and tactics, later known as [blitzkrieg](https://en.wikipedia.org/wiki/Blitzkrieg), which depend on radio communication for command and coordination. Since adversaries would likely intercept radio signals, messages had to be protected with secure encipherment. Compact and easily portable, the Enigma machine filled that need.

**CHAPTER-3**

1. **REQUIREMENT ARTIFACTS**

**3.1 Introduction**

This project based on hardware and software without these thing it cant be execute that’s why here we are using software and hardware

**3.2 HARDWARE & SOFTWARE REQUIREMENT**

HARDWARE REQUIREMENTS

* One PC
* Processor – Min Core i3
* RAM – Min 4GB
* SSD – 256GB/128GB
* System Bus:- Either 32-Bit or 64-Bit
* Keyboard:- Windows compatible

SOFTWARE REQUIRERMENTS

* Processing 4 software
* Operating Environment :-

Windows XP/Vista/7/8,

Mac, OSX, Linux

**3.3 Algorithm :-**

The Enigma machine implemented a *substitution cipher*, which encrypts a message by substituting one character for another. Such ciphers go back at least as far as Julius Caesar, who used a simple substitution cipher to encrypt military orders.

By rotating the rotor we obtain a new substitution cipher. As an example, suppose the rotor used to produce the substitutions is given by the following values in the first position:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

TMKGOYDSIPELUAVCRJWXZNHBQF.

To encrypt the first letter we use the substitutions given above; i.e. we substitute B by M and Y by Q. However, to encrypt the second letter we rotate the rotor by one position, i.e. we move the bottom row one step to the left, and so use the substitutions.

ABCDEFGHIJKLMNOPQRSTUVWXYZ MKGOYDSIPELUAVCRJWXZNHBQFT,

whilst for the third letter we use the substitutions

ABCDEFGHIJKLMNOPQRSTUVWXYZ KGOYDSIPELUAVCRJWXZNHBQFTM

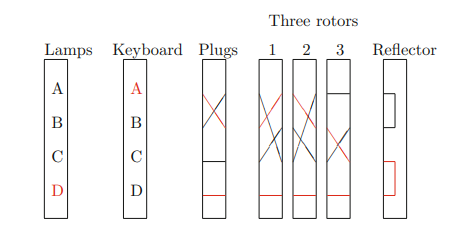


Figure :- Simplified Enigma Machine

**CHAPTER-4**

**DESIGN METHODOLOGY AND ITS NOVELTY**

**4.1 Introduction**

The goal of every encryption algorithm is to make it as difficult as possible to decrypt the generated ciphertext without using the key. If a really good encryption algorithm is used, then there's no technique significantly better than methodically trying every possible key. For such an algorithm, the longer the key, the more difficult it is to decrypt a piece of ciphertext without possessing the key.It's difficult to determine the quality of an encryption algorithm. Algorithms that look promising sometimes turn out to be very easy to break, given the proper attack. When selecting an encryption algorithm, it's a good idea to choose one that's been in use for several years, and has successfully resisted all attacks.For more information, see Data encryption and decryption functions.

**4.2 Methodology and goal**

Data encryption and decryption Encryption is the process of translating plain text data (plaintext) into something that appears to be random and meaningless (ciphertext). Decryption is the process of converting ciphertext back to plaintext.To encrypt more than a small amount of data, symmetric encryption is used.

We want to write a program to simulate the Enigma machine to decrypt the secret code produced by the Enigma machine.

And also we try to write a program to decrypt the secret code produced by Enigma machine.

Rotating Ciphers

After each letter is encoded, the key is rotated so that the first character is moved to the end.

Example: a b cdef→ hjasdb

encode: a a a⇒hjaob

encode: a b c → had

It is a combination of three rotating rotor (wheel).

The inner rotor rotate one step after every single character is encrypted.

The middle rotor rotate one step after the inner rotor complete a round of rotation.

It is a combination of three rotating rotor.

The inner rotor rotate one step after every single character is encrypted.

The middle rotor rotate one step after the inner rotor complete a round of rotation.

**4.3 Functional modules design and analysis**

**Enigma:-** meaning hard to understand or explain

The Enigma was influential in the field of cipher machine design, spinning off other rotor machines.

**Enigma SIM:-** Enigma simulator, the message procedures as used by the German Armed Forces, including some authentic message.

Light :- For each letter pressed, one lamp lit indicating a different letter according to a pseudo-random substitution determined by the electrical pathways inside the machine.

**Plugpoint :-** The Enigma machine had several cables with a plug at each end that could be used to plug pairs of letters together.

**Rotor :-** The rotors (alternatively *wheels* or *drums*, *Walzen* in German) form the heart of an Enigma machine. Each rotor is a disc approximately 10 cm (3.9 in) in diameter made from [Ebonite](https://en.wikipedia.org/wiki/Ebonite) or [Bakelite](https://en.wikipedia.org/wiki/Bakelite) with 26 [brass](https://en.wikipedia.org/wiki/Brass), spring-loaded, [electrical contact](https://en.wikipedia.org/wiki/Electrical_contact) pins arranged in a circle on one face, with the other face housing 26 corresponding [electrical contacts](https://en.wikipedia.org/wiki/Electrical_contacts) in the form of circular plates. The pins and contacts represent the [alphabet](https://en.wikipedia.org/wiki/Alphabet) — typically the 26 letters A–Z, as will be assumed for the rest of this description.

**4.4 Design and User Interface**

The Enigma Machine version will determine the complexity of the project. An early machine may have three rotors and no plug board. A later version could have four rotors of a possible subset of eight to ten and a plug board. The goal of this project is to provide an Enigma Machine of variable version, allowing the user to select the number and type of rotors used and if the plug board and ring settings will be required. The user will be provided multiple options for

plain or cipher text input into the machine. These may include the following:

1. Completed Goal – Copy/Paste or typed input into a text box
2. Completed Goal – Submit a text file for encryption/decryption
3. Completed Goal – Manual key input simulating a machine
4. Completed Goal – The ability to switch back and forth between the Enigma GUI and a Cryptanalysis GUI via the use of a tabbed pane
5. Completed Goal – A machine version dropdown that restricts rotor and reflector choices based on historically accurate Enigma Machine types
6. Completed Goal – Dropdown that allows the user to choose output text space (groups of four letters, five letters, no spaces, etc)
7. Completed Goal – A reset button

Stretch Goal (Researched, but not implemented) – Accurate machine sounds.

**GUI Interface :-**

****

**4.5 Software Architectural designs**

**FLOW DIAGRAM:-**

Yes

Decrypted Message

Return a Character

Check and Rotate

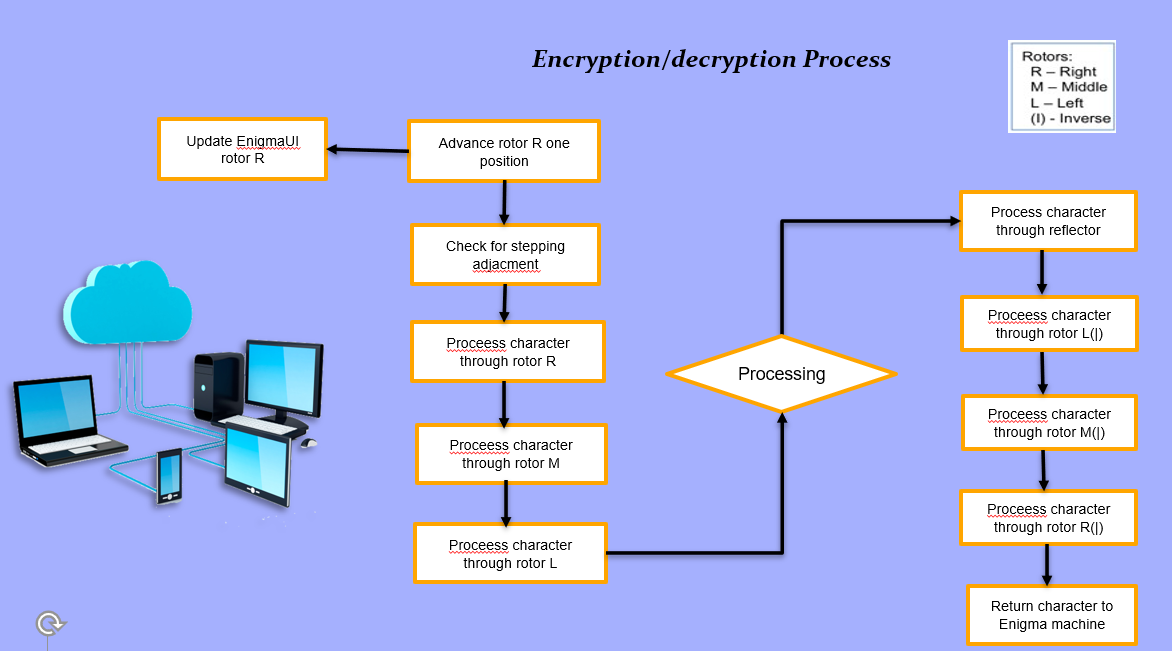
Processing

Read a character

Give the Command encrypt message

Give the Command Normal Text

**Overall System Architecture Diagram :-**



**CHAPTER-5**

**TECHNICAL IMPLEMENTATION & ANALYSIS**

**5.1 Outline :-**

We will discuss the coding and implementation part of our developed system and the analysis of our system.

**5.2 Technical coding and code solutions**

In this project, the team will create a Java program which will emulate an Enigma Machine and produce accurately encrypted or decrypted results from a given input. This software can be used as an educational device, as a historical piece, or as a tool for puzzle creation and decryption in intellectual social gatherings. The team will also spend a portion of the project researching and implementing possible algorithms for decrypting communications

In this project we are written the code for many part if Enigma machine .

Like

End Thing

Enigma

Enigma simulator

Light

Plug

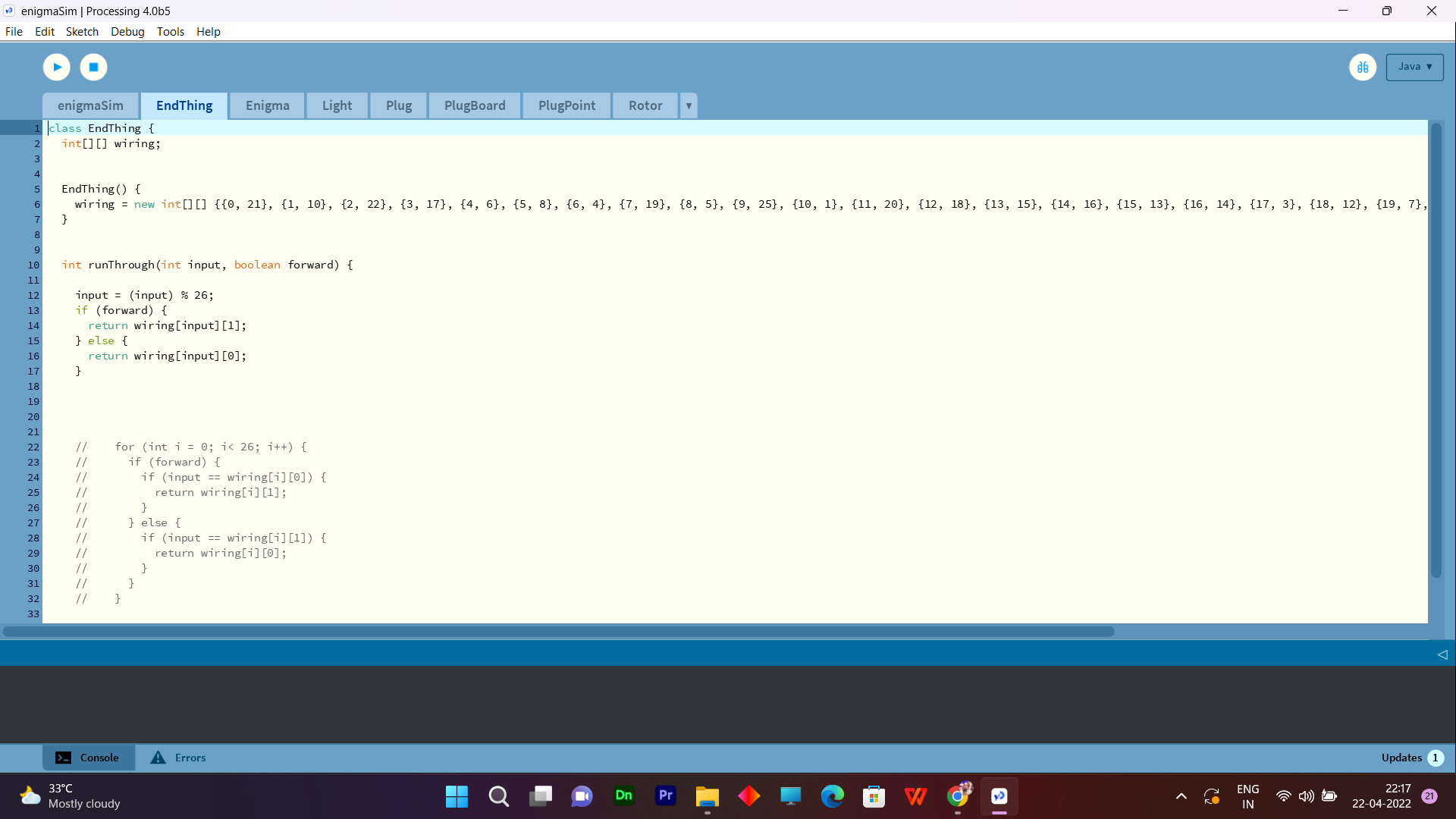
Plugboard

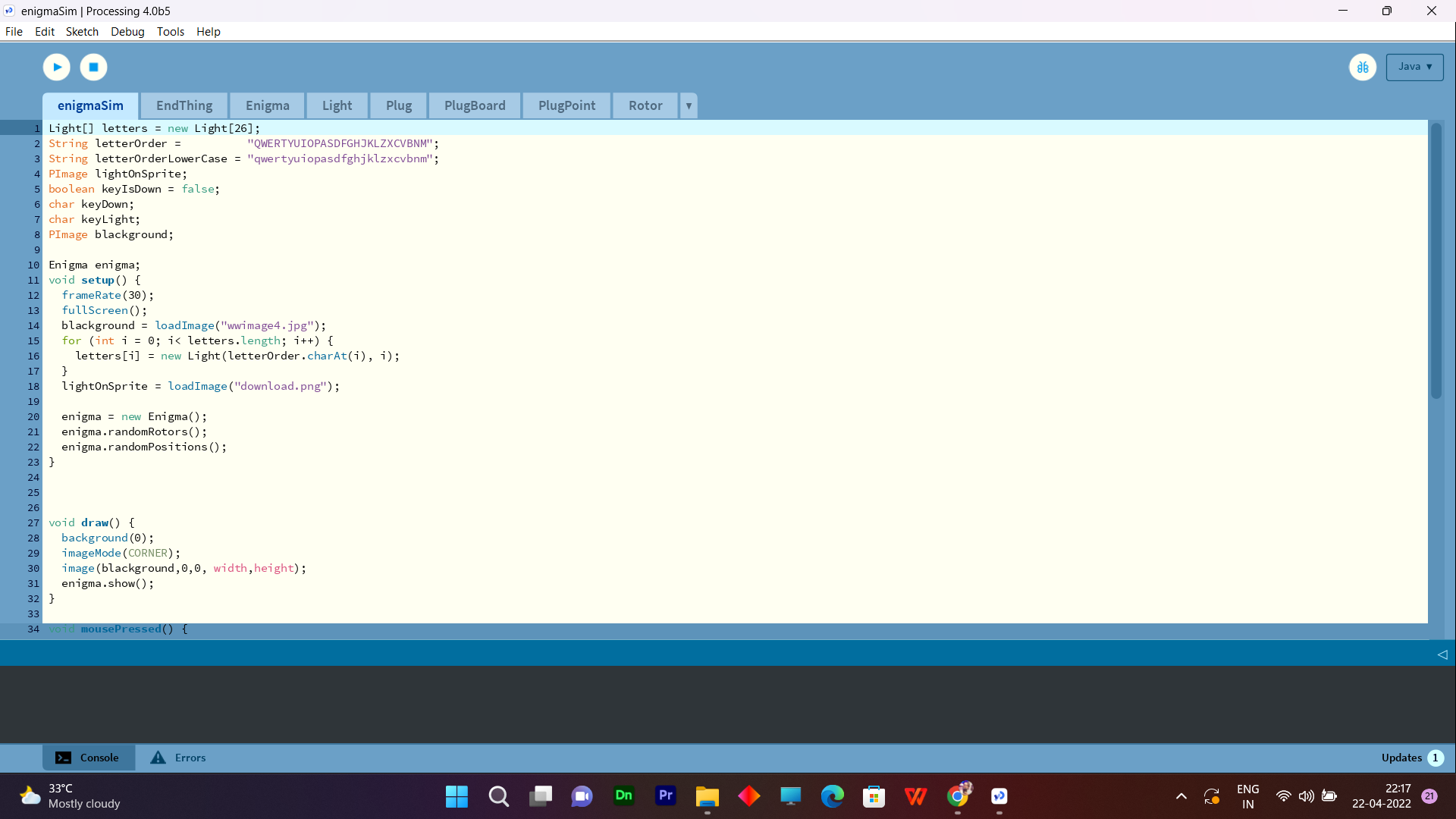
Plugpoint

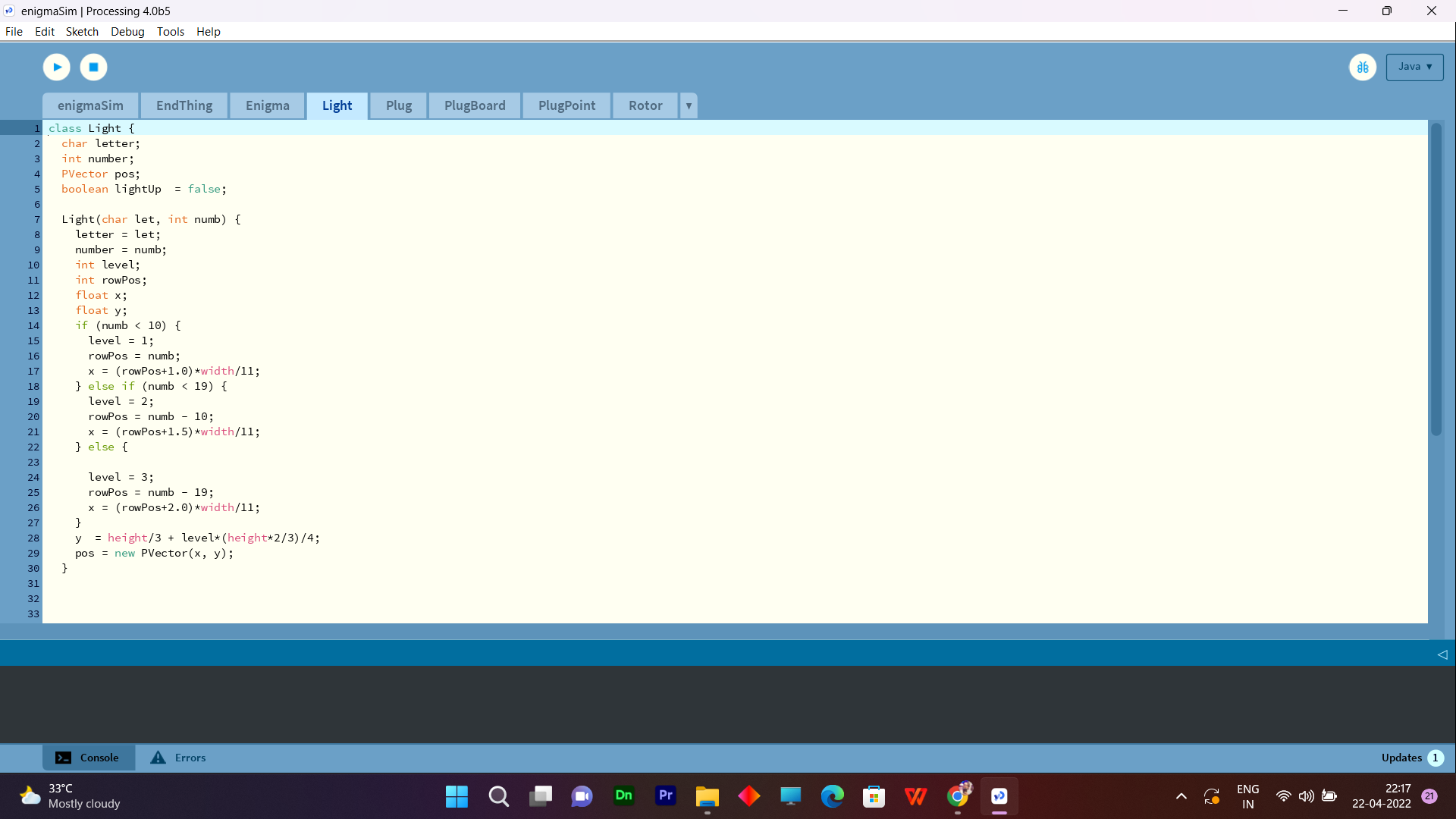
Rotor

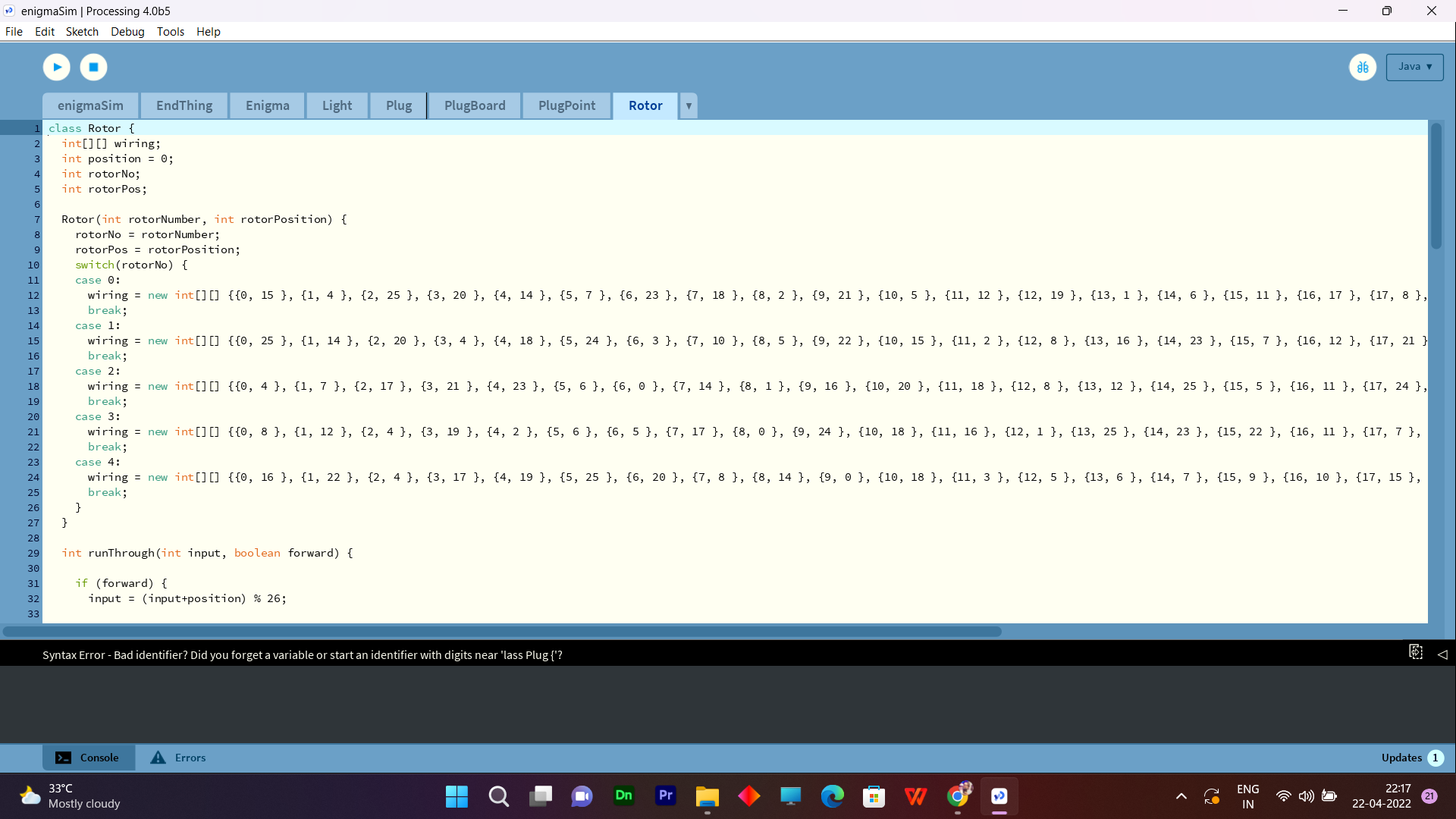
So we show here only the snapshot of our code part because its very less space consumed

But if we write the code here so it take much time and also take much space









**OUTPUT INTERFACE :-**





**TESTING** :-

For the testing purpose here we have taken one example

Normal Text Message:- VIT BHOPAL

Rotor Position :- 1-5-2

Rotor Dial No. :- 12-1-5

Connection :- Q-B E-M T-P U-P I-D

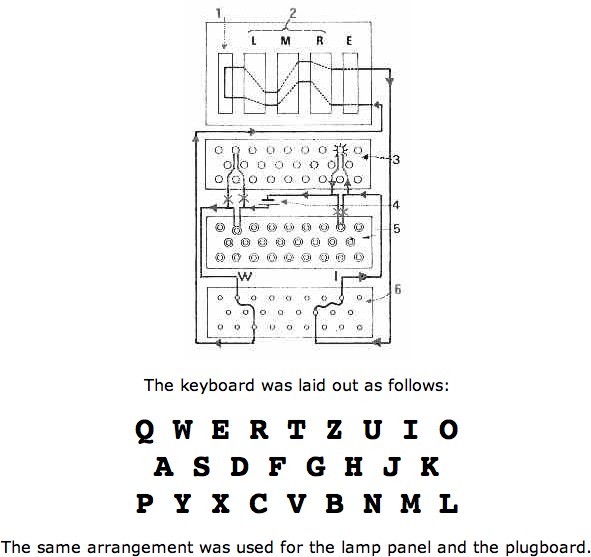
O-J X-L S-L G-V C-N

Encrypted Message :- SJJQSXXVB

Now, Again set the same rotor position because after enter the Normal message rotor dial position will change so we need to set the same rotor dial position and Enter the Encrypted Message.

Decrypted Message:- VIT BHOPAL

**Enigma Circuit :-**



**CHAPTER-6**

**PROJECT OUTCOME AND APPLICABILITY**

**6.1 Outine :-**

We are going to discuss the significant outcomes and the applicability of our developed project. It will help us to know about the system and real word used of that system.

**6.2 Significant project outcomes**

In Software Approach To Enigma Machine produce a good Result

Which is very clear and clarifying that

When we are trying to encrypt or decrypt the any messages using substitution techniques or encryption and decryption method.

That is easly encrypt or decrypt the messages without any error.

This project is very capable to secure the information .

And as you know the Enigma machine is used in world war II so it also use to for our military base where they can use software approach method and communicate with each other.

**6.3 Project applicability on Real-world applications**

Firstly we have implement our code and run.

Then apply Substitution cipher and execute properly

Then open the Enigma machine Interface run the program succesfully

Implement our system Architecture Diagram.

**Application :-**

* In this technological world it will protect information using Encrypt and Decrypt method.
* This is also use for our military base where they can use software approach method and communicate with each other.

**6.4 Conclusion :-**

The Enigma was a very save ciphering machine at its time. Because its heavy usage, the operators of the army made errors which allowed the first breaking.

In this technological world it will protect information using incrypt and decrypt method.

**6.5 Interface :-**

After reading the research paper and feedback of users we can say our developed system is helping the peoples and they are feeling secure about their Secret Messages .

**CHAPTER-7**

**CONCLUSIONS AND RECOMMENDATION**

* 1. **Outline**

We will discuss the constraints and the enhancement for our developed project.

* 1. **Limitation/Constraints of the System**

Enigma code was that a letter could never be encoded as itself.

(Modern computers would be able to crack the code in several minutes)

* 1. **Future Enhancements**

In future this project may be .

In World War II where the Enigma Machine was used for communication .

Similer this project use in future like for gaming .

If we developed this project a large structure then it will be sufficient for more secure the information.

And it is very reliable for our military base where they can use software approach method and communicate with each others.

**7.4 Inference-**

After reading the research paper and feedback of users we can say our developed system is helping the peoples and they are feeling secure about their Secret Messages .

**REFERENCES**

1. ***BehrouzA.Forouzan,CryptographyandNetworkSecurity,2008***
2. ***KeithMartin,“EverydayCryptography” ,2nd Edition,2018***
3. [***"EnigmaHistory"***](https://www.cryptomuseum.com/crypto/enigma/hist.htm)**. cryptomuseum.com*. Retrieved 16 December 2020***
4. **Miller, A. Ray (January 1995).**[**"The cryptographic mathematics of Enigma"**](https://www.tandfonline.com/doi/abs/10.1080/0161-119591883773)**. *Cryptologia*. 19 (1): 65–80.**[**doi**](https://en.wikipedia.org/wiki/Doi_(identifier))**:**[**10.1080/0161-119591883773**](https://doi.org/10.1080%2F0161-119591883773)**.**
5. [***https://www.researchgate.net/figure/Schematic-diagram-of-Enigma-machine-from-Scheribus-1928\_fig3\_273320579***](https://www.researchgate.net/figure/Schematic-diagram-of-Enigma-machine-from-Scheribus-1928_fig3_273320579)

**Lord, Bob (1998–2010).**[***"Enigma Manual"***](http://www.ilord.com/enigma-manuals)***. Retrieved 31 May 2011*.**