**SYNOPSIS REPORT**

**ON**

**Encryption Decryption Techniques**

**Submitted by:**

|  |  |  |
| --- | --- | --- |
| Saksham Mathur | 500068404 | R164218061 |
| Rishabh Tyagi | 500068317 | R164218057 |
| Priyansh Bhatt | 500067895 | R142218046 |
| Divyanshu Sharma | 500068965 | R142218026 |

# Under the guidance of

**Sumit Kumar**

**Assistant Professor Department of Systematics**



**Department of Systematics**

# School of Computer Science and Engineering

**UNIVERSITY OF PETROLEUM AND ENERGY**

**STUDIES**

**Project Proposal Approval Form (2020-21)**

|  |  |  |
| --- | --- | --- |
| I |  |  |
|  |  |

**Minor**

**Synopsis Report (2020-21)**

**Project Title:** Encryption Decryption Techniques

1. **Abstract:**

For the security and privacy of a message while sending them from one point to other these techniques are implemented. It includes changing the plain text to cipher text and then sending it to the justified location for the security of the data in it.

The techniques used for the same include Playfair Cipher, Hill Cipher and Rail Fence Cipher. These are used for the safe transmission of text by turning the plain text into cipher text. And a cipher or cypher is an algorithm for performing these changes which are a series of well-defined steps that can be followed as a procedure. These are coded using C programming language.

1. **Introduction:**

This project is basically based on encryption and decryption of data. For the same we are going to use three kinds of techniques which are Playfair Cipher, Hill Cipher and Rail Fence Cipher.

Before going into any further details about these techniques let us discuss what is the basic meaning of encryption, decryption and cipher.

Encryption is the method by which information is converted into secret code that hides the information's true meaning and the conversion of encrypted data into its original form is called Decryption. It is generally a reverse process of encryption.

The science of encrypting and decrypting information is called cryptography.

A cipher or cypher is an algorithm for performing encryption or decryption which are a series of well-defined steps that can be followed as a procedure. An alternative, less common term is encipherment. To encipher or encode is to convert information into cipher or code. In common parlance, "cipher" is synonymous with "code", as they are both a set of steps that encrypt a message; however, the concepts are distinct in cryptography, especially classical cryptography.

These techniques are coded using C language. It will use the concept of file handling. File handling in C enables us to create, update, read, and delete the files stored on the local file system through our C program. There are many functions in the C library to open, read, write, search and close the file.

The Playfair Cipher was the first practical digraph substitution cipher. The scheme was invented in 1854 by Charles Wheatstone but was named after Lord Playfair who promoted the use of the cipher and were also used during the first and the second World War.

Hill cipher is a polygraphic substitution cipher based on linear algebra. Each letter is represented by a number modulo 26. Invented by Lester S. Hill in 1929, it was the first polygraphic cipher in which it was practical to operate on more than three symbols at once.

And the last, which is the rail fence cipher which is also called a zigzag cipher is a form of transposition cipher. It derives its name from the way in which it is encoded. Given a plain-text message and a numeric key, cipher/de-cipher the given text using Rail Fence algorithm.

**2. Problem Statement:**

Messages being transmitted daily is a very common task. And the security of these messages are important for viewing purposes and much more. Therefore there is a need to develop a way to encrypt and decrypt these files before transmitting. Codes generally substitute different length strings of character in the output, while ciphers generally substitute the same number of characters as are input. There are exceptions and some cipher systems may use slightly more, or fewer, characters when output versus the number that were input.

1. **Literature Review:**
2. The Playfair cipher is notable because it is one of the first ciphers that paired letters (also known as a digraph) instead of using a single letter cipher. This is important because it makes breaking messages much, much harder. Instead of a twenty-six possible monograms, with a digraph; there are six-hundred possibilities.
3. The hill cipher - unlike the others though it is extendable to work on different sized block of letters . So , technically it is a polygraphic substitution cipher , as it can work on digraphs , trigraphs ,(3 letter blocks ) or theoretically any sized blocks .
4. The rail fence cipher is an easy to apply transposition cipher that jumbles up the order of the letters of a message in a quick convenient way . It also has the security of a key to make it a little bit harder to break .
5. **Objective:**

The objective of this project is to develop a tool which could convert cipher text to plain text and plain text to cipher text using ciphers of the user’s choice.

**Sub objectives:**

* Read the message from a source file and then convert the message to cipher text.
* Write the cipher text back into the destination file.
* Convert the cipher text to plain text from the source file.

1. **Methodologies**
2. Prerequisites
3. Defining the various use cases of the project
4. Preparing the data flow diagram of the project
5. Preparing the various modules of the project .
6. Implementation & unit testing
7. Creating the modules using C language.

ii. The project is divided into four major section:

1. Requirement Analysis
2. Studying the existing techniques and journals published on the cipher techniques.
3. Assessment of the requirements of the project.
4. Defining the scope of the project.
5. Design and development of language.
6. Integrating the modules
7. Functioning of different transitions of probabilities in model
8. Testing each module separately.
9. Testing
10. Testing the integration of modules

ii.Testing the system.

1. **System Requirements:**

**Hardware requirements:**

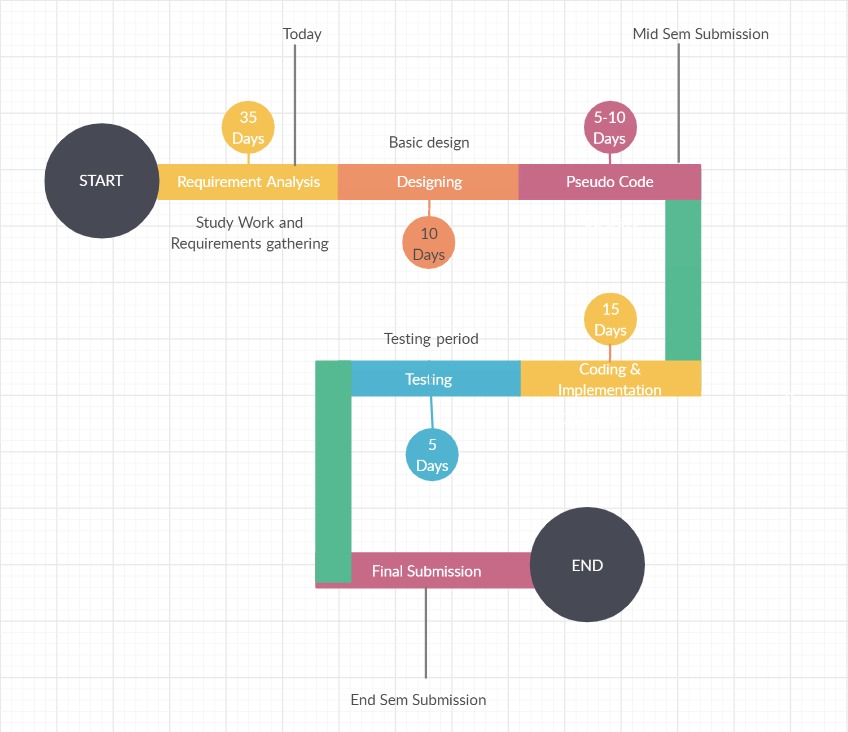
One personal computer with:

* + - * Minimum 4 gigabytes of RAM
      * System with 64-bit processor

**Software requirements:**

* + - * Windows 10
      * Code Editor - Codeblocks

1. **Schedule:**



1. **References:**

* Gaines, Helen Fouché (1956) [1939], *[Cryptanalysis / a study of ciphers and their solutions](https://archive.org/details/cryptanalysis00hele)*, Dover, [ISBN](https://en.wikipedia.org/wiki/ISBN_(identifier)" \o "ISBN (identifier)) [0-486-20097-3](https://en.wikipedia.org/wiki/Special:BookSources/0-486-20097-3" \o "Special:BookSources/0-486-20097-3)
* Smith, Michael *Station X: The Codebreakers of Bletchley Park* (1998, Channel 4 Books/Macmillan, London) [ISBN](https://en.wikipedia.org/wiki/ISBN_(identifier)" \o "ISBN (identifier)) [0-7522-2189-2](https://en.wikipedia.org/wiki/Special:BookSources/0-7522-2189-2" \o "Special:BookSources/0-7522-2189-2)
* Lester S. Hill, Cryptography in an Algebraic Alphabet, *The American Mathematical Monthly* Vol.36, June–July 1929, pp. 306–312. ([PDF](https://web.archive.org/web/20110719235517/http://w08.middlebury.edu/INTD1065A/Lectures/Hill Cipher Folder/Hill1.pdf))
* Lester S. Hill, Concerning Certain Linear Transformation Apparatus of Cryptography, *The American Mathematical Monthly* Vol.38, 1931, pp. 135–154.
* Pratt, Fletcher (1939). *Secret and Urgent: The story of codes and ciphers*. [Aegean Park Press](https://en.wikipedia.org/wiki/Aegean_Park_Press" \o "Aegean Park Press). pp. 143–144. [ISBN](https://en.wikipedia.org/wiki/ISBN_(identifier)" \o "ISBN (identifier)) [0-89412-261-4](https://en.wikipedia.org/wiki/Special:BookSources/0-89412-261-4" \o "Special:BookSources/0-89412-261-4).
* [Helen Fouché Gaines](https://en.wikipedia.org/wiki/Helen_Fouch%C3%A9_Gaines" \o "Helen Fouché Gaines), *Cryptanalysis, a study of ciphers and their solution*, Dover, 1956, [ISBN](https://en.wikipedia.org/wiki/ISBN_(identifier)" \o "ISBN (identifier)) [0-486-20097-3](https://en.wikipedia.org/wiki/Special:BookSources/0-486-20097-3" \o "Special:BookSources/0-486-20097-3)

**Synopsis verified by:**

**Sumit Kumar**

**(Project Guide) (Program Head)**