RESEARCH PAPER

**“Rail Fence Cipher”**

**Prepared By**

Prathmesh Chougule **(2003063)**

Digvijay Patil **(2003065)**

Shreyash Patil **(2003071)**

Devraj Patil **(2003076)**

*Under the subject of*

**INFORMATION SECURITY**



**K.E.S.**

**Rajarambapu Institute of Technology, Rajaramnagar**

**2022-2023**

**History Of Rail Fence cipher:**

A transposition cipher, such as the rail fence cipher, rearranges the letters in a plaintext message to produce an encoded version. The letters are arranged in a form that resembles a fence or a zigzag pattern, giving the cipher its name.

The rail fence cipher was originally mentioned in Nathaniel Bowditch's book "The American Practical Navigator" in 1802, where it served as a straightforward illustration of a transposition cipher. As a code used in scouting and in the Boy Scouts handbooks, the cipher gained popularity in the early 20th century. Today, it mostly serves as a teaching tool for the idea of transposition ciphers.

A plaintext message's letters are rearranged using the rail fence cipher, a straightforward transposition cipher, to produce an encoded message. The main concept behind the cipher is to write the message along a series of "rails" in a zigzag pattern, and then to read the information off the rails in a particular order. The letters you encounter when reading off the beaten path make up the encoded message.

The receiver needs to be aware of the number of utilised rails as well as the reading order in order to decode the message. Decryption often involves writing the ciphertext in a grid in the opposite direction from how it was written during encryption.

The rail fence cipher is a relatively weak cipher that a determined attacker can easily break. Trying different rail sizes and reading off the message in different orders until a meaningful message is found is a simple method of breaking the cipher. Furthermore, the rail fence cipher is susceptible to frequency analysis, a method of breaking a cipher by analysing the frequency of letters in the encoded message.

Because of the cipher's limitations, it is not used for serious cryptographic communication. It is, however, still used as an educational tool to teach the concepts of transposition ciphers and to demonstrate the flaws of simple encryption techniques.

**Rail Fence cipher algorithm explanation :**

The rail fence cipher algorithm is a simple method of encoding a message by rearranging the letters of the plaintext in a zigzag pattern along a set of "rails". The algorithm's basic steps are as follows:

1) Select the number of rails: The number of rails determines the height of the fence and the cipher's level of security. The greater the number of rails used, the more difficult it will be to break the cipher.

2) Along the rails, write the plaintext message in a zigzag pattern: Write the first letter of the plaintext message beginning at the top rail. Continue down the rail, writing the next letter, and so on until you reach the bottom rail. Then, continue writing the message in the same zigzag pattern on the rail above the bottom rail. Continue until the entire plaintext message has been written.

3) Read the message from the rails in the following order: Start at the top rail and read off the letters in the order they appear to decode

the message. Then proceed to the next rail and repeat the process with the letters in the same order.

Repeat this process until all of the letters from all of the rails have been read. The encoded message is the letter sequence obtained when reading off the rails.

4) To decrypt the message, repeat the steps in reverse order. Create a grid along the rail with the ciphertext and read the message diagonally.

For example, suppose you have a message "HELLO" and three rails.

You will write the message as follows:

H . . . O

. E . L .

. . L . .

"HEOLL" will be the ciphertext.

5) It should be noted that the rail fence cipher is relatively weak and easily broken by a determined attacker. It is primarily used as an educational tool or for recreational purposes, rather than for serious cryptographic communication.

6)In proposed algorithm, during encryption string of any length is provided.

Next, string is converted into Ascii code which will increase encryption security.

This Ascii is provided into decimal function which converts it into decimal

For key multiply length of decimal string by 8 and key is passed to the encryption function by creating square root of key.

For decryption Process is just reversed and decrypt the code and get original string.

**The rail fence cipher has the following advantages:**

1) It is a simple and easy-to-implement algorithm that can be used to introduce beginners to the concept of transposition ciphers.

2) It does not require any special mathematical knowledge and is simple to understand.

3) It is simple to use, even for those with no technical background.

4) It can be used to teach the concept of transposition ciphers as well as the limitations of simple encryption techniques.

**The rail fence cipher has the following Disadvantages:**

1) The rail fence cipher is relatively weak, and it can be easily cracked by a determined attacker using simple methods such as frequency analysis or known plaintext attacks.

2) The number of possible keys is limited by the number of rails employed.

3) The ciphertext pattern is easily recognised, and frequency analysis can be used to determine the possible keyword.

4) It is vulnerable to the known-plaintext attack, which allows an attacker to easily decrypt the ciphertext by examining the relationship between the known plaintext and the corresponding ciphertext.

5) It is easily broken by automated tools, such as computer programmes, which attempt all possible keys and decrypt the message.

6) The rail fence cipher is not suitable for serious cryptographic communication, but it can be used as an educational tool or for fun.

**ADVANTAGES OF USING RAIL FENCE CIPHER:**

1) *Simple algorithm:*

The rail fence cipher is a simple algorithm that requires no special mathematical knowledge and is simple to understand and implement.

2) *User-friendly:*

Because it does not require a deep understanding of cryptography, the rail fence cipher can be used by people with no technical background.

3) *Educational Tool:*

The rail fence cipher can be used as an educational tool to introduce beginners to the concept of transposition ciphers and to teach the limitations of simple encryption techniques.

4) *For short Messages:*

Because the rail fence cipher is a transposition cipher and does not change the letters of the plaintext, it is appropriate for short messages.

5) *Simple to implement*:

The rail fence cipher is a basic algorithm that requires no specific mathematical expertise and is straightforward to implement.

Requirements for few resources: Because the rail fence cipher uses few computational resources, it can be used on devices with limited processing capacity.

6) *Recognized Ciphertext:*

The rail fence ciphertext is immediately recognisable, which might be advantageous in cases where the encrypted communication needs to be identified visually from other messages.

**DISADVANTAGES OF USING RAILFENCE CIPHER:**

*1) Weak Security:*

The rail fence cipher is relatively weak, and it can be easily broken by a determined attacker using simple methods such as frequency analysis or known plaintext attacks.

2) *Limited number of keys:*

The number of possible keys is small and it is determined by the number of rails used.

3) *Vulnerable to Known-plaintext attack:*

It is vulnerable to the known-plaintext attack, an attacker can easily decrypt the ciphertext by analyzing the relationship between the known plaintext and the corresponding ciphertext.

4) *Easy to Break:*

It can be easily broken by automated tools, such as computer programs, that will try all possible keys and decrypt the message.

5) *Not recommended for serious cryptographic communication:*

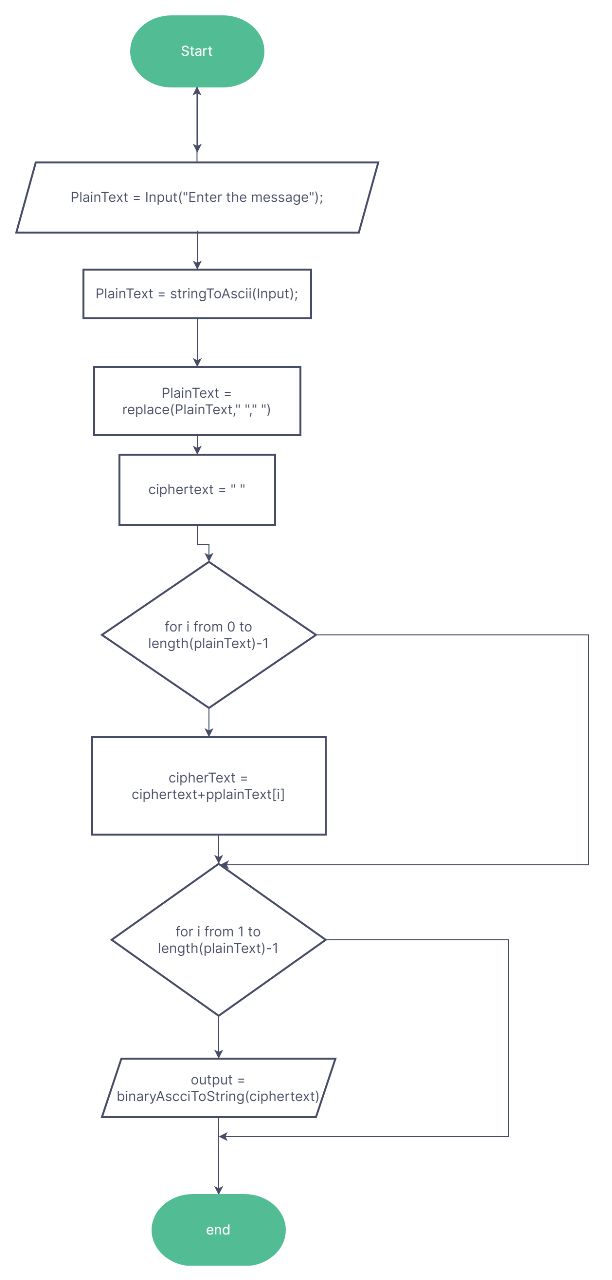
The rail fence cipher is not recommended for serious cryptographic communication as it does not provide a high level of security.

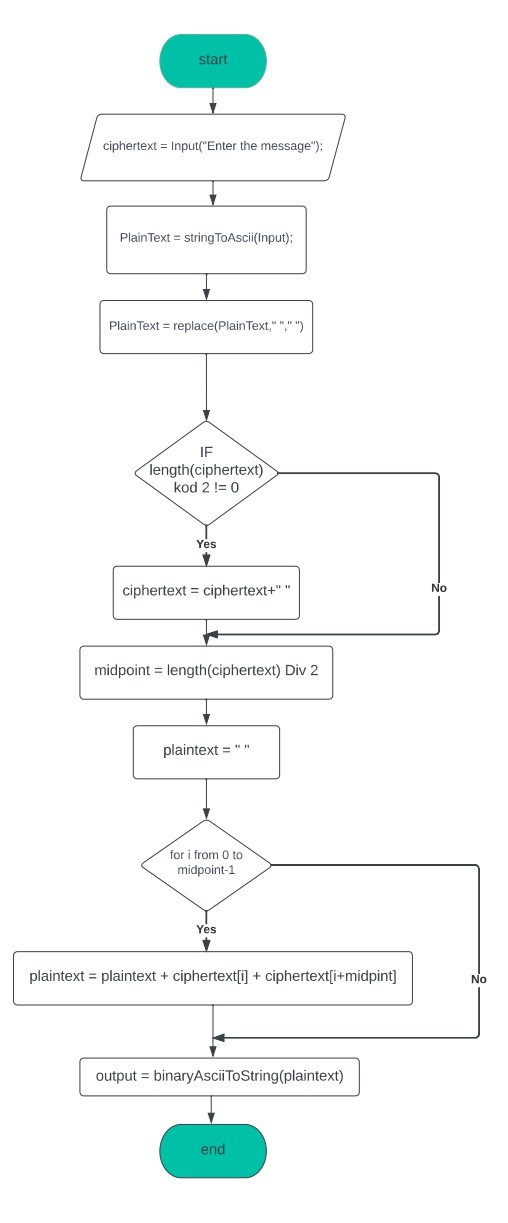
6) *Not suitable for long messages:*

Since the rail fence cipher rearranges the letters of the plaintext, it can cause the repetition of certain patterns that can be used to easily break the cipher. Furthermore, this repetition increases the ciphertext length and make it impractical for long messages.

**Flowchart**

Figure 1:





**IMPLEMENTATION**

Tech-stack used for making of the project:

* HTML
* CSS
* Bootstrap

To implement the logic of the encryption we have used C++ and to provide a Graphical User Interface (GUI) for the user we have made a webpage using above mentioned technologies.

The decryption procedure is performed in the reverse way of the encryption. In which it takes cipher text as the msg value and key is the same, and converts the cipher into plain text by backshifting the alphabets in the alphabet series according to a certain value from the key provided.

In the GUI there is only one web page to encrypt and decrypt the plain text and cipher text respectively. Hence we have seen how the project works ensuring the security of the message.