

**Project**

**Titled**

|  |
| --- |
| **Cryptography Using Transposition** |

|  |  |
| --- | --- |
| ***Class and Section*** |  |
| ***Session*** |  |
| ***Submitted to*** |  |
| ***Submission Deadline*** |  |

***Submitted by:***

|  |  |  |  |
| --- | --- | --- | --- |
| ***Sr No*** | ***Name*** | ***Roll No*** | ***Signature*** |
| ***1*** |  |  |  |
| ***2*** |  |  |  |
| ***3*** |  |  |  |
| ***4*** |  |  |  |
| ***5*** |  |  |  |
|  |  |  |  |

**Marks Obtained:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Signature of Project Advisor:** \_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Abstract:**

This report studies class of cryptography using transposition cipher , its applications and types and it’s importance. Firstly, we introduce cryptography which is the practice of securing communication and data through the use of mathematical algorithms. It involves encoding information in a way that only authorized parties can decode and understand. Secondly , we define it’s application using the method transposition which is defined as a technique where the positions of characters in a message are rearranged according to a certain system or key. Unlike substitution, which replaces characters with other characters, transposition involves changing the order of characters without altering their identities. The goal is to obscure the original message and enhance security.

1. **Introduction:**
   1. Historical Background:

* In 17th century cryptography continued to evolve with the work of notable figures such as Blaise de Vigenère, who devised the Vigenère cipher, an early form of polyalphabetic substitution.
* The 19th century saw the rise of more complex cryptographic systems, including the invention of the Playfair cipher.
* The Enigma machine, used by the Germans during World War II, represented a significant cryptographic challenge. The Allies, including British mathematician Alan Turing, played a crucial role in breaking the Enigma code, contributing to the development of early computers.
* The latter half of the 20th century saw the development of public-key cryptography, with the invention of the RSA algorithm by Ron Rivest, Adi Shamir, and Leonard Adleman in the 1970s.
* The Data Encryption Standard (DES) was adopted as a federal standard in the United States in the 1970s and later replaced by the Advanced Encryption Standard (AES) in the early 2000s.

2.2 Cryptography:

Cryptography is the science and practice of securing communication and information through the use of mathematical techniques and algorithms. It involves encoding data in such a way that only authorized individuals can decipher and understand it, ensuring the confidentiality, integrity, and authenticity of information.

* 1. Types:

In the realm of cryptography, ciphers play a crucial role. Ciphers are algorithms or methods used to encrypt and decrypt messages. There are various types of ciphers, each with its own approach to transforming plaintext into ciphertext. Here are some common types of ciphers:

* + 1. **Substitution Ciphers:**

**Monoalphabetic Substitution:** Each letter in the plaintext is replaced with a corresponding single letter in the ciphertext. Examples include the Caesar cipher and the Atbash cipher.

**Polyalphabetic Substitution:** Multiple alphabets are used for encryption, typically with a key determining the shift. The Vigenère cipher is an example.

* + 1. **Transposition Ciphers:**

**Rail Fence Cipher:** The plaintext is written in a zigzag pattern on multiple lines, and the ciphertext is read off in a different order.

**Columnar Transposition:** The plaintext is written in columns, and the columns are rearranged based on a key before reading off the ciphertext.

* + 1. **Block Ciphers:**

**Data Encryption Standard (DES):** A symmetric key block cipher that operates on 64-bit blocks of data.

**Advanced Encryption Standard (AES):** A symmetric key block cipher widely used for encryption today.

* + 1. **Stream Ciphers:**

**RC4 (Rivest Cipher 4):** A widely used stream cipher, often employed in secure socket layer (SSL) and transport layer security (TLS) protocols.

* 1. Rail fence cipher using transposition cipher

The Rail Fence Cipher is a simple transposition cipher that rearranges the characters of a message by writing them in a zigzag pattern across a set number of rows. It derives its name from the way the letters are arranged, resembling a fence with rails.

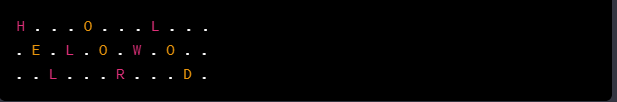
**2**.4.1 **Example no 1:**

2.4.1.1 Encryption

Plaintext: "HELLO WORLD"

Number of Rails: 3

Write the message in a zigzag pattern:



Read the ciphertext row by row:



2.4.1.2 Decryption

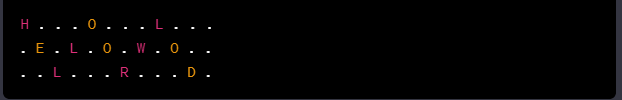
Ciphertext: "HOLELWRLOLD"

Number of Rails: 3

Re-create the zigzag pattern:



Write the ciphertext in the pattern:



Read the original message diagonally:



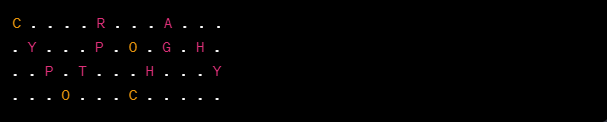
So, in this example, the Rail Fence Cipher encrypts "HELLO WORLD" to "HOLELWRLOLD" using three rails and decrypts it back to the original message.

* + 1. Example no 2:
       1. Encryption

Plaintext: "CRYPTOGRAPHY"

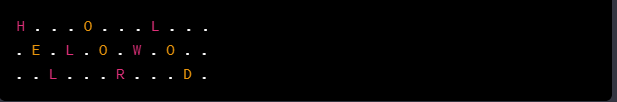
Number of Rails: 4

Write the message in a zigzag pattern:



Read the ciphertext row by row:

Write the message in a zigzag pattern:



Read the ciphertext row by row:



2.4.1.2 Decryption

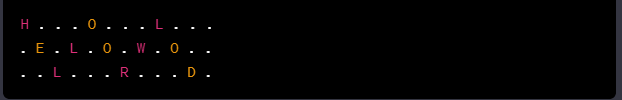
Ciphertext: "HOLELWRLOLD"

Number of Rails: 3

Re-create the zigzag pattern:



Write the ciphertext in the pattern:



Read the original message diagonally:



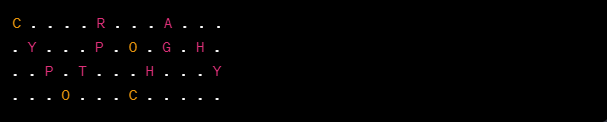
So, in this example, the Rail Fence Cipher encrypts "HELLO WORLD" to "HOLELWRLOLD" using three rails and decrypts it back to the original message.

* + 1. Example no 2:
       1. Encryption

Plaintext: "CRYPTOGRAPHY"

Number of Rails: 4

Write the message in a zigzag pattern:



Read the ciphertext row by row:

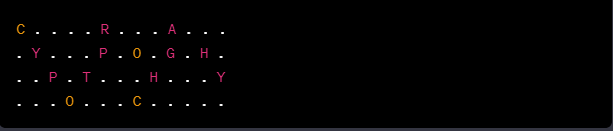


2.4.2.2 Decryption

Ciphertext: "CRAYPGHTHYOCC"

Number of Rails: 4

Re-create the zigzag pattern:



Write the ciphertext in the pattern:

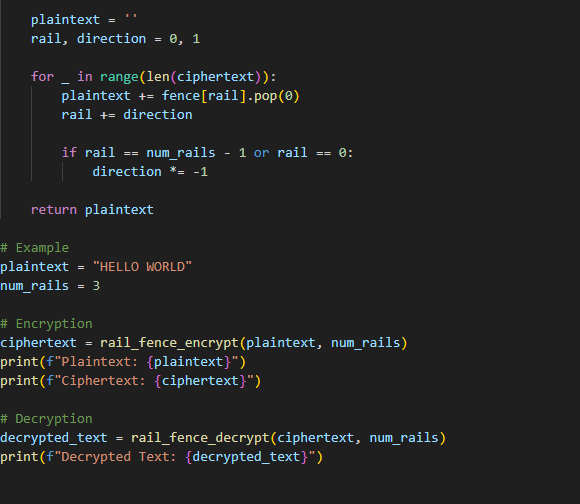
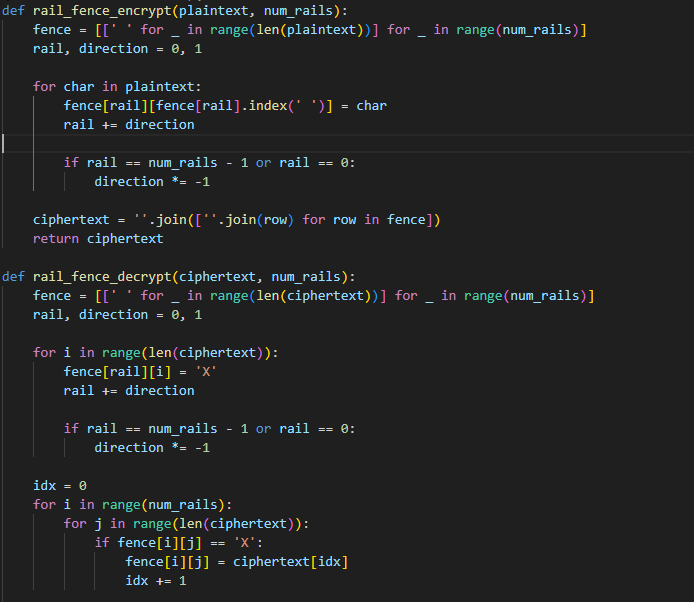


Read the original message diagonally:



In this example, the Rail Fence Cipher encrypts "CRYPTOGRAPHY" to "CRAYPGHTHYOCC" using four rails and successfully decrypts it back to the original message.

1. **Matlab Code:**

****

1. **Results:**

****

1. **Conclusion :**

In conclusion, the Rail Fence Cipher provides a simple and easy-to-understand method of transposing a message. However, it is not considered a highly secure encryption method, as it can be easily deciphered through various techniques such as brute force or frequency analysis. While it may be suitable for educational purposes or as a basic form of encryption, more advanced ciphers with stronger security features are typically preferred for practical applications where data security is crucial.

1. **References:**

* https://www.csfieldguide.org.nz/en/chapters/computer-graphics/graphics
* https://hrcak.srce.hr/file/297879
* https://forum.patagames.com/posts/t50
* https://forum.patagames.com/posts/t501-
* https://www.studysmarter.us/explanations/math/pure-maths/
* https://youtu.be/fkZ72uLULR0
* https://youtu.be/K6QT69hgj50