GPH - International Journal of Mathematics
Journal homepage: www.gphjournal.org e-ISSN 2795-3278 p-ISSN 2795-3274
DOI: https://doi.org/10.5281/zenodo.10209885

CRYPTOGRAPHIC ENCRYPTION BASED ON RAIL-FENCE PERMUTATION CIPHER

Michael N. John[a] Ogoegbulem Ozioma[b] Udoaka Otobong. G.[c] Boniface O. Nwala[d] Obi Perpetua Ngozi[e]

[a]*Department of Mathematics, Akwa Ibom State University, Nigeria Email: storm4help1@gmail.com*
[b]*Department of Mathematics, Dennis Osadebay University, Anwai, asaba, Delta, State, Nigeria Email: Ozioma.ogoegbulem@dou.edu.ng*
[c]*Department of Mathematics, Akwa Ibom State University, Nigeria Email: otobongawasi@aksu.edu.ng*
[d]*Department of Mathematics, Ignatius Ajuru University of Education, Nigeria Email: boninwala@gmail.com*
[e]*Department of Mathematics, Imo State College of Education, Nigeria Email: Zikkyn2016@gmail.com*

A B S T R A C T

Cryptographic systems play a pivotal role in securing sensitive information in various domains. Permutation ciphers, a fundamental component of classical cryptography, involve the rearrangement of characters in a message to achieve confidentiality. This paper explores the principles and applications of permutation ciphers in cryptographic encryption. The study delves into the historical context, the underlying mechanisms of permutation ciphers, and their relevance in contemporary cryptographic practices. Using permutation on n symbols and Rail Fence Cipher, we construct an algorithm for encrypting and decrypting a message for n = 2, 3

Keywords: Cryptographic Encryption, Permutation Ciphers, Confidentiality, Classical Cryptography, Security, Cipher Mechanisms

1. INTRODUCTION

In the ever-evolving landscape of information security, encryption stands as a critical safeguard against unauthorized access and data breaches. Permutation ciphers, a class of cryptographic algorithms, operate by rearranging the order of characters within a message. This rearrangement introduces complexity, making it challenging for adversaries to decipher the original content without knowledge of the specific permutation key. Understanding how cipher works will need an in-depth knowledge of number theory, so I recommend you to read [2], [4] and [6].

An essential aspect of permutation ciphers is their adaptability to modern cryptographic requirements. The study investigates how permutation ciphers can be integrated into contemporary encryption protocols, considering the strengths they bring to the table and potential vulnerabilities that need to be addressed. Additionally, the paper explores innovative approaches and enhancements to permutation-based encryption, such as combining permutation ciphers with other cryptographic techniques to create more robust and secure systems. Read more on cipher algorithms [8], [9].

Cryptography is a secret way to share any message by using Encryption and decryption [10]. Cryptography is most needed area for our society. Many researchers have contributed to developing algorithms for encryption and decryption. In today's world we want more security to share any message. So we need most complicated algorithms for Encryption and decryption. Some known algorithms are DS, DES, AES and RSA algorithms. In this paper we used analog of Permutation and Rail Fence Cipher [12] to develop our algorithm. Here we mixed both of them to create a new algorithm for Encryption and decryption. In [1], B.M. Hamed used the idea of

* *Corresponding author.* Michael N. John.
E-mail address: storm4help1@gmail.com

cipher method modulo 26 and modify it by method modulo 27 (26 Alphabets + Space). Permutation of a finite set A is bijection from A to itself [3]. In this paper, we use congruence relation and idea of matrix multiplication and multiplicative inverse for encryption and decryption.

2. PRELIMINARIES DEFINITION

Definition 2.1: (Permutation Cipher [11]), permutation ciphers are a type of cryptographic algorithm that involves rearranging the positions of characters within a message. The fundamental idea behind permutation ciphers is to change the order of characters in the plaintext to create the ciphertext, providing a form of encryption.
A permutation of a finite set;

- X is bijective function $\pi : X \rightarrow X$. For every $x \in X$ there is a unique element $x' \in X$ such that $\pi(x') = x$.

,

- The inverse permutation $\pi' : X \rightarrow X$ by $\pi^{-1}(x) = x'$ if and only if $\pi(x') = x$. The permutation cipher is also known as Transposition cipher.

Definition 2.2 (Rail Fence Cipher [11], [12]). The Rail Fence Cipher can be mathematically defined using an algebraic representation, particularly in terms of matrix operations. Let's denote the plaintext as *P*, the key as *K* representing the number of rows, and the ciphertext as *C*. The Rail Fence Cipher operation can be viewed as a matrix transformation. Let's create a matrix *M* where the rows represent the rail positions and columns represent the characters in the plaintext.

$$\begin{cases} P_k \; if \; i \; mod K = j \; mod \; K \\ 0 \; otherwise \end{cases}$$

Here, *i* is the row index, *j* is the column index, and *k* is the index of the character in the plaintext.

3. RAIL FENCE CIPHER WITH A TWO SYMBOLS PERMUTATION

We are dealing with a binary scenario where there are two symbols or characters. Let's denote these two symbols as *A* and *B*. The encryption involves rearranging these symbols in a zigzag pattern across a certain number of rows. Here's a mathematical illustration and an example:

3.1 Rail Fence Cipher with a Two Symbols Permutation

We are dealing with a binary scenario where there are two symbols or characters. Let's denote these two symbols as *A* and *B*. The encryption involves rearranging these symbols in a zigzag pattern across a certain number of rows. Here's a mathematical illustration and an example:

3.1.1 Matrix Representation:

Let *M* be the matrix representing the Rail Fence Cipher operation. The symbols *A* and *B* are placed in the matrix according to the Rail Fence pattern. Read the work of [7] to understand Cryptographic Algorithm involving the Matrices.

$$\begin{cases} A \; if \; i \; mod K = j \; mod K (for \; A) \\ B \; if \; i \; mod K = j \; mod K (for \; B) \\ 0 \; otherwise \end{cases}$$

Here, *i* is the row index, *j* is the column index, and *K* is the number of rows.

3.1.2 Mapping Function:

The encryption process can be expressed using a mapping function *F* as follows:

$$C = F(P,K)$$

Here, C is the ciphertext, and P is the plaintext consisting of symbols A and B.

3.1.3 Matrix Operation:

The encryption operation can be represented as a matrix multiplication:

$$C = M \cdot P$$

3.1.4 Example:

Consider the plaintext "ABABA" and the key K=3.

Matrix Representation: $M = \begin{bmatrix} A & 0 & 0 & 0 & B \\ 0 & B & 0 & A & 0 \\ 0 & 0 & A & 0 & 0 \end{bmatrix}$

Reading off the matrix column-wise gives the ciphertext "AAOBBA."

Decryption

To decrypt, the matrix is reconstructed with the same key, and the original plaintext is obtained by reading off the characters row-wise.

The Rail Fence Cipher with a Two Symbols Permutation extends the basic concept to a binary scenario, where symbols A and B are rearranged in a zigzag pattern. The mathematical representation involves matrices and mapping functions, providing a clear structure for encryption and decryption processes

3.2 RAIL FENCE CIPHER WITH A THREE SYMBOLS PERMUTATION

A Rail Fence Cipher with Three Symbols Permutation extends the concept to a ternary scenario, where three symbols (let's denote them as A, B, and C) are rearranged in a zigzag pattern.

3.2.1 Matrix Representation:

Let M be the matrix representing the Rail Fence Cipher operation. The symbols A, B, and C are placed in the matrix according to the Rail Fence pattern.

$$\begin{cases} A\ if\ i\ mod K = j\ mod K (for\ A) \\ B\ if\ i\ mod K = j\ mod K (for\ B) \\ C\ if\ i\ mod K = j\ mod K (for\ C) \\ 0\ otherwise \end{cases}$$

Here, i is the row index, j is the column index, and K is the number of rows.

3.2.2 Mapping Function:

The encryption process can be expressed using a mapping function F as follows:

$$C = F(P,K)$$

Here, C is the ciphertext, and P is the plaintext consisting of symbols A, B, and C.

3.2.3 Matrix Operation:

The encryption operation can be represented as a matrix multiplication:

$$C = M \cdot P$$

3.2.4 Example:

Consider the plaintext "ABCACB" and the key K=4.

Matrix Representation: $M = \begin{bmatrix} A & 0 & 0 & 0 & 0 & C \\ 0 & B & 0 & 0 & B & 0 \\ 0 & 0 & C & C & 0 & 0 \\ 0 & 0 & 0 & 0 & C & 0 \end{bmatrix}$

Reading off the matrix column-wise gives the ciphertext "AACCBCB."

Decryption:
To decrypt, the matrix is reconstructed with the same key, and the original plaintext is obtained by reading off the characters row-wise.

Proof of Reversibility
The Rail Fence Cipher is a transposition cipher, and its basic proof of reversibility involves demonstrating that the rearrangement is invertible. This means that for any ciphertext C, there exists a unique plaintext P such that $F(P,K)=C$. The specifics of the proof depend on the specific permutation applied, and it typically involves showing the existence of an inverse permutation.

4. EXAMPLE

Let's illustrate the encryption and decryption of the word "MICHAEL" using a Rail Fence Cipher with a key of 5. We'll create a table to show the permuted ciphertext, and then we'll demonstrate the ordered pair for encryption and decryption.

Plain text: MICHAEL
Key: 5

Matrix Representation

The matrix M for the Rail Fence Cipher with a key of 5 is created as follows:

$$M = \begin{bmatrix} M & 0 & 0 & 0 & 0 & 0 & H \\ 0 & I & 0 & 0 & 0 & L & 0 \\ 0 & 0 & C & 0 & E & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & A & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Reading off the matrix column-wise gives the ciphertext "MHILEAC."

Matrix Representation (for Decryption): To decrypt, the matrix M is reconstructed with the same key.

$$M = \begin{bmatrix} M & 0 & 0 & 0 & 0 & 0 & H \\ 0 & I & 0 & 0 & 0 & L & 0 \\ 0 & 0 & C & 0 & E & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & A & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Reading off the matrix row-wise gives the original plaintext "MICHAEL."

Table of Permutated Ciphertext

Row/Column	1	2	3	4	5	6	7
1	M	0	0	0	0	0	H
2	0	I	0	0	0	L	0
3	0	0	C	0	E	0	0
4	0	0	0	0	0	A	0
5	0	0	0	0	0	0	0

Ciphertext: "MHILEAC"

Proof of Reversibility

The proof of reversibility involves demonstrating that the rearrangement is invertible. In this case, the rearrangement can be easily reversed by reading off the characters row-wise to obtain the original plaintext.

This example illustrates the encryption and decryption of the word "MICHAEL" using a Permutation on Rail Fence Cipher with a key of 5.

5. CONCLUSION

Permutation ciphers remain a relevant and valuable tool in the cryptographic arsenal. Their historical significance and adaptability make them a subject of continued research and development. As technology advances, permutation ciphers are likely to evolve, and their integration with other cryptographic methods will shape the future of secure communication and data protection. In this paper, we have developed a cryptographic algorithm involving permutation cipher based on Tail-Fence. Here, we provide an example for the permutations based on Rail Fence Cipher with 2, and 3 symbols. One can modify this paper by changing the considered permutation or extend the length by more than 3.

REFERENCES

[1] B. Abdulaziz, M. Hamed and Ibrahim O. A. Albudawe, Encrypt and decrypt messages using invertible matrices modulo 27, American Journal of Engineeering Research, 6(6)(2017), 212-218.
[2] T. M. Apostol, Introduction to analytic number theory, Springer- Verlag, New York, (2011).
[3] S. Arumugam and A. Thangapandi Issac, Modern algebra, Scitech Publications Pvt. Ltd, India, (2018).
[4] D. M. Burton, Elementary Number Theory, McGraw-Hill, New York, (2011).
[5] J. Kannan and Manju Somanath, Congruum Problem, International Journal of Pure and Applied Mathematical Sciences, 9(2)(2016), 123-131.
[6] J. Kannan and Manju Somanath, Fundamental Perceptions in Contemporary Number Theory, Nova Science Publishers, New York, (2023).
[7] J. Kannan, M. Mahalakshmi and A. Deepshika, Cryptographic Algorithm involving the Matrix $Qp*$, Korean J. Math., 30(3)(2022), 533-538.
[8] Manju Somanath, K. Raja, J. Kannan and M. Mahalakshmi, On a class of solutions for a quadratic Diophantine equation, Advances and Applications in Mathematical Sciences, 19(11)(2020), 1097-1103.
[9] Neha Sharma and Sachin Chirgaiyam, A Novel Approach to Hill Cipher, International Journal of Computer Applications, 108(11)(2014), 34-37. Cryptographic Algorithm Based on Permutation Ciphers / A. Deepshika et al. 7
[10] K. H. Rosen, Elementary number theory and its applications, Addison-Wesley Publishing Company, Boston, (1987).
[11] D. R. Stinson and M. B. Paterson, Cryptography theory and practice, CRC Press, Taylor and Francis Group, (2006). [12] S. G. Telang, Number Theory, Tata McGraw - Hill Publishing Company Limited, New York, (1996).
[12] Knight, S., n.d. *The Rail Fence Cipher.* [Online] Available at: http://www.cs.trincoll.edu/~crypto/historical/railfence.html