Scientific Publications

Journal of Mathematics Letters, 2023, 1, 822
www.scipublications.org/journal/index.php/jml
DOI: 10.31586/jml.2023.822

*Article*

# Combined Techniques of Hill Cipher and Transposition Cipher

**A. Hassan [1,*], A. Garko [2], S. Sani [3], U. Abdullahi [4], S. Sahalu [5]**

[1] Department of Mathematics, Federal University Birnin Kebbi, Nigeria
[2] Department of Computer Science, Federal University Dutse, Nigeria
[3] Department of Computer Science, Kebbi State Polytechnic Dakingari, Nigeria
[4] Teachers Service Board Sokoto, Nigeria
[5] Department of Mathematical Sciences, Federal University Gusau, Nigeria

*Correspondence: A. Hassan (husainialiyu@gmail.com)

**Abstract:** Encryption is a method of encoding data so that only authorized parties can read or access that data. With the fast improvement of digital data exchange in electronic way, Information Security is becoming much more important in data storage and transmission. In this paper, the authors work on improving the security of data using a combination of Hill cipher and a Transposition cipher ($\mathbf{G_P}$) , the plaintext will be encrypted using ordinary Hill cipher technique and encrypted again using $\mathbf{G_P}$ cipher there by producing a more complex ciphertext that will be very difficult for cryptanalyst to intrude, and the decryption process is done in two phases, the first decryption will return the ciphertext of the ordinary Hill cipher method and the second decryption will return the original plaintext.

**Keywords:** Encryption, Decryption, Plaintext, Cipher, Permutation, Cryptanalyst, Hill Cipher

**How to cite this paper:**
Hassan, A., Garko, A., Sani, S., Abdullahi, U., & Sahalu, S. (2023). Combined Techniques of Hill Cipher and Transposition Cipher. *Journal of Mathematics Letters, 1*(1), 57–64. Retrieved from https://www.scipublications.com/journal/index.php/jml/article/view/822

**Academic Editor:**
Mohammad Alqudah

**Received:** September 1, 2023
**Revised:** November 12, 2023
**Accepted:** December 2, 2023
**Published:** December 4, 2023



## 1. Introduction

Cryptography is the study of secure communications techniques that allow the sender and intended recipient of a message to view its contents. The term is derived from the Greek word kryptos, which means hidden. It is closely associated to encryption, which is the act of scrambling ordinary text into what is known as cipher text and then back upon required which is known as decryption, this is done primarily in two ways, one to change the position of letters or words in a message known as transposition and the other is by substitution of letters by different ones known as substitution respectively, A "substitution" cipher replaces plaintext symbols with other systems to produce cipher text, as a simple example, the plaintext might be "CONGRATULATIONS" when the letters (C, O, N, G, R, A, T, U, L, A, T, I, O, N, S) are replaced (C=E, O=Q, N=P, G=I, R=T, A=C, T=V, I=K, S=U) the text becomes "EQPITCVWVCVKQPU" respectively. With a transposition cipher, we permute the places where the plaintext letters sit. What this means is that we do not change the letters but rather move them around, transpose them, without introducing new letters. Here is a simple illustration. Suppose that we have seven letters in our plaintext, and the following is a permutation that tells us how to move the seven positions around.

| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| W | E | L | C | O | M | E |

Now if we interchange the numbers, then we are getting our cipher text as in

| 5 | 2 | 4 | 1 | 3 | 7 | 6 |
|---|---|---|---|---|---|---|
| O | E | C | W | L | E | M |

We have the cipher text as "OECWLEM".

Transposition (permutation) pattern have been used in the past decade to study mathematical structures. For instance [2], [3], [21] and [4] studied the concept of permutation pattern using some elaborate scheme to determine the order of precedence and the position of each of the elements in a finite set of prime size. The science of cryptography can be traced back to 2000BC in Egypt. Subsequently many research on transposition and substitution ciphers were conducted by different researchers such as [11], [13] and [15]. Many discussions on transposition and substitution ciphers were made [5],[7],[9], [12] and [17] evaluates the security of transposition ciphers using stack approaches, [1],[20] and [22] discusses a combination of two independent ciphers for a better securing of a data over a communication channels, [4], [6], [8] and [10] investigated enhancement of Ceaser cipher method, [15] discusses an approaches in improving transpositions cipher systems, [16] on modified Ceaser cipher for a better security situations, Azzam and [18] discusses a strong cipher text by combining Hill and Substitution Ciphers, and [14] on modification of an Affine ciphers algorithm for cryptography password. Cryptographic techniques uses two fundamental systems which are symmetric (secret key) and asymmetric (public key), in this study we use a symmetric key for both encryption and decryption. In 2006, [9] using the concept of Catalan numbers a new scheme of generating function for prime numbers ($p \geq 5$) was developed. And furthermore some new studies on the algebraic theoretic properties were been investigated by [19], [20] and [23] the generating function was defined as, $w_{\mathbf{p}} = \{w_1, w_2, \ldots, w_{p-1}\}$ for $p \geq 5$such that $w_i = \big((1)(1+i)mp(1+2i)mp \ldots . (1+(p-1)i)mp\big)$ where **mp ≔ modulop**. Many algebraic properties of $\mathbf{G_p}$ were been investigated, and also cryptographic aspect of $\mathbf{G_p}$ were been investigated by [2] and [18].

## 2. Materials and Method

The concept of Hill cipher and Transposition cipher are necessary tools for this study, they were presented in this section.

### *2.1. Preliminaries*

**Definition 2.1** Plaintext: - Plaintext is the original text from the sender's end

**Definition 2.2** Cipher: Cipher is a systematic mathematical method for encryption and decryption.

**Definition 2.3** Ciphertext: Ciphertext is encrypted text transformed from plaintext using an encryption algorithm

**Definition 2.4** Encryption is a process of transforming information that usually are plaintext using an algorithm (known as cipher) to make it unreadable to anyone except those who have the special knowledge known of the key.

**Definition 2.5** Decryption: Is the process of converting cipher text to plaintext using a cipher and a key.

**Definition 2.6** Key: Is a relatively small piece of information that is used by an algorithm to transform a plaintext into the ciphertext during encryption or a ciphertext into the plaintext during decryption.

**Definition 2.7 Modulo arithmetic:** A modulo of a number in terms of another number (i.e. a mod b) for a, b integers means that, if a number a is divided by b, it gives another number and a remainder then the remainder is the answer. E.g. If a mod b = r, then it implies that ab = C + r. where C is the answer. E.g. 80 mod 26 = 2. As in [2].

**Definition 2.8** Padding: Is the addition of characters in a permutation when the letters are scarce. As in [4].

**Definition 2.9** Hill cipher: Hill cipher is a polygraphic substitution cipher based on linear algebra, invented by Lester S. Hill in 1929, to encrypt a message, each block of n letters (n-component vector) is multiplied by an invertible "n x n matrix", against modulus 26. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.

Example. Let the plaintext message be "HELP" and let "$K = \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}$" be the key invertible matrix to be used.

Then, this plaintext is represented by two pairs $\binom{H}{E}, \binom{L}{P} \rightarrow \binom{7}{4}, \binom{11}{15}$

i. Encryption stage of Hill cipher, in encryption, the key multiplies the n-component vectors.

C=KP, where K is key, P is plaintext and C is the resulting plaintext.

Then we compute $\begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}\binom{7}{4} \equiv \binom{7}{8} (mod 26) and \begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}\binom{11}{15} \equiv \binom{0}{19} (mod 26)$

Then, $\binom{7}{8}, \binom{0}{19} \rightarrow \binom{H}{I}, \binom{A}{T}$ the ciphertext of "HELP = HIAT"

ii. Decryption stage of Hill cipher, in decryption, inverse key multiplies n-component vectors.

P=$K^{-1}$C where P is the resulting plaintext, $k^{-1}$ is the inverse key matrix and C is the cipher text

Then, $\begin{pmatrix} 3 & 3 \\ 2 & 5 \end{pmatrix}^{-1} \equiv \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} (mod 26)$ and $HIAT \rightarrow \binom{H}{I}, \binom{A}{T} \rightarrow \binom{7}{8}, \binom{0}{19}$

Then we compute $\begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix}\binom{7}{8} \equiv \binom{7}{4} (mod 26)$ and $\begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix}\binom{0}{19} \equiv \binom{11}{15} (mod 26)$

Therefore, $\binom{7}{4}, \binom{11}{15} \rightarrow \binom{H}{E}, \binom{L}{P} \rightarrow HELP$. The receiver of the message can now read the cipher text HIAT as HELP.

**Definition 2.10** Cryptanalysis: Is the study of principles and methods of transforming an unintelligible message back into an intelligible message without knowledge of the key, sometimes using frequency analysis of the alphabets as in the table below.

**Table 1. The Prequency of English Letters**

| Letters | Frequency (%) | Letters | Frequency (%) |
|---|---|---|---|
| E | 11.1607 | M | 3.0129 |
| A | 8.4966 | H | 3.0034 |
| R | 7.5809 | G | 2.4705 |
| I | 7.5448 | B | 2.0720 |
| O | 7.1635 | F | 1.8121 |
| T | 6.9509 | Y | 1.7779 |
| N | 6.6544 | W | 1.2899 |
| S | 5.7351 | K | 1.1016 |
| L | 5.4893 | V | 1.0074 |
| C | 4.5388 | X | 0.2902 |
| U | 3.6308 | Z | 0.2722 |
| D | 3.3844 | J | 0.1965 |
| P | 3.1671 | Q | 0.1962 |

**Definition 2.11** Let Ω be a non-empty ordered set such that Ω ⊂ N. Let Gp = {$w_i$: 1≤i≤p-1} be a subgroup of symmetry group $S_n$, such that every $\omega_i$ is generated by arbitrary set Ω for any prime p ≥ 5. That means $G_p$ = {$w_1$, $w_2$, $w_3$, --- $w_{p-1}$} be structure such that each $w_i$ is generated from the arbitrary set w for any prime$p \geq 5$, using the scheme below:

$$w_i = \big((1)(1+i)mp(1+2i)mp \ldots\ldots (1+(p-1)i)mp\big)$$

Then each $w_i$ is called a cycle and the elements in each $w_i$ are distinct and called successors.

When p = 5, we have:

$$G_5 = \{w_1, w_2, w_3, w_4\}, \quad G_5 = \{(12345), (13524), (14253), (15432)\}$$

**Definition 2.12** Transposition cipher (Gp): Transposition cipher is a method of encryption which scrambles the position of characters without changing the characters themselves.

**Encryption on $G_P$**

Since $\boldsymbol{G}_P = (1, \omega_2, \omega_3, \ldots, \omega_{p-1})$ then for the encryption process we can define a relation:

$$C: \ \omega_1 \rightarrow_{(1+i)}$$

Where $i < p-1$ Where $\omega_1$= P, and P is called a plaintext.

**Decryption On $G_P$**

Since $\boldsymbol{G} = (1, \omega_2, \omega_3, \ldots, \omega_{p-1})$ then for the decryption process we have:

$$P: \ _{(1+i)} \rightarrow \omega_1$$

**Definition 2.13** Modulo Inverse: In a modular arithmetic a number ''a'' has a modular inverse $a^{-1}$ for a number m, if $(a.a^{-1}) \bmod_m = 1$, The table below shows all the possible modular inverses of $\bmod_{26}$.

**Table 2. Modulo Inverse of Mod 26**

| A | 1 | 3 | 5 | 7 | 9 | 11 | 15 | 17 | 19 | 21 | 23 | 25 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $a^{-1}$ | 1 | 9 | 21 | 15 | 3 | 19 | 7 | 23 | 11 | 5 | 17 | 25 |

E.g. The modular inverse of 9 is 3 since 9x3 = 27 and 27 mod26 = 1.

**Definition 2.14** Inverse Matrix: The inverse $K^{-1}$ of a matrix K is defined by the equation: $KK^{-1} = K^{-1}K = I$, where *I* is an "n x n" square identity matrix.

**Table 3. Plaintext Alphabet and Their Corresponding Values**

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

## 3. Result

Encryption and decryption processes will take place through two processes. In the encryption process, the plaintext will be encrypted twice with the Hill cipher and Transposition cipher ($G_P$) algorithm, different keys will be used for the two encryptions because the two algorithms are different and also in order to make the cipher text more secure from attackers. So different plaintext, different keys.

$\mathbf{C_i}$ ≔ Multiple cipher texts.

**The encryption process will take the following steps.**

i. Apply encryption function of the Hill cipher on the plaintext (P) to produce cipher text ($C_1$).
ii. Apply encryption function of $G_p$ on $C_1$ to produce $C_2$, where $C_2$ is the ciphertext sent to the receiver.

**The decryption process will use the following steps.**

i. Apply the decryption function of $G_p$ on $C_2$ to produce first ciphertext ($C_1$).
ii. Apply Hill decryption function on $C_1$ to produce the original text (plaintext)

**Example.** Encrypt the message "safe messages" using the key "ciphering"

### *3.1. Encryption Statge*

1. We encrypt the text using Hill cipher. The key is "ciphering", plaintext should be converted into column vectors of length 3.

   $(n \times 1) \equiv (3 \times 1)$ matrices, which is equivalent to $\begin{pmatrix} s \\ a \\ f \end{pmatrix}\begin{pmatrix} e \\ m \\ e \end{pmatrix}\begin{pmatrix} s \\ s \\ a \end{pmatrix}\begin{pmatrix} g \\ e \\ s \end{pmatrix}$, where

   $\begin{pmatrix} s \\ a \\ f \end{pmatrix} = \begin{pmatrix} 18 \\ 0 \\ 5 \end{pmatrix}, \begin{pmatrix} e \\ m \\ e \end{pmatrix} = \begin{pmatrix} 14 \\ 12 \\ 4 \end{pmatrix}, \begin{pmatrix} s \\ s \\ a \end{pmatrix} = \begin{pmatrix} 18 \\ 18 \\ 0 \end{pmatrix}, \begin{pmatrix} g \\ e \\ s \end{pmatrix} = \begin{pmatrix} 6 \\ 4 \\ 18 \end{pmatrix}$ , and the key ciphering is $\begin{pmatrix} c & i & p \\ h & e & r \\ i & n & g \end{pmatrix} = \begin{pmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{pmatrix}$,

   The encryption is given by $C_1 = K\,P$.

$$\begin{pmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{pmatrix}\begin{pmatrix} 18 \\ 0 \\ 5 \end{pmatrix} mod 26 = \begin{pmatrix} 7 \\ 3 \\ 18 \end{pmatrix} = \begin{pmatrix} H \\ D \\ S \end{pmatrix},$$

$$\begin{pmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{pmatrix}\begin{pmatrix} 14 \\ 12 \\ 4 \end{pmatrix} mod 26 = \begin{pmatrix} 8 \\ 14 \\ 4 \end{pmatrix} = \begin{pmatrix} I \\ O \\ E \end{pmatrix}$$

$$\begin{pmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{pmatrix}\begin{pmatrix} 18 \\ 18 \\ 0 \end{pmatrix} mod 26 = \begin{pmatrix} 24 \\ 16 \\ 14 \end{pmatrix} = \begin{pmatrix} Y \\ Q \\ O \end{pmatrix}$$

$$\begin{pmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{pmatrix}\begin{pmatrix} 6 \\ 4 \\ 18 \end{pmatrix} mod 26 = \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} C \\ A \\ A \end{pmatrix}$$

   The cipher text is **$C_1$=HDSIOEYQOCAA.**

2. We encrypt the **$C_1$=HDSIOEYQOCAA** using Gp where number of letters is 12 but **p** is always prime, then we pad the $C_1$with a padding letter X, now $C_1^* =$ **HDSIOEYQOCAAX.**

   $\boldsymbol{G}_{13}$=($_1$,$\omega_2$,$\omega_3$,…, $\omega_{12}$), and $w_1$is given below by the table.

**Table 4. Value of $W_1$**

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| H | D | S | I | O | E | Y | Q | O | C | A | A | X |

Let key =1, then we have. $w_1 \rightarrow w_{(1+k)}$and k=1, then, we have $w_1 \rightarrow w_2$, and $w_2$ is a transposition, given by the table below using the scheme of definition 2.1.11 for $w_i$.

**Table 5. Value of $W_2$**

| 1 | 3 | 5 | 7 | 9 | 11 | 13 | 2 | 4 | 6 | 8 | 10 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| H | S | O | Y | O | A | X | D | I | E | Q | C | A |

Then, **$C_2$ = HSOYOAXDIEQCA,** the intended receiver and the intruder will receive $C_2$ as the message, and then decryption will be performed to get the original message sent.

### *3.2. Decryption Stage.*

1. We decrypt the code by using Gp cipher decryption using k=1, as shown method below.

$$w_{(1+k)} \rightarrow w_{((1+k)-k)}$$

$$w_2 \rightarrow w_{(2-1)}$$

$$\rightarrow w_1$$

And $w_1$ is given in Table 3 above,

2. We decrypt the code "**HDSIOEYQOCAAX**"using Hill cipher decryption algorithm : $P = K^{-1}C$ where $C = C_1$= HDSIOEYQOCAAX, and k is the key.

$$k = \begin{pmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{pmatrix} and\ K^{-1} = \begin{pmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \\ 8 & 13 & 6 \end{pmatrix}^{-1} mod26 = \begin{pmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{pmatrix}$$

Therefore, "HDSIOEYQOCAAX" will be written in n-component vectors as

$$\begin{pmatrix} H \\ D \\ S \end{pmatrix} = \begin{pmatrix} 7 \\ 3 \\ 18 \end{pmatrix}, \begin{pmatrix} I \\ O \\ E \end{pmatrix} = \begin{pmatrix} 8 \\ 14 \\ 4 \end{pmatrix}, \begin{pmatrix} Y \\ Q \\ O \end{pmatrix} = \begin{pmatrix} 24 \\ 16 \\ 14 \end{pmatrix}, \begin{pmatrix} C \\ A \\ A \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}$$

Where X is a padded later to be ignored. Then,

$$\begin{pmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{pmatrix} \begin{pmatrix} 7 \\ 3 \\ 18 \end{pmatrix} mod26 = \begin{pmatrix} 18 \\ 0 \\ 5 \end{pmatrix} = \begin{pmatrix} s \\ a \\ f \end{pmatrix}$$

$$\begin{pmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{pmatrix} \begin{pmatrix} 8 \\ 14 \\ 4 \end{pmatrix} mod26 = \begin{pmatrix} 4 \\ 12 \\ 4 \end{pmatrix} = \begin{pmatrix} e \\ m \\ e \end{pmatrix}$$

$$\begin{pmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{pmatrix} \begin{pmatrix} 24 \\ 16 \\ 14 \end{pmatrix} mod26 = \begin{pmatrix} 18 \\ 18 \\ 0 \end{pmatrix} = \begin{pmatrix} s \\ s \\ a \end{pmatrix}$$

$$\begin{pmatrix} 3 & 7 & 16 \\ 2 & 6 & 17 \\ 9 & 8 & 20 \end{pmatrix} \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix} mod26 = \begin{pmatrix} 6 \\ 4 \\ 18 \end{pmatrix} = \begin{pmatrix} g \\ e \\ s \end{pmatrix}$$

P = safemessages, after paraphrasing we have “safe messages”, the process of decryption is now complete.

## 4. Discussion and Conclusion

The idea of using transposition on Gp was first proposed by [1] and [7] considering security features of transposition cipher which include being more simple to decipher for the intended recipient and very difficult for the unintended recipient of the message and therefore it provides higher level of security to the data being sent over communication channels, and also the Hill cipher is a digraph in nature but can expand to multiply any size of letters, adding more complexity and reliability for better security of the information sent. And finally, the authors discovered that, combination of Hill and transposition gives a cipher text that is somehow impossible for the attackers to get the original message due to multiple algorithms applied there by providing a more complicated cipher text for the intruders.

Hill cipher and transposition cipher (Gp) were been studied individually and their combination give more secure ciphertext than in their ordinary form and cryptanalysis fails due to multiple algorithms employed in the study.

**Acknowledgement**

We would like to express our gratitude to all of the staff of UDUSOK and FUBK Mathematics Department for their immense support in the development of this manuscript for their guidance and contribution in finishing this manuscript.

**Author Contributions**

Conception and design: Hassan, A., and Sani, S. Drafting of the manuscript: Hassan, A and Sani, S. Revision of the manuscript: Abdullahi, U and Sahalu, S. S. Critical Revision of the manuscript: all authors. All authors read and approved the final version of the manuscript.

## References

[1] Alhassan, M. J; Hassan, A; Sani, S. and Alhassan, Y. (2021). A Combined Technique of an Affine Cipher and Transposition Cipher *Quest Journals Journal of Research in Applied Mathematics Volume 7. Issue 10 (2021) pp: 08-12*

[2] Audu M.S. (1986), Generating Sets for Transitive Permutation groups of prime-power order. The Journal of Mathematical Association of Nigeria Abacus, **17**(2), 22-26.

[3] Azzam A and Sumarsono (2017), A Modifying of Hill Cipher Algorithm with 3 Substitution Ceaser Cipher. Proceedings International Conference of Science and Engineering, Indonesia.**1**: 157-163.

[4] Fahrul I, K., Hassan F, S., Toras P and Rahmat W. (2017), Combination of Ceaser Cipher Modification with Transposition Cipher. Advances in Science Technology and Engineering Systems Journal. **2**(5): 22-25.

[5] Garba A. I, Yusuf A and Hassan A. (2018), Some Topological Properties of a Constructed Algebraic Structure. Journal of the Nigerian Association of Mathematical Physics, 45:21-26

[6] Garba A. I, Zakari, Y. and Hassan, A. (2019), on the fuzzy nature of constructed algebraic structure $G_p$. Bayero Journal of Pure and applied sciences, 12(1):146-150

[7] Hassan, A; Alhassan, M. J; Alhassan, Y. and Sani, S. (2021). Cryptography as a Solution for a Better Security International Journal of Advances in Engineering and Management (IJAEM :3(12). pp: 849-853

[8] https://www3.nd.edu/~busiforc/handouts/cryptography/letterfrequencies.html

[9] Ibrahim A. A. (2006), Correspondence between the Length of some Class of Permutation patterns and Primitive Elements of Automophism Group modulo n, Abacus. The Journal of mathematical Association of Nigeria, 33:143-154.

[10] Kuriakkottu A. R. (2021). Use of Transposition Cipher and its Types. International Journal of Research and Engineering, Science and Management 4(11), 164-165

[11] Kashish G and Supriya K. (2013) Modified Ceaser Cipher for a Better Security Enhancement. International Journal of Computer Application.**73**:26-31

[12] Mishra A. (2013), Enhancing security of Ceaser cipher using different methods. International Journal of Research in Engineering and Technology **2**(09):327-332.

[13] Massoud S., Sokouti B. and Saeid P. (2009), An Approach in Improving Transposition cipher System. Indian Journal of Science and Technology.**2**(8):9-15.

[14] Pooja S and Pintu S. (2017), Enhancing security of Ceaser cipher using "Divide and Conquer Approach". International Journal of Advance Research in Science and Engineering. **06**(02):144-150.

[15] Rajput Y., Naik D. and Mane C. (2014), An improved cryptographic technique to encrypt Text message using double encryption. International Journal of Computer Applications**86**(6):24-28.

[16] Sriramoju Ajay Babu. (2017), modification affine ciphers algorithm for cryptography password, Programmer Analyst, Randstad Technologies, EQT Plaza 625 Liberty Avenue, Suite 1020, Pittsburgh, Pennsylvania -15222, USA.

[17] Shahid B. D. (2014), enhancing the security of Ceaser cipher using double substitution method. International Journal of Computer Science and Engineering Technology.**5**:772-774.

[18] M. S. Magami and A. A. Ibrahim (2011). Construction of Association Scheme using some (123) – avoiding class of Aunu patterns. Nigerian Journals of Basic & Applied Sciences (NJBAS). 19(1), 5-8. ISSN 0794-5698. (Index)

[19] Usman. A. and Magami M. S. (2015). An Analysis of Group Theoretic Properties of a Class of (123)- avoiding Pattern of Aunu Numbers Using Thin Cyclic Design. Mathematical Theory and Modeling. 5(5) 45-48. ISSN (Paper) 2224-5804 ISSN (Online) 2225-0522DOI: 10.7176/MTM

[20] M. S. Magami, O. U. Amama, A. I. Garba, (2022). Construction of Vector Space Using Permutation Patterns. Journal of the Mathematical Association of Nigeria. Abacus (Mathematics Science Series) 49(2) 147-153.

[21] S. M. Magami and S. U. Ashafa. (2023). Some parameters of commuting graph of a Multigroups. Far East Journal of Applied Mathematics Pushpa Publishing House, Prayagraj, India http://www.pphmj.comhttp://dx.doi.org/10.17654/0972096023005116 (1), 61-71 P-ISSN: 0972-0960

[22] Magami M. S. and Ibrahim M. (2021). Partition block coordinate statistics on $\Gamma_1$ non-deranged permutation. Journal of Research in Applied Mathematics, 7(9) 28-33. ISSN (Online):2394-0743: ISSN(Print): 2394-0735 (Index)

[23] Magami M. S. and Ibrahim M. (2021). "Admissible Inversion on $\Gamma_1$ non-deranged permutations" Asian Research Journal of Mathematics. ISSN: 2456-477X DOI:10.9734/ARJOM/2021/v17i830322