International Journal of
Mathematics And its Applications
ISSN: 2347-1557

Int. J. Math. And Appl., **11(4)**(2023), 1–7
Available Online: http://ijmaa.in

Cryptographic Algorithm Based on Permutation Ciphers

A. Deepshika[1], J. Kannan [2,*], M. Mahalakshmi[3], K. Kaleeswari[4]

[1,2,3,4]*Department of Mathematics, Ayya Nadar Janaki Ammal College (Autonomous, affiliated to Madurai Kamaraj Univeristy), Sivakasi, Tamil Nadu, India*

Abstract

Cryptography is one of the most needed areas for our society as well as the development of research works. So far, many researchers have contributed to developing algorithms for encryption and decryption. This work is also analogous to them. In this paper, using permutation on n symbols and Hill ciphers, we construct an algorithm for encrypting and decrypting a message. Also, examples for $n = 2, 3, 4$ and are displayed.

Keywords: Cryptography; hill cipher; permutation cipher; modified hill cipher; modified permutation cipher.
2020 Mathematics Subject Classification: 94A60, 05A05, 11C20.

1. Introduction

Cryptography is a secret way to share any message by using Encryption and decryption. 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 Hill Cipher [11] 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 Hill 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 2.1 (Permutation Cipher [11])**.** *The idea of a permutation cipher is to keep the plaintext character inchanged, but to alter their positions by rearranging them using a permutation. A permutation of a finite set*

*Corresponding author (jayram.kannan@gmail.com)

X is bijective function $\pi : X \to X$. For every $x \in X$ there is a unique element $x' \in X$ such that $\pi(x') = x$. The inverse permutation $\pi' : X \to X$ by $\pi^{-1}(x) = x'$ if and only if $\pi(x') = x$. The permutation cipher is also known as Transposition cipher.

Definition 2.2 (Hill cipher [11])**.** *Hill cipher is polygraphic substitution cipher based on linear algebra. Each letter is represented by a number modulo 26. Often the simple scheme $A = 0$, $B = 1, \ldots, Z = 25$. To encrypt a message, each block of n letter is multiplied by an invertible $n \times n$ matrix against modulo 26. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.*

3. Two Symbols Permutation

	*	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
ß(x)	0	4	25	8	1	7	22	5	3	15	12	21	10	16	18	9	13
	Q	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**							
x	17	18	19	20	21	22	23	24	25	26							
ß(x)	20	14	23	17	11	6	19	26	2	24							

Table 1: Permutation and it's inverse table on two symbols

2-Symbol Permutation Algorithm:

1. We take 2×2 non singular matrix(B) as an encryption key.
2. Take any Message. Break the message into two consecutive letters.
3. Assign each character to a single numerical value. And find the image of the corresponding numerical value from the above table.
4. Convert the image value into column matrix as $\begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$
5. The substitution of cipher letter into plaintext, we can express as matrix multiplication $\begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \end{bmatrix} \pmod{27}$ and find the preimage value and corresponding letter for the column matrix from the above table.

2-Symbol Permutation Example

1. Let the key Matrix M= $\begin{bmatrix} 3 & 5 \\ 1 & 6 \end{bmatrix}$
2. Let the plaintext "HELP"

3. $HE = \begin{bmatrix} 3 \\ 7 \end{bmatrix} \implies \begin{bmatrix} 3 & 5 \\ 1 & 6 \end{bmatrix} \begin{bmatrix} 3 \\ 7 \end{bmatrix} \pmod{27} = \begin{bmatrix} 17 \\ 18 \end{bmatrix} \implies TN.$

   $LP = \begin{bmatrix} 10 \\ 13 \end{bmatrix} \implies \begin{bmatrix} 3 & 5 \\ 1 & 6 \end{bmatrix} \begin{bmatrix} 10 \\ 13 \end{bmatrix} \pmod{27} = \begin{bmatrix} 14 \\ 7 \end{bmatrix} \implies RE.$

4. Encrypted Word is "TNRE"

5. For Decryption we use the inverse of key matrix modulo 27 and use inverse Permutation table.

6. The inverse of the key matrix is $M^{-1} = \begin{bmatrix} 15 & 10 \\ 2 & 21 \end{bmatrix}$

7. Now multiplying the inverse matrix with column matrix for the encrypted word.

8. $TN = \begin{bmatrix} 17 \\ 18 \end{bmatrix} \implies \begin{bmatrix} 15 & 10 \\ 2 & 21 \end{bmatrix} \begin{bmatrix} 17 \\ 18 \end{bmatrix} \pmod{27} = \begin{bmatrix} 3 \\ 7 \end{bmatrix} \implies HE$

   $RE = \begin{bmatrix} 14 \\ 7 \end{bmatrix} \implies \begin{bmatrix} 15 & 10 \\ 2 & 21 \end{bmatrix} \begin{bmatrix} 14 \\ 7 \end{bmatrix} \pmod{27} = \begin{bmatrix} 10 \\ 13 \end{bmatrix} \implies LP$

9. The Decrypted Word is "HELP".

4. Three Symbols Permutation

	*	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
ß(x)	1	0	2	3	5	4	8	7	6	11	10	9	12	14	13	17	16
	Q	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**							
x	17	18	19	20	21	22	23	24	25	26							
ß(x)	15	19	18	20	21	23	22	26	25	24							

Table 2: Permutation and it's inverse table on three symbols

3-Symbol Permutation Table Algorithm:

1. We take 3×3 non singular matrix(B) as an encryption key.

2. Take any Message. Break the message into three consecutive letters.

3. Assign each character to a single numerical value. And find the image of the corresponding numerical value from the above table.

4. Convert the image value into column matrix as $\begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix}$

5. The substitution of cipher letter into plaintext, we can express as matrix multiplication $\begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix} \pmod{27}$ and find the cipher text.

3-Symbol Permutation Example:

1. Let the key Matrix N= $\begin{bmatrix} 2 & 5 & 3 \\ 3 & 1 & 2 \\ 1 & 2 & 1 \end{bmatrix}$
2. Let the plaintext "HELLO"
3. $HEL = \begin{bmatrix} 6 \\ 4 \\ 12 \end{bmatrix} \implies \begin{bmatrix} 2 & 5 & 3 \\ 3 & 1 & 2 \\ 1 & 2 & 1 \end{bmatrix} \begin{bmatrix} 6 \\ 4 \\ 12 \end{bmatrix} \pmod{27} = \begin{bmatrix} 14 \\ 19 \\ 26 \end{bmatrix} \implies "MRX"$ Similarly we get $LO* = \begin{bmatrix} 4 \\ 1 \\ 20 \end{bmatrix} \implies "E*T"$
4. Encrypted Word is "MRXE*T"
5. For Decryption we use the inverse of key matrix modulo 27 and use inverse Permutation table.
6. The inverse of the key matrix is N^{-1}= $\begin{bmatrix} 6 & 7 & 22 \\ 20 & 20 & 8 \\ 8 & 7 & 17 \end{bmatrix}$
7. Now multiplying the inverse matrix with column matrix for the encrypted word.
8. We get $MRX = \begin{bmatrix} 6 \\ 4 \\ 12 \end{bmatrix} \implies "HEL"$ and $E*T = \begin{bmatrix} 12 \\ 17 \\ 1 \end{bmatrix} \implies "LO*"$
9. Decrypted Word is "HELLO".

5. Four Symbols Permutation

	*	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
ß(x)	1	0	2	3	5	4	8	7	6	11	10	9	12	14	13	17	16
	Q	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**							
x	17	18	19	20	21	22	23	24	25	26							
ß(x)	15	19	18	20	21	23	22	26	25	24							

Table 3: Permutation and it's inverse table on three symbols

4-Symbol Permutation Algorithm:

1. We take 4×4 non singular matrix(B) as an encryption key.
2. Take any Message. Break the message into four consecutive letters.

3. Assign each character to a single numerical value. And find the image of the corresponding numerical value from the above table.
4. Convert the image value into column matrix as $\begin{bmatrix} p_1 \\ p_2 \\ p_3 \\ p_4 \end{bmatrix}$
5. The substitution of cipher letter into plaintext, we can express as matrix multiplication $\begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{bmatrix} = \begin{bmatrix} b_{11} & b_{12} & b_{13} & b_{14} \\ b_{21} & b_{22} & b_{23} & b_{24} \\ b_{31} & b_{32} & b_{33} & b_{34} \\ b_{41} & b_{42} & b_{43} & b_{44} \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ p_3 \\ p_4 \end{bmatrix} \pmod{27}$ and find the cipher text.

4-Symbol Permutation Example:

1. Let the key Matrix G= $\begin{bmatrix} 2 & 4 & 3 & 2 \\ 3 & 6 & 5 & 2 \\ 2 & 5 & 2 & -3 \\ 4 & 5 & 14 & 14 \end{bmatrix}$
2. Let the plaintext "HELP ME PLEASE"
3. $HELP = \begin{bmatrix} 9 \\ 6 \\ 15 \\ 16 \end{bmatrix} \implies \begin{bmatrix} 2 & 4 & 3 & 2 \\ 3 & 6 & 5 & 2 \\ 2 & 5 & 2 & -3 \\ 4 & 5 & 14 & 14 \end{bmatrix} \begin{bmatrix} 9 \\ 6 \\ 15 \\ 16 \end{bmatrix} \pmod{27} = \begin{bmatrix} 11 \\ 8 \\ 3 \\ 14 \end{bmatrix} \implies "JIBM"$ similarly we get $*ME* = \begin{bmatrix} 24 \\ 11 \\ 0 \\ 10 \end{bmatrix} \implies "ZJAK", PLEA = \begin{bmatrix} 2 \\ 6 \\ 11 \\ 7 \end{bmatrix} \implies "CEJG"$ and $SE** = \begin{bmatrix} 9 \\ 13 \\ 9 \\ 18 \end{bmatrix} \implies "HNHR"$
4. The Encrypted Word is "JIBMZJAKCEJGHNHR"
5. For Decryption we use the inverse of key matrix modulo 27 and use inverse Permutation table.
6. The inverse of the key matrix is G^{-1}= $\begin{bmatrix} -23 & 2 & -2 & -9 \\ 10 & -12 & 16 & 23 \\ 1 & -2 & 12 & 22 \\ 2 & -2 & 6 & 11 \end{bmatrix}$
7. Now multiplying the inverse matrix with column matrix for the encrypted word.

8. We get $JIBM = \begin{bmatrix} 9 \\ 6 \\ 15 \\ 16 \end{bmatrix} \implies \text{“}HELP\text{”}$, $ZJAK = \begin{bmatrix} 1 \\ 14 \\ 6 \\ 1 \end{bmatrix} \implies \text{“}*ME*\text{”}$, $CEJG = \begin{bmatrix} 16 \\ 15 \\ 6 \\ 0 \end{bmatrix} \implies$ $\text{”}PLEA\text{”}$ and $HNHR = \begin{bmatrix} 17 \\ 6 \\ 1 \\ 1 \end{bmatrix} \implies \text{”}SE**\text{”}$
9. The decrypted Word is "HELP ME PLEASE".

6. Conclusion

In this paper, we have developed a cryptographic algorithm involving permutation ciphers. Here, we provide an example for the permutations with 2, 3 and 4 symbols. One can modify this paper by changing the considered permutation or extend the length by more than 4.

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 Q^{p*}*, 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.

[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).