International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-2, December, 2019

Encryption And Decryption of a Message Involving Byte Rotation Technique and Invertible Matrix

Amit Kumar Mandle, Varsha Namdeo

Abstract: ***The aim of this paper is to introduce a new encryption algorithm involving byte rotation and invertible matrix. In the proposed algorithm firstly we apply byte rotation to get an intermediate cipher and then applying the invertible matrix (modulo 27), which gives the final cipher text. Using secret key matrix along with congruence modulo, the message can be encrypted and decrypted perfectly.***

Keywords: Congruence, Byte Rotation Invertible Matrix, Encryption and Decryption.

I. INTRODUCTION

For hiding the information we use cryptography, which is an art of encryption and decryption. Cryptography is a mathematical technique, which is used for information security. It plays vital role in cellular communication viz. ATM Card, transmitting funds, digital signature etc. It is categories into two parts symmetric and asymmetric. When sender and receiver both use the same key for encryption and decryption, then it is known as symmetric cryptography. But in asymmetric cryptography w use two different keys [3, 5].

In this research paper we use byte rotation technique and invertible matrix. Firstly we apply matrix operation under modulo system to get intermediate cipher. After that on applying byte rotation technique on different blocks of plaintext, we obtain the final cipher text. A matrix is invertible if it is non-singular. To encrypt the message the key matrix used and for decrypt the encoded message we use inverse of the matrix under modulo system. The key matrix should be secret between sender and receiver.

A square matrix X is said to be an invertible matrix iff there exist another square matrix Ys.t.XY = YX = I. It may be noted that all the square matrices are not invertible. If a square matrix has an invertible matrix or non-singular, then its determinant value must be non-zero.

Revised Manuscript Received on December 30, 2019.
* Correspondence Author
Amit Kumar Mandle, Research Scholar, Department of Computer Applications (MCA) SRK University, Bhopal, India.
Varsha Namdeo, Associate Professor, Department of Computer Science Engineering, SRK University, Bhopal, India.

II. LITERATURE REVIEW:

Sani Isa [6], Hamed [4], Bhati [1], Bhati [2] and other authors introduced various algorithms for encryption and decryption of a message involving Byte rotation techniques and using of invertible matrix separately time to time. For encryption and decryption there is no single algorithm is sufficient. Therefore researchers worked hard to remove the deficiency and finding better algorithm.

III. METHODOLOGY

To provide sufficient security we use multiple encryption and multilevel encryption system. Here we develop an algorithm model having two steps. Firstly,we apply the secret key matrix along with congruence modulo 27 and obtain an intermediate cipher. Thereafter we apply the byte rotation technique (agree both sender and receiver), to get final cipher text.

For decrypting the message we will use the reverse process of encryption along with byte rotation technique and invertible matrix of congruence modulo 27.

Numerical values for alphabets and some symbols used in the paper given in the following table:

Table – 1

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

IV. ALGORITHM

4.1 Encryption:

1. Take a non-singular square matrix of order 4 as key (say K).
2. Arrange the character/symbol of plain text in a block size of 16 bytes as 4×4 matrix.
3. Convert the alphabet/symbol into their corresponding values using Table1 and call this resultant matrix M.
4. Multiply the key matrix K and plain text matrix M under modulo 27 i.e.

MK (mod 27) = M_1(say)

5. Obtain the transpose of M_1, say M_1^T.
6. Apply the vertical rotation (as per agreement of sender and receiver) on last three columns of M_1^T. Call this resultant matrix C_1.
7. Now apply the horizontal rotation of last three rows of C_1 (as per agreement of sender and receiver). Obtain another matrix say C_2.
8. Convert the numeric values of element of C_2 into alphabets using Table1, we get a cipher text.

4.2 Decryption:

In a reverse process of encryption having following steps:

1. Take the cipher text and arrange it in a square matrix of order 4 of block sized of 16 bytes. After arranging correct them into numeric values using table I, and get a resultant matrix say D_1.
2. Apply the horizontal rotation (same as encryption method) on D_1, we get a matrix say D_2.
3. Now applying the vertical rotation (same as encryption method) on D_2, we get a matrix say D_3.
4. Obtain the transpose of D_3, say D_4.
5. Now calculate $D_4\, k^{-1}$ (mod 27) = M (say)
6. Convert the element of M into alphabet/symbol using Table I and arrange them row wise we get a plain text.

ILLUSTRATION:

Encryption Steps:

1. Consider a non-singular key matrix of order 4 × 4 as follows:

$$K = \begin{bmatrix} 2 & 1 & 2 & 1 \\ 3 & 5 & 2 & 2 \\ 5 & 1 & 3 & 1 \\ 3 & 1 & 3 & 2 \end{bmatrix}$$

2. Let plain text is

SYMMETRIC CIPHER

Arrange them in a block size of 16 bytes i.e. 4 × 4 matrix, we get

$$\begin{bmatrix} S & Y & M & M \\ E & T & R & I \\ C & 0 & C & I \\ P & H & E & R \end{bmatrix}$$

3. In the above block matrix substitute numeric values of letters, as follows:

$$M = \begin{bmatrix} 19 & 25 & 13 & 13 \\ 5 & 20 & 18 & 9 \\ 3 & 0 & 3 & 9 \\ 16 & 8 & 5 & 18 \end{bmatrix}$$

4. Multiply the key matrix and text matrix M under modulo system, we get the following Multiplicative matrix

M_1 = MK (mod 27)

$$= \begin{bmatrix} 19 & 25 & 13 & 13 \\ 5 & 20 & 18 & 9 \\ 3 & 0 & 3 & 9 \\ 16 & 8 & 5 & 18 \end{bmatrix} \begin{bmatrix} 2 & 1 & 2 & 1 \\ 3 & 5 & 2 & 2 \\ 5 & 1 & 3 & 1 \\ 3 & 1 & 3 & 2 \end{bmatrix} \text{(mod 27)}$$

$$= \begin{bmatrix} 1 & 8 & 4 & 0 \\ 25 & 25 & 23 & 0 \\ 21 & 15 & 15 & 24 \\ 0 & 25 & 9 & 19 \end{bmatrix}$$

5. Obtain the transpose of M_1, we get

$$M_1^T = \begin{bmatrix} 1 & 25 & 21 & 0 \\ 8 & 25 & 15 & 25 \\ 4 & 23 & 15 & 9 \\ 0 & 0 & 24 & 19 \end{bmatrix}$$

6. Now apply the vertical rotation on last three columns. M_1^T such that rotate three bytes from 2nd column, rotate two bytes from 3rdcolumn, rotate one byte from 4thcolumn and 1stcolumn unchanged. Denote the resultant matrix by C1, we get

$$C_1 = \begin{bmatrix} 1 & 0 & 15 & 25 \\ 8 & 25 & 24 & 9 \\ 4 & 24 & 21 & 19 \\ 0 & 23 & 15 & 0 \end{bmatrix}$$

7. Applying the horizontal rotation on last three rows of C_1 such that rotate three bytes from 2nd row, rotate two bytes from 3rd row, rotate one byte from 4th row and 1st row remains unchanged. Denote the resultant matrix by C_2, we get –

$$C2 = \begin{bmatrix} 1 & 0 & 15 & 25 \\ 25 & 24 & 9 & 8 \\ 21 & 19 & 4 & 24 \\ 23 & 15 & 0 & 0 \end{bmatrix}$$

8. Convert the numeric values of C2 into their corresponding alphabet letters using table1, we get the following cipher text block

$$C_3 = \begin{bmatrix} A & 0 & O & Y \\ Y & X & I & H \\ U & S & D & X \\ W & O & 0 & 0 \end{bmatrix}$$

Therefore cipher text is

A0OYYXIHUSDXWO00

Decryption Steps:

1. Consider the cipher text
   A0OYYXIHUSDXWO00
2. Arrange it in block size of 16 bytes i.e. 4×4 matrix and convert them into their corresponding numeric value using Table1, we get –

$$\begin{bmatrix} 1 & 0 & 15 & 25 \\ 25 & 24 & 9 & 8 \\ 21 & 19 & 4 & 24 \\ 23 & 15 & 0 & 0 \end{bmatrix} = D_1(\text{say})$$

3. Applying the horizontal rotation on last three rows of D_1s.t.rotate three bytes from 2nd row, rotate two bytes from 3rd row rotate one byte from 4th row and 1st row remains unchanged, we get –

$$\begin{bmatrix} 1 & 0 & 15 & 25 \\ 8 & 25 & 24 & 9 \\ 4 & 24 & 21 & 19 \\ 0 & 23 & 15 & 0 \end{bmatrix} = D_2(\text{say})$$

4. Now apply the vertical rotation on last three columns of D_2s.t. rotate three bytes from 2nd column, rotate two bytes from 3rd column, rotate one byte from 4th column and 1st column remains unchanged, we get –

$$\begin{bmatrix} 1 & 25 & 21 & 0 \\ 8 & 24 & 15 & 25 \\ 4 & 23 & 15 & 9 \\ 0 & 0 & 24 & 19 \end{bmatrix} = D_3(\text{say})$$

5. Obtain the transpose of D_3, we get –

$$\begin{bmatrix} 1 & 8 & 4 & 0 \\ 25 & 24 & 23 & 0 \\ 21 & 15 & 15 & 24 \\ 0 & 25 & 9 & 19 \end{bmatrix} = D_4(\text{say})$$

6. Now calculate –

$D_4K^{-1} \pmod{27} = M$ (says)

$$\Rightarrow M = \begin{bmatrix} 1 & 8 & 4 & 0 \\ 25 & 24 & 23 & 0 \\ 21 & 15 & 15 & 24 \\ 0 & 25 & 9 & 19 \end{bmatrix} \begin{bmatrix} 16 & 5 & 25 & 15 \\ 8 & 10 & 22 & 2 \\ 5 & 12 & 7 & 9 \\ 5 & 10 & 22 & 4 \end{bmatrix} \pmod{27}$$

$$= \begin{bmatrix} 19 & 25 & 13 & 13 \\ 5 & 20 & 18 & 9 \\ 3 & 0 & 3 & 9 \\ 16 & 8 & 5 & 18 \end{bmatrix}$$

7. Convert the above matrix into their corresponding alphabet/symbol using Table1, we get a matrix of order 4×4 of block size 16 as follows:

$$\begin{bmatrix} S & Y & M & M \\ E & T & R & I \\ C & o & C & I \\ P & H & E & R \end{bmatrix}$$

8. Arrange them in row wise we get the original plain text as –

SYMMETRIC CIPHER

V. RESULT AND DISCUSSION

In order to encrypt and decrypt a message, in this paper we used invertible key matrix congruent modulo 27. To keep the information secure from others (except receiver) mathematical relations have been logically implemented. Among the other cryptographic technique using of matrices, is the strongest method since it uses mathematical logics.

Due to the chosen byte rotation technique along with invertible key matrix congruent modulo 27, it is very difficult to extract the original information. Due to key size (16 bytes) brute force attack is also difficult. Explanation of result is as follows:

SN	Name of attack	Opportunity of attack	Explanation
1	Cipher text attack	Very Difficult	Due to the chosen Byte rotation technique and invertible key matrix(size is 16 bytes) congruent modulo 27
2	Chosen cipher text attack	Very Difficult	Due to the chosen Byte rotation technique and invertible key matrix(size is 16 bytes) congruent modulo 27
3	Adaptive chosen cipher text attack	Very Difficult	Due to the chosen Byte rotation technique and invertible key matrix(size is 16 bytes) congruent modulo 27
4	Known plain text attack	Difficult	Due to the chosen Byte rotation technique and invertible key matrix (size is 16 bytes) congruent modulo 27
5	Chosen plain text attack	Difficult	Due to the chosen Byte rotation technique and invertible key matrix (size is 16 bytes) congruent modulo 27
6	Adaptive chosen plain text attack	Difficult	Due to the chosen Byte rotation technique and invertible key matrix of 16 bytes

VI. CONCLUSION

Since in this paper, we use the byte rotation technique and invertible matrix. Therefore the proposed algorithm in this paper arise the strong security system and produced cipher text cannot be broken easily.

It is also generate the double encryption system, firstly from invertible matrix and secondly, from byte rotation technique. Using the above method the information could be sent and received safely. Without key matrix and congruence relations the message could not decrypt.

REFERENCES

1. BhatiSunita and Sharma S.K.: Block wise parallel encryption through multithreading Concept, Aishwarya Research Communication Journal, Vol.3, 2011, pp. 101-106.
2. BhatiSunita, Bhati Anita and Sharma S.K.: A new approach towards Encryption Schemes: Byte-Rotation Encryption Algorithm, Proceedings of the Word Congress on Engineering and Computer Science, 2012, Vol.11, pp. 1-4.
3. ForouzanBehrouz A.: Cryptography & Network Security, McGraw Hill Education, 2007.
4. HamedAbdulaziz B.M. and Albudawe Ibrahim O.A.: Encrypt and Decrypt Message Using Invertible Matrices Modulo 27, AJER, Vol.6, Issue 6, 2017, pp. 212-217.
5. KahateAtul: Cryptography and Network Security, Tata McGraw Hill, New Delhi, 2008.
6. Soni Isa and Abdulaziz B.M. Hamed: Cryptography Using Congruence Modulo Relations, American Journal of Engineering Research, Vol.6, Issue 3, 2017 pp. 156-160.

AUTHORS PROFILE

Amit Kumar Mandle is a Research Scholar in the Department of Computer Applications (MCA) at SRK University, Bhopal, India. He completed his Master in Computer Application from MPBOU, Bhopal (M.P.) in 2006.

Varsha Namdeo is an Associate Professor in the Department of Computer Science and Engineering at SRK University, Bhopal, India. She is a teacher and researcher in the field of computer science and information technology. She earned her Master in Computer Application from Barkatullah University Bhopal (M.P.) in 2000 and in Computer Science and Engineering from Barkatullah University Bhopal (M.P.) in 2009 and PhD degree from Maulana Azad National Institute of Technology; Bhopal (M.P.) in 2015.She had a long career in teaching and research.