ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **9** (2020), no.7, 4751–4759
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.7.41

MODULAR INVERSE BASED SECURED DATA TRANSMISSION BY THE APPLICATION OF GRAPH THEORY

S. NANDHINI, A. MANIMARAN[1], SADHU NARAYANA NAIDU,
AND MALLELA NIKHIL CHAKRAVARTHY

ABSTRACT. Data communication is inevitable in current world of networking and transformation of data securely through the channels is a challenging task due to various threats. This paper presents an efficient cryptographic algorithm for the messages sent across the channels. A graph theoretic approach is implemented for the encryption and decryption process. Messages are converted into graphs and adjacency matrix of the graphs are used for encryption and decryption process. The key which has to be transmitted along with the encrypted message is also encrypted using modular inverse. Then the encrypted message is again converted to a matrix for decryption to get the original message

1. INTRODUCTION

Cryptography is a process of sending messages from a sender to a receiver through communication channels in a secured way without loss of data. Data security plays a vital role in communication process. Acharya [1] in 2020, described the idea of efficient public key multi-channel broadcast for effective and more secure encryption. In 2018, Alvarez [2] proposed two optimized alternatives that enhance the performance of a Password-based key derivation functions which are commonly used to transform user passwords into keys for symmetric

[1]*corresponding author*

2010 *Mathematics Subject Classification.* 94A60, 68P25.

Key words and phrases. Encryption, Decryption, Modular Inverse, Rail Fence Cipher, Complete Graph.

encryption, for user authentication, password hashing and preventing attacks based on custom hardware. Amudha et al. [3] described the idea of encryption and decryption based on graph and XORed in 2018. Bala et al. [4] dealt the idea of sharing the information by using spanning trees with labelled sequence for encryption and decryption in 2019 and in the same year, Domosi et al. [5] described the idea of a cryptographic system with a class of Binary Error-Correcting Codes. For security purpose in optical encryption to avoid various attacks the authors Dou et al. [6] introduced optical nonlinear cryptosystem based on double random phase encoding in 2020. Lau and Tan [7] proposed a new rank metric code-based encryption based on the hard problem of rank syndrome decoding problem by considering a generator matrix in 2019. It is invoked that the idea of encrypting data in a complex way and for decrypting the same [8] without any hacking through complete bipartite graph by assigning some weights to the edges. Nandhini et al. [9] proposed an algorithmic measure in connection with the queuing model to find the fastest route between the given two nodes. Phan et al. [10] introduced the idea of adaptive CCA broadcast encryption with constant size secret keys and cipher texts in 2013. Saudy et al. [11] has discussed the fault detection scheme in the Elliptic Curve Cryptography with the ability to perform with increased protection and reliability in the year 2019. The idea of the conservative labelling [12] is introduced in terms of fuzziness and it it explored in 2018. Yamuna et al. [13] explored the technique of double encryption using the Hamiltonian path and complete graph with matrix method.

2. METHODOLOGY

Let n be the length of the message. A code is assigned to each character of the message by the following procedure. Here we assume that the message contains upper case letters, numerical values and a dot.

TABLE 1. Code Assignment

Character:	A	B	C	$\cdots$	Z	0	1	2	$\cdots$	9	$\bullet$
Code Assigned:	1	2	3	$\cdots$	26	27	28	29	$\cdots$	36	37

2.1. **Encryption Algorithm.**

Step 1: A graph G with $n+1$ vertices is formed. Assign the codes of each character as in Table 1 in the original message as the weight of edges of graph G. An adjacency Matrix say E_1 is formed for the graph $G_{(n+1)\times(n+1)}$. Matrix E_1 represents the original message.

Step 2: Form a complete graph K_p with $p = n + 1$ vertices from G, by assigning pseudo weights for the remaining edges. Form an adjacency Matrix say E_2 for the graph K_p.

Step 3: Form the matrix, $E_3 = E_2 + I$, where I is the identity matrix of order $p \times p$.

Step 4: Form the matrix E_4 which is the Modular Inverse of E_3. Matrix E_4 is the encryption code of the original message which will be sent to the receiver.

Step 5: Let $A_1 = [a_{ij}]$ be the key matrix of order $p \times p$. Find the matrix A_2 = Modular Inverse of A_1. Let $B = E_1 * E_3$ and $E_5 = B * A_1$, which is of order $p \times p$.

Step 6: The subsequent process is used to form the matrix E_6 of order $p \times (p + 1)$ and the remaining elements are allocated with dummy values.

$k = n + 2$
$x = 1$
$for(x = 1\ to\ n)$
    $z = x$
    $for(i = 1\ to\ x)$
        $a_{x,k-z} = a_{x+1,i}$
        $z = z - 1$
    $next\ i$
    $i = 1$
    $for(j = 1\ to\ n - i)$
        $a_{i+1,j} = a_{i+1,j+1}$
    $next\ j$
$next\ x$

Step 7: Form the matrix E_7 and E_8 by shifting row and mix columns as per the following procedure:

Zeroth row zero shift, first row one circular left shift, second row two circular left shifts $\cdots$ p^{th} row p circular left shifts. Mix columns zeroth and $(p+1)^{th}$columns zero circular upper shifts, first column one upper circular shif $\cdots$ p^{th} column p circular upper shifts. E_8 and E_4 represents the encrypted message and the characters are mixed up using $Rail\ Fence\ Cipher$ technology with two rows and sent to the receiver along with the information about the order of original matrix represented as p.

TABLE 2. Rail Fence Cipher

1		a_{11}		a_{13}		$\cdots$		a_{21}		$\cdots$	
	n		a_{12}		a_{14}		a_{1n}		a_{22}		a_{np}

The encrypted message of A_2 contains the information about the key which is sent along with E_8 and E_4 using $Rail\ Fence\ Cipher$ method along with the information about the order of key matrix as per Table 2.

2.2. **Decryption Algorithm.**

Step 1: Obtain the Matrix D_5 from the encrypted matrix E_8 by mixing columns, shifting rows and converting $p \times (p+1)$ to $p \times p$ matrix.
Step 2: Find Modular Inverse of the matrix A_2 to get the key matrix A_1.
Step 3: Get the matrix $E_3 = Modular\ Inverse\ (ModularInverse\,(D_5 * Inverse\,(A_1)))$.
Step 4: Find inverse of the matrix E_3. Then the obtained original matrix is $E_1 = E_4 * inverse(E_3)$.

3. MATHEMATICAL ILLUSTRATION

The proposed algorithm is implemented by assuming the original message as ***INDIA*** for encryption and decryption. From the Table 1, the word ***INDIA*** is encrypted with numbers as 9, 14, 4, 9, 1. Assign the encrypted numbers as the weights for the edges of the graph which is given in Figure 1.
For the graph in Figure 1, the adjacency matrix E_1 is given by

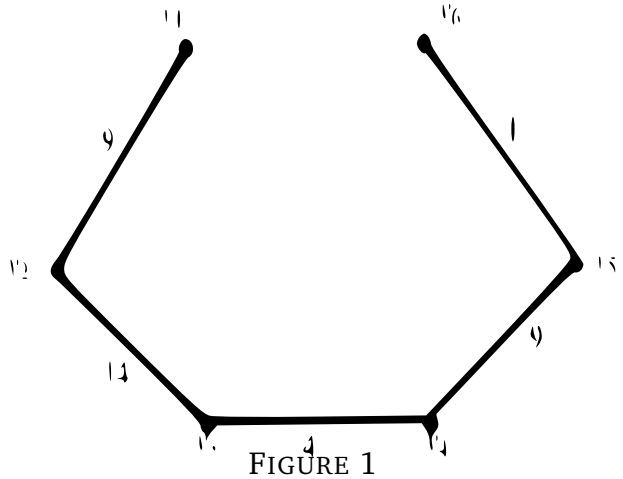

FIGURE 1

$$E_1 = \begin{pmatrix} 0 & 9 & 0 & 0 & 0 & 0 \\ 9 & 0 & 14 & 0 & 0 & 0 \\ 0 & 14 & 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 & 9 & 0 \\ 0 & 0 & 0 & 9 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Then by assigning some random weights construct the complete graph as in Figure 2 with same number of vertices of Figure 1

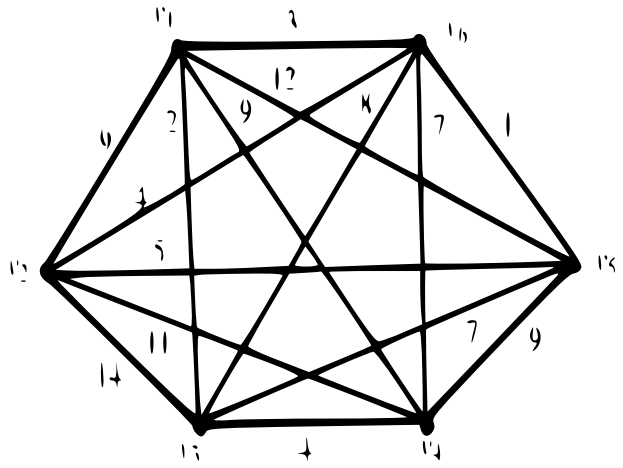

FIGURE 2

and the adjacency matrix for the complete graph in Figure 2 is given by,

$$E_2 = \begin{pmatrix} 0 & 9 & 2 & 9 & 12 & 3 \\ 9 & 0 & 14 & 11 & 5 & 4 \\ 2 & 14 & 0 & 4 & 7 & 8 \\ 9 & 11 & 4 & 0 & 9 & 7 \\ 12 & 5 & 7 & 9 & 0 & 1 \\ 3 & 4 & 8 & 7 & 1 & 0 \end{pmatrix}$$

Let the original key matrix is A_1 and the encrypted key matrix is A_2. We have

$$A_1 = \begin{pmatrix} 1 & 2 & 5 & 9 & 7 & 11 \\ 13 & 2 & 4 & 3 & 9 & 6 \\ 4 & 5 & 13 & 19 & 23 & 4 \\ 15 & 11 & 6 & 2 & 3 & 1 \\ 5 & 4 & 8 & 2 & 4 & 12 \\ 2 & 1 & 4 & 6 & 2 & 1 \end{pmatrix} \text{ and } \mathrm{A}_2 = \begin{pmatrix} 1 & 19 & 15 & 33 & 16 & 27 \\ 20 & 19 & 28 & 25 & 33 & 31 \\ 28 & 15 & 20 & 2 & 29 & 28 \\ 5 & 25 & 31 & 19 & 25 & 1 \\ 15 & 28 & 14 & 19 & 28 & 34 \\ 19 & 1 & 28 & 31 & 19 & 1 \end{pmatrix}$$

After applying the encryption algorithm, the encrypted matrix is given by,

$$\begin{pmatrix} 2484 & 3292 & 3419 & 2481 & 2782 & 40 & 7129 \\ 4735 & 4492 & 2412 & 3031 & 150 & 2124 & 3258 \\ 7598 & 1162 & 323 & 200 & 4095 & 3746 & 6692 \\ 2377 & 282 & 212 & 3654 & 4835 & 5930 & 2732 \\ 237 & 190 & 3177 & 4945 & 2897 & 3783 & 173 \\ 90 & 2115 & 5001 & 2025 & 3134 & 247 & 60 \end{pmatrix}$$

Now the encrypted matrix will be sent to the receiver as a *Rail Fence Cipher* which is given below,

TABLE 3. Encrypted Rail Fence Cipher - 1

1		2484		3419		2782		7129		4492		3031		2124		7598	
	6		3292		2481		40		4735		2412		150		3258		1162

323		4095		6692		282		3654		5930		237		3177		2897	
	200		3746		2377		212		4835		2732		190		4945		3783

173		2115		2025		247	
	90		5001		3134		60

TABLE 4. Encrypted Rail Fence Cipher - 2

1		19		34		33		8		15		19		1		16		33		28		33		34	
	33		33		25		1		27		28		8		28		14		27		1		16		15

16		1		25		14		1	
	33		1		28		16		1

TABLE 5. Encrypted Rail Fence Cipher - 3

1		15		16		20		28		33		28		20		29		5		31		25		15	
	19		33		27		19		25		31		15		2		28		25		19		1		28

14		28		19		28		19	
	19		34		1		31		1

After applying the decryption algorithm on A_2 we will obtain the original key matrix A_1 and the matrix for the original message as E_1 respectively.

$$A_1 = \begin{pmatrix} 1 & 2 & 5 & 9 & 7 & 11 \\ 13 & 2 & 4 & 3 & 9 & 6 \\ 4 & 5 & 13 & 19 & 23 & 4 \\ 15 & 11 & 6 & 2 & 3 & 1 \\ 5 & 4 & 8 & 2 & 4 & 12 \\ 2 & 1 & 4 & 6 & 2 & 1 \end{pmatrix} \text{and } \mathrm{E}_1 = \begin{pmatrix} 0 & 9 & 0 & 0 & 0 & 0 \\ 9 & 0 & 14 & 0 & 0 & 0 \\ 0 & 14 & 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 & 9 & 0 \\ 0 & 0 & 0 & 9 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

which gives the decrypted data as 9, 14, 4, 9, 1 and as per the Table 1 the decrypted message is ***INDIA***.

4. CONCLUDING REMARKS

The proposed encryption algorithm provides secure data transmission. In this method of data transmission, the data is been encrypted using the application of the complete graph and modular multiplication inverse which makes the algorithm more secured. The implementation of the various codes and assignee values makes it very difficult and arbitrary for the decryption. As the algorithm requires the corpus (Dictionary of the assigned characters and values) to decrypt, which makes the system more complex and difficult to retrieve the data

easily. As discussed in the above algorithm's methodology, the random weights included in the algorithm adds another layer of arbitration to the algorithm.

REFERENCES

[1] K. ACHARYA: *Secure and efficient public key multi-channel broadcast encryption schemes*, Journal of Information Security and Applications, **51** (2020), 102436.

[2] R. ALVAREZ, A. ANDRADE, A. ZAMORA: *Optimizing a Password Hashing Function with Hardware-Accelerated Symmetric Encryption*, Symmetry, **10**(12) (2018), 1 – 11.

[3] P. AMUDHA, A. C. SAGAYARAJ, A. S. SHEELA: *An Application of Graph Theory in Cryptography*, International Journal of Pure and Applied Mathematics, **119**(13) (2018), 375 – 383.

[4] P. BALA MANOJ KUMAR, K. SAI TEJA, A. MANIMARAN, G. DEEPA, B. PRABA: *Information Sharing by Spanning Trees of a Graph by labelled sequence as a key*, International Journal of Recent Technology and Engineering, **8**(3) (2019), 3498 – 3503.

[5] P. DOMOSI, C. HANNUSCH, G. HORVATH: *A cryptographic system based on a new class of binary error – correcting codes*, Tatra Mountains Mathematical Publications, **73**(1) (2019), 83 – 96.

[6] S. DOU, X. SHEN, C. LIN: *Security-enhanced optical nonlinear cryptosystem based on double random phase encoding*, Optics and Laser Technology, **123** (2020), 105897.

[7] T. S. C. LAU, C. H. TAN: *New rank codes based encryption scheme using partial circulant matrices*, Designs, Codes and Cryptography, **87**(12) (2019), 2979 – 2999.

[8] A. MANIMARAN, B. PRABA, V. M. CHANDRASEKARAN, G. KAILASH: *Data Transfer Using Complete Bipartite Graph*, IOP Conference Series: Materials Science and Engineering, **263**(4-3) (2017), 1 – 6.

[9] S. NANDHINI, S. SHAJITHA BEGUM, M. S. SANJAY: *Routing Algorithm for Fastest Path - a Queuing Approach*, International Journal of Engineering and Technology, **7**(4.10) (2018), 753 – 754.

[10] D. H. PHAN, D. POINTCHEVAL, S. F. SHAHANDASHTI, M. STREFLER: *Adaptive CCA broadcast encryption with constant-size secret keys and ciphertexts*, International Journal of Information Security, **12**(4) (2013), 251 – 265.

[11] N. F. SAUDY, I. A. ALI, R. AL BARKOUKY: *Error analysis and detection procedures for elliptic curve cryptography*, Ain Shams Engineering Journal, **10**(3) (2019), 587 – 597.

[12] S. SHAJITHA BEGUM, S. NANDHINI: *Fuzzy Conservative and Fuzzy Strongly Conservative Labeling*, International Journal of Civil Engineering and Technology (IJCIET), **9**(13) (2018), 859 – 863.

[13] M. YAMUNA, M. GOGIA, A. SIKKA, M. J. H. KHAN: *Encryption using graph theory and linear algebra*, International Journal of Computer Application, **5** (2) (2012), 102 – 107.

Department of Mathematics
School of Advanced Sciences
Vellore Institute of Technology
Vellore, Tamil Nadu, India - 632014
E-mail address: nandhini.s@vit.ac.in

Department of Mathematics
School of Advanced Sciences
Vellore Institute of Technology
Vellore, Tamil Nadu, India - 632014
E-mail address: marans2011@gmail.com

School of Information Technology and Engineering
Vellore Institute of Technology
Vellore, Tamil Nadu, India - 632014
E-mail address: narayananaidu1998.10@gmail.com

School of Information Technology and Engineering
Vellore Institute of Technology
Vellore, Tamil Nadu, India - 632014
E-mail address: nikhilchakravarthy.mallela@gmail.com