JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 1821-1826
https://publishoa.com
ISSN: 1309-3452

An Encryption Technique Using A Complete Graph With A Self-Invertible Matrix

[1] P. Mohan, [2] Dr. K. Rajendran, [3] Dr. A. Rajesh,

[1]Research Scholar, Department of Mathematics, VISTAS, India.
[1]mohan14palani@gmail.com, mohan.phd@velsuniv.ac.in
[2] Assistant Professor, Department of Mathematics, VISTAS, India,
[2] gkrajendra59@gmail.com,
[3] Associate Professor, Department of CSE, VISTAS, India, [3] arajesh.se@velsuniv.ac.in

Received 2022 April 02**; Revised** 2022 May 20**; Accepted** 2022 June 18**.**

ABSTRACT:

Nowadays, the process of message encryption is the most important thing to secure our messages and communication between people. Message encryption methods are rapidly increasing currently due to the growth and evolution of the internet and network communications. Sharing information, personal messages, images, or data from one person to another over unsecured channels opens the door for attack, or hacking. To reduce this terminology and to provide better security, cryptographic or encryption techniques play an essential role. We have many kinds of symmetric enciphering techniques like the Caesar Cipher, Atbash Cipher, Hill Cipher, etc., In this paper, we are going to give the enciphering technique with the help of a complete graph, an adjacency matrix, and a generated self-invertible key matrix to encrypt and decrypt the given messages to produce a complicated ciphertext. Since we are using the self-invertible matrix as a key matrix, the inverse of this key matrix is always existing, and while we are decrypting the ciphertext, we do not need to compute the inverse of the key matrix. It helps us to reduce the computational complexity involved in the process of finding the inverse of a key matrix.

Key Words: Graph theory Encryption, Hill Cipher, Hamiltonian Path, Complete graph, Adjacency Matrix, Matrix encryption, Self-Invertible Matrix.

1. Introduction

Cryptography is one of the important mathematical techniques that help us protect our data, messages, and images from hackers and increase the security of the transferred data. Cryptography is the process of converting original messages or plaintext into an unreadable, unrecognizable form so that only the deliberate recipients can remove the disguised form and read the original plaintext message. The hackers or intermediates do not identify the data. The message we are sending is known as plain text, and the unrecognizable form of the message is called encrypted text or ciphertext. Although both plain text and ciphertext are written in the form of alphabets. In certain cases, the messages are written in the form of some special characters like punctuation marks, numerals, and blanks or any other special characters to reduce the possibility of hacking or stealing the information. Usually, the given plain texts are encoded using the following encoded table.

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
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	26

Table 1.0. Encoded Table

The process of converting a given plaintext message units into an unrecognizable form is known as encryption or enciphering, decryption or deciphering is nothing but the reverse process of enciphering that is the process of converting ciphertext into an original message. This transformation from plaintext to ciphertext is a mapping or a function sometimes

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 1821-1826
https://publishoa.com
ISSN: 1309-3452

it may call as trapdoor function $h: \mathcal{M} \to \mathcal{C}$, where $\mathcal{M}$ is known as the collection of all possible plaintext message units and $\mathcal{C}$ is known as the collection of all possible ciphertext message units. This function h is basically a $1-1$ function. That is the conversion is unique, for every plaintext message unit there is only one ciphertext message unit for the encryption process, while the reverse process, that is decryption is a map h^{-1} which helps in the process of finding plaintext from ciphertext ($h^{-1}: \mathcal{C} \to \mathcal{M}$).

In a cryptography a **key** is the variable quantity or parameter which help us to convert the plain text original message units into ciphertext message units and vice versa. The length of the key is an element which considering how difficult the process of decryption to get the original message. Since we are having two kind of cryptography techniques, they are private key cryptography or **symmetric key cryptography** (both the users the sender as well as the receiver should use the unique key for both encryption and decryption) and public key cryptography or **asymmetric key cryptography** (the private and public both the keys are used in the process of encryption and decryption) the public key cryptosystem is sometimes called as one way function or **trap door** function this means that it is easy to compute in one direction but it is extremely too difficult to compute the other direction.

Hill Cipher is one among the most important symmetric key cryptography techniques, here the processes of encryption and decryption is done by using matrices and its inverse, some operations of matrices, also the key matrix for both the process are same that is the sender and receiver both should use the same key matrix for encryption and decryption (here we need to find the inverse for the key matrix while decrypting the ciphertext). It is easy to break once the intentional people who knows the technique, also it has difficulty for sharing the common key matrix over any kind of channels. In order to reduce this terminology and to provide more security we are proposed the new technique that uses adjacency matrix and for the key matrix the self-invertible matrix was used for both encryption and decryption.

The technique that has been proposed in this paper is by using the concept of a complete graph of a Hamiltonian path and a corresponding adjacency matrix. The self-invertible key matrix is used here as the key to encrypt and decrypt the given original message units to strengthen the security and produce a new and effective approach. Since in this approach we are using a self-invertible key matrix as the key matrix, we do not need to compute the inverse of the key matrix while performing the decryption process. This approach is made by first the sender should draw the path of n vertices, n being the number of letters in the plaintext, starting from the vertex 1. This adjacency matrix can be multiplied with the generated self-invertible key matrix and sent to the receiver over an unsecured channel. So, it is too difficult to retrieve the original message unless the intermediates know this approach. The rest of this paper is defined as follows: In Section 2, we discussed some preliminary aspects of graph theory; in Section 3, we discussed the generating procedure of a self-invertible key matrix. Section 4 explains the proposed approach. The implementation example will be given in Section 5. Finally, the conclusion and future works are given in Section 6.

2. Preliminaries of Graph Theory

Graph: A graph is simply a collection of vertices and edges (or) a Graph G is an ordered pair(V,E), where V is its vertices and E be the edges.

Directed/Undirected Graphs: In an undirected graph every edges as a set of vertices, an edge a, b is going to be the set ab, so it connects {a, b} this is same as the set {b, a} they both are same, there is no direction for the graphs and order does not matter for a graph. For directed graph the directions and order of the graphs are important.

Path: A path is a walk with no repeated vertices., If a graph is connected then there is a a-b path for all a, b in V.

Hamiltonian Path: A connected graph G contains an open walk that visits every vertices of a given graph G exactly once is called Hamiltonian path.

Adjacency Matrix: The matrix which is based on the adjacency of vertices of a given graph. The adjacency matrix is a $n \times n$ matrix, where n is the number of vertices of graph.

$$P = \{p_{ij}\} = \begin{cases} 1, & \text{if there is an edge between vertex} \\ 0, & \text{otherwise} \end{cases}$$

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 1821-1826
https://publishoa.com
ISSN: 1309-3452

3. Generation of self-invertible key matrix

A matrix M is said to be self-invertible matrix if $M = M^{-1}$, that is $M \cdot M^{-1} = M^{-1} \cdot M = I$, the self-invertible matrix was generated by using the following procedure, consider any arbitrary $\frac{n}{2} \times \frac{n}{2}$ matrix M_{22} (since n being the order of adjacency matrix) with the help of M_{22} we can compute the remaining $\frac{n}{2} \times \frac{n}{2}$ matrices using the following properties,

$$M_{11} + M_{22} = 0, \quad M_{12} = I - M_{22}, \qquad M_{21} = I + M_{22}$$

After computing $M_{11}, M_{12}, M_{21}, M_{22}$ the self-invertible matrix M was created by

$$M = \begin{bmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{bmatrix} = \left[\begin{array}{cccc:ccc} m_{11} & m_{12} & \cdots & \cdots & m_{1n} \\ m_{21} & m_{22} & \cdots & \cdots & m_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \hdashline \cdots & \cdots & \cdots & \cdots & \cdots \\ m_{n1} & m_{n2} & \cdots & \cdots & m_{nn} \end{array}\right]$$

4. The proposed cryptosystem

This section explained the proposed approach of using the Hamiltonian path of an undirected graph, the complete graph of this Hamiltonian path, and the corresponding adjacency matrix with the self-invertible key matrix

Complete graph-based encryption algorithm:

The given plain text message is converted into their numerical equivalent values with the help of encoded table that is using Table1.0, these numerical equivalent values are put into the edges of an undirected graph (i.e.,) these values are put into the edges of the path, known as weights of the path. Construct a path with n-vertices (n represents the number of plaintext units) begins with the vertex 1, this path is made by connecting the sequential letters in the given plain text message unit, convert this weight assigned path into a Hamiltonian path by connecting dummy edges, and then connects every vertices by drawing edges between each vertices to make the graph into a complete, a false weights was given to the newly created edges and then the adjacency matrix for this corresponding complete graph was computed. For the key matrix, we are generating a self-invertible key matrix of even order, after generating self-invertible key matrix multiply it with the adjacency matrix, the final matrix is the encrypted data for the original message units, finally this encrypted matrix shared to other user over an unsecure channel, these values are shared either in the form of row wise or column wise also represent the number of vertices, order of a adjacency matrix, $\frac{n}{2} \times \frac{n}{2}$ matrix which help us to generate a required self-invertible key matrix. i.e., I, n, <Adjacency matrix> <$\frac{n}{2} \times \frac{n}{2}$ matrix>, here I is known as the index value of the given graph, n be the size of matrix.

Complete graph-based decryption algorithm:

With the help of received data the receiver is able to find the index value, order of the adjacency matrix, the receiver separates the matrices, and with the help of $\frac{n}{2} \times \frac{n}{2}$ matrix the receiver is also generating the self-invertible key matrix using the procedures which are explained in Section 3, then the given encrypted matrix can be multiplied with the generated self-invertible key matrix the receiver is able to get the adjacency matrix, tracing back the graph with the help of the resultant adjacency matrix and write the edge wights of the graph from the given index value, decode these values with their numerical equivalent values using Table 1.0. Then finally the receiver is able to read the original message.

5. Implementation example:

Suppose that User A(sender) wants to send the message “KEY” to User B(receiver) using the technique which explained in Section 3, assuming that both the users should know the encryption and decryption techniques of the given procedure.

Encryption- User A (The sender): Encryption is done by the following steps

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 1821-1826
https://publishoa.com
ISSN: 1309-3452

Step1: Firstly, the sender converts the given message units" KEY" into their numerical equivalent values that is using Table 1.0 $K \to 11,\ \ E \to 5,\ \ Y \to 25.$

Step2: Draw a path which begins from the index value 1, label the above mentioned numerical equivalent values as the edges of this path, these vertices are connected by sequential letters.

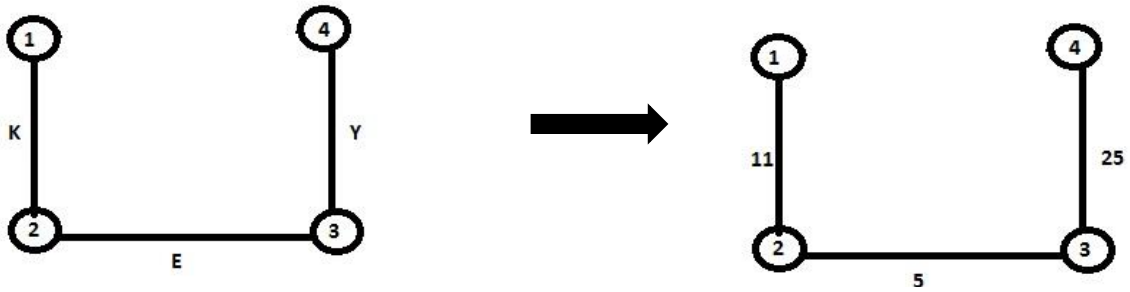


Figure1.0. The path for given plain text message

Step3: The Hamiltonian path was constructed with false edge weight

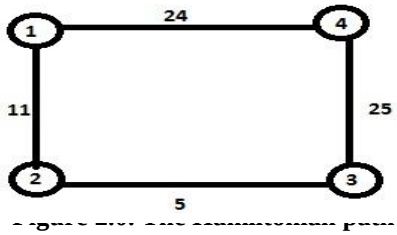


Figure 2.0. The Hamiltonian path

Step4: Connecting all the edges to make the given graph into a complete graph

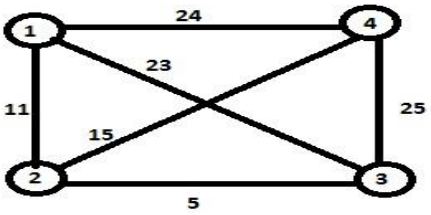


Figure 3.0. Complete graph

Step5: Compute the adjacency matrix for the above Complete graph and denote it as 'P'

$$P = \begin{bmatrix} 0 & 11 & 23 & 24 \\ 11 & 0 & 5 & 15 \\ 23 & 5 & 0 & 25 \\ 24 & 15 & 25 & 0 \end{bmatrix}$$

Step6: Now we need to compute the key matrix for that purpose we construct the self-invertible key matrix 'M' with the help of $\frac{n}{2}$ matrix M_{22}.

Let $M_{22} = \begin{bmatrix} 25 & 5 \\ 19 & 0 \end{bmatrix}$ then $M_{11} = \begin{bmatrix} 1 & 21 \\ 7 & 26 \end{bmatrix}$, $M_{12} = \begin{bmatrix} 0 & -21 \\ 7 & -25 \end{bmatrix} = \begin{bmatrix} 0 & 5 \\ 19 & 1 \end{bmatrix}$, and $M_{21} = \begin{bmatrix} 2 & 21 \\ 7 & 1 \end{bmatrix}$

$$\therefore M = \begin{bmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{bmatrix} = \begin{bmatrix} 1 & 21 & 0 & 5 \\ 7 & 0 & 19 & 1 \\ 2 & 21 & 25 & 5 \\ 7 & 1 & 19 & 0 \end{bmatrix}$$

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 1821-1826
https://publishoa.com
ISSN: 1309-3452

Step7: Finally, we have to compute PM, this multiplication is known as the encrypted data of the original message.

$$C = P \cdot M = \begin{bmatrix} 0 & 11 & 23 & 24 \\ 11 & 0 & 5 & 15 \\ 23 & 5 & 0 & 25 \\ 24 & 15 & 25 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 21 & 0 & 5 \\ 7 & 0 & 19 & 1 \\ 2 & 21 & 25 & 5 \\ 7 & 1 & 19 & 0 \end{bmatrix} = \begin{bmatrix} 291 & 507 & 1240 & 126 \\ 126 & 351 & 410 & 80 \\ 233 & 508 & 570 & 120 \\ 179 & 1029 & 910 & 260 \end{bmatrix}$$

This PM matrix can be converted into either row or column matrix and sent is to the other user over an unsecure channel with index number, size of matrix and the matrix

$[1, 4, 291, 507, 1240, 126, 126, 351, 410, 80, 233, 508, 570, 120, 179, 1029, 910, 260, 25, 5, 19, 0]$

Decryption- User A (The sender): Decryption is done by the following steps

With the received information, the receiver separates the following matrix as follows

$$C = P \cdot M = \begin{bmatrix} 291 & 507 & 1240 & 126 \\ 126 & 351 & 410 & 80 \\ 233 & 508 & 570 & 120 \\ 179 & 1029 & 910 & 260 \end{bmatrix}$$

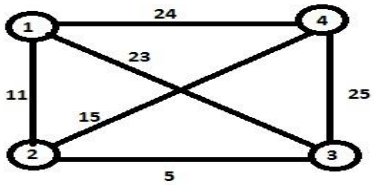
And the self-invertible key matrix be $M = \begin{bmatrix} 1 & 21 & 0 & 5 \\ 7 & 0 & 19 & 1 \\ 2 & 21 & 25 & 5 \\ 7 & 1 & 19 & 0 \end{bmatrix}$

$$CM = PMM = \begin{bmatrix} 291 & 507 & 1240 & 126 \\ 126 & 351 & 410 & 80 \\ 233 & 508 & 570 & 120 \\ 179 & 1029 & 910 & 260 \end{bmatrix} \cdot \begin{bmatrix} 1 & 21 & 0 & 5 \\ 7 & 0 & 19 & 1 \\ 2 & 21 & 25 & 5 \\ 7 & 1 & 19 & 0 \end{bmatrix} = \begin{bmatrix} 7202 & 32277 & 43027 & 8162 \\ 3963 & 11336 & 18439 & 3031 \\ 5769 & 16983 & 26182 & 4523 \\ 11022 & 23129 & 47241 & 6474 \end{bmatrix}$$

Taking modulo 26, we get then we get, 7202(mod 26) = 0, 32277(mod26) = 11, 43027(mod26) = 23, …

$$\therefore CM = \begin{bmatrix} 0 & 11 & 23 & 24 \\ 11 & 0 & 5 & 15 \\ 23 & 5 & 0 & 25 \\ 24 & 15 & 25 & 0 \end{bmatrix} = P$$

The Corresponding graph for the above adjacency matrix is



The edges(weights) of the above path are $11, 5, 25, 24, 23, 15$.

∴The original message is $11 \rightarrow K,\ \ 5 \rightarrow E,\ \ 25 \rightarrow Y$ i.e., KEY.

6. Conclusion:

Nowadays securing our information is the most important issue, encryption techniques using Hill cipher, graphical methods are used many articles to provide security of the given messages. A new approach cryptosystem encryption using

complete graphs and self-invertible matrix has been proposed in this paper which is used by the concepts of undirected path, Hamiltonian path, complete graph and adjacency matrix, an even order self-invertible matrix as key matrix in order to increase the security of our information. The proposed approach is more efficient and resists against the intermediate. The proposed approach is a simple encryption/decryption technique with better security, since we are using a self-invertible matrix as a key matrix so we don't need to find the inverse of the key matrix while decrypting the ciphertext, also we are not sharing the full key matrix over an unsecure channel (we share only a $\frac{n}{2} \times \frac{n}{2}$ matrix which helps us to generates the self-invertible matrix). In this paper, we applied this approach of message encryption, decryption with some concepts of graphs, also we are using even order self-invertible matrix as key matrix. In the future, this approach will be modified and to be used for some other advanced graph theory concepts, self-invertible matrix of any order, also to extend this approach to image encryption, decryption, etc.

7. References:

1. Acharya, B., Rath, G.S., Patra, S.K., Panigrahy, S.K., (2007), A Novel methods of generating self-invertible matrix for Hill Cipher Algorithm, Int J. Secur.
2. Acharya, B., Panigrahy, S.K., Patra, S.K., Panda, G., (2009), Image encryption using advanced Hill Cipher algorithm, Int. J. Recent Trends Eng. 1(1).
3. P. Amudha, J. Jayapriya, J. Gowri.,(2021),An algorithmic approach for encryption using graph Labeling, ICMS 2020.
4. Diffie, W., Hellman, M., 1976. New directions in Cryptography, IEEE Trans. Inf. Theory 22 (6), 644 – 654.
5. J.Gallian, a dynamic survey of graph labeling, The electronic journal of combinatories,(2015)
6. Joseph H. Silverman, An Introduction to the Theory of Elliptic Curve, University of Wyoming.
7. Invitation to Graph theory, S. Arumugam, S Ramachandran, Scitech Publications, 2015.
8. M. Yamuna, Meenal Gogia, Ashish Sikka, Md. Jazib Hayat Khan, Encryption using Graphh theory and Linear algebra.
9. Girija Sankar Rath, Bibhudendra Acharya, Sarat Kumar Patra and Saroj Kumar Panigrahy, Novel methods of generating Self- invertible matrix of Hill Cipher algorithm.
10. Neal Koblitz, A course in Number Theory and Cryptography, second edition, Springer.
11. Nandhini R, Maheswari V and Balaji V, A Graph Theory Approach on Cryptography, 2018.
12. Uma Dixit, Cryptography a Graph theory approach, International journal of Advance Research in Science and Engineering, 6(01), 2017.
13. Ziad E. Dawahdeh, Shahrul N. Yaakob, Rozmie Razif bin Othman, A new image encryption scheme by using Elliptic Curve Cryptography and Hill Cipher.