Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Enhancement of Minimal Spanning Tree Computing Performance in a Complete Graphic Based Enciphering Method Using Self-Invertible Key Matrix

Dr. P. Mohan[1], Dr. M. V. Suresh[2], Dr. C. Periyasamy[3]

[1]Assistant Professor, Department of Mathematics, FSH, SRM Institute of Science and Technology, Vadapalani Campus, mohan14palani@gmail.com
[2]Assistant Professor, Department of Mathematics, Panimalar Engineering College, Poonamallee, Chennai, dr.m.v.suresh1708@gmail.com
[3]Assistant Professor, Department of Mathematics, FSH, SRM Institute of Science and Technology, Vadapalani Campus, periasamy.cps@gmail.com

In the current era of communication, message encryption is the most crucial step in protecting our personal data, interpersonal communications, and interpersonal relationships. Due to the expansion and growth of network connections and the rise of the internet, communication encryption techniques have become increasingly prevalent in recent times. One technique to hack or steal original details is to share data, confidential conversations, photographs, data, or other stuff with another user over unprotected channels. Cryptographic or encoding techniques are essential for reducing this terminology and improving security. There are many different types of symmetric encoding techniques in cryptography, such as the Caesar, Atbash, Play Fair, and Hill ciphers. This study presents an encoding methodology that generates a complex the ciphertext by encrypting and decrypting the given data utilising the ideas of a corresponding adjacency matrix, a minimal traversing tree of a complete graph, and a created self-invertible key matrix. We don't need to compute the inverse while decrypting the ciphertext because the inverse of this key matrix always exists because we are using the self-invertible matrix as the encryption key matrix. It helps to reduce the amount of work involved in figuring out a key matrix's inverse.

Keywords: Matrix encryption, Self-Invertible Matrix, Graph Encryption, Complete graph, Minimal spanning tree, Adjacency Matrix.

1. Introduction

The study and practice of converting plain texts or messages into an incomprehensible disguised form—in which the intermediaries remain anonymous—so that only the intended recipients can remove the disguise and read the original message is known as cryptography. Cryptography, which helps us increase the security of data transmissions, is one of the

mathematical techniques used to protect communications and data from hackers. The message we received was in plain text, but the one that was buried was in encrypted text. Even if different alphabets are used to write encrypted and plain text, they are not identical alphabets as well. In certain situations, messages are sent using special characters that the sender and the recipient have agreed upon, such as numerals, punctuation marks, and blanks. This method uses an afterwards encoded table to encode the provided plain texts.

A	B	C	D	E	F	G	H	I	J	…	…	…	W	X	Y	Z		.	?
1	2	3	4	5	6	7	8	9	10	…	…	…	23	24	25	26	27	28	29

Table 1.0. Encoded Table

Encryption, commonly referred to as enciphering, is the process of transforming plaintext, or the original communication, into ciphertext, which is unreadable by others. Deciphering, or decrypting, is the process of converting ciphertext back into plaintext. A key is a variable amount or parameter used in cryptography that allows us to translate message units from plain text to ciphertext and back again. The length of the key determines how difficult it will be to decode the text from the original transmission. Both the sender and the one receiving the message must use the same key for encrypting and decryption. It is also referred to as symmetric key encryption for private keys and asymmetric key encryption for public keys.

The foundation of cryptography is graph theory [1]. [1, 2] provided an explanation of the symmetric cryptography technique utilizing the cycle graph, full graph, and least spanning tree. The upper triangular matrix served as the shared key matrix in both situations. In [3], the idea of encryption methods utilizing full graphs and Hamiltonian routes was used with the use of a lower triangular matrix for a key matrix. In [4], the relationship between graph theory and encryption was elucidated; the upper triangular matrix was employed as a key matrix in this instance. In order to increase the cipher's security, a novel message encoding and decoding method utilizing graph labeling was described in [5]. Here, the upper triangular matrix served as a key matrix. A self-invertible matrix of rank 4 was utilized in the tetragraphic trifunction [6]. The majority of the techniques listed above make use of the symmetrical encryption algorithm. Both the sender and the recipient utilize the same key, which is often lower and upper triangular, and they share this key across all types of medians. Sharing the shared key matrix over an insecure channel is challenging, yet it is simple to expose whenever the intermediaries figure out how to do it.

Using an adjacency matrix and self-invertible matrix [7-11] as the key for both decryption and encryption, we have presented an innovative method that aims to minimize this jargon, reinforce the key, and generate higher security for the data that is provided. Since the self-invertible matrix, we're using as our key matrix is identical to its inverse, we can decrypt the encrypted text without having to calculate the inverse. It facilitates the reduction of the inverse's complexity. Furthermore, the complete key matrix is not being shared over an unprotected connection. This reduces the possibility that the crucial matrix will be compromised and strengthens the privacy of information.

The idea of a minimal spanning tree of a complete graph and its associated adjacency matrix are used in this work to offer a technique. In this case, the self-invertible key matrix serves as the key for both encryption and decryption of the designated original message units, enhancing security and generating a fresh and effective technique. Because this method uses a self-

invertible key matrix as the encryption key matrix, we are not required to compute an inverse of the key matrix's value when performing the decryption procedure. The sender must first construct a cycle graph with n vertices—where n is the total number of characters in the plaintext—in order to employ this method.

2. Generation of self-invertible key matrix

The matrix S is considered self-invertible if $= S^{-1}$, or $S \cdot S^{-1} = S^{-1} \cdot S = I$, The techniques that follow were used to create the self-invertible matrix:

Procedure 1: First, we will take any randomized S_{22} matrix of order $\frac{n}{2} \times \frac{n}{2}$, where n is the even adjacency matrix's order. Utilizing S_{22}, the additional $\frac{n}{2} \times \frac{n}{2}$ matrices are computed by applying the subsequent properties:

$$S_{11} + S_{22} = 0 \Rightarrow S_{22} = -S_{11},\ S_{21} = I + S_{11},\ S_{12} = I - S_{11}.$$

After computing $S_{11}, S_{12}, S_{21}, S_{22}$ the self-invertible matrix S was created as follows,

$$S = \begin{bmatrix} S_{11} & S_{12} \\ S_{21} & S_{22} \end{bmatrix} = \left[\begin{array}{cccc:c} s_{11} & s_{12} & \cdots & \cdots & s_{1n} \\ s_{21} & s_{22} & \cdots & \cdots & s_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \hdashline \cdots & \cdots & \cdots & \cdots & \cdots \\ s_{n1} & s_{n2} & \cdots & \cdots & s_{nn} \end{array}\right]$$

Example:

Let us consider the commonly shared $\frac{n}{2} \times \frac{n}{2}$ matrix $S_{22} = \begin{bmatrix} 1 & 4 \\ 9 & 6 \end{bmatrix}$. Then the remaining matrices are (under modulo 29)

$$S_{11} = \begin{bmatrix} -1 & -4 \\ -9 & -6 \end{bmatrix} = \begin{bmatrix} 28 & 25 \\ 20 & 23 \end{bmatrix},$$

$$S_{12} = I - S_{11} = \begin{bmatrix} -27 & -25 \\ -20 & -22 \end{bmatrix} = \begin{bmatrix} 2 & 4 \\ 9 & 7 \end{bmatrix},$$

$$S_{21} = I + S_{11} = \begin{bmatrix} 29 & 25 \\ 20 & 24 \end{bmatrix} = \begin{bmatrix} 0 & 25 \\ 20 & 24 \end{bmatrix}$$

$$\therefore S = \begin{bmatrix} S_{11} & S_{12} \\ S_{21} & S_{22} \end{bmatrix} = \begin{bmatrix} 28 & 25 & 2 & 4 \\ 20 & 23 & 9 & 7 \\ 0 & 25 & 1 & 4 \\ 20 & 24 & 9 & 6 \end{bmatrix}$$

Procedure 2: Let us consider the random S_{22} matrix of order $(n-1) \times (n-1)$, where n being the order of adjacency matrix.

Using S_{22}, the remaining $(n-1) \times (n-1)$ matrices are calculated by using the following characteristics,

$S_{11} = -\lambda = -$[one of the eigen value of S_{22}], S_{12} and S_{21} are calculated by finding

consistent solution of equation $S_{12} \cdot S_{21} = I - (S_{22})^2$

After computing $S_{11}, S_{12}, S_{21}, S_{22}$ the self-invertible matrix S was created as follows,

$$S = \begin{bmatrix} S_{11} & S_{12} \\ S_{21} & S_{22} \end{bmatrix} = \begin{bmatrix} s_{11} & s_{12} & \cdots & \cdots & s_{1n} \\ s_{21} & s_{22} & \cdots & \cdots & s_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ s_{n1} & s_{n2} & \cdots & \cdots & s_{nn} \end{bmatrix}$$

Example:

Let us consider the random S_{22} matrix of order $(n-1) \times (n-1)$, (under modulo 29)

$$S_{22} = \begin{bmatrix} 27 & 2 & 3 \\ 28 & 3 & 1 \\ 28 & 2 & 2 \end{bmatrix}$$

The eigen values of S_{22} are $\lambda_1 = 1$, $\lambda_2 =$-1, $\lambda_3 = 32 (= 3 (\text{mod } 29))$

The other matrices are $S_{11} = -\lambda_3 = -3 = 26 (\text{mod } 29) \implies S_{11} = [26]$

The consistent solutions of $S_{12} \cdot S_{21} = I - (S_{22})^2$ are $S_{12} = [\,28 \;\; 4 \;\; 1], S_{21} = \begin{bmatrix} 27 \\ 27 \\ 27 \end{bmatrix}$

Hence the self-invertible key matrix is $S = \begin{bmatrix} S_{11} & S_{12} \\ S_{21} & S_{22} \end{bmatrix} = \begin{bmatrix} 26 & 28 & 4 & 1 \\ 27 & 27 & 2 & 3 \\ 27 & 28 & 3 & 1 \\ 27 & 28 & 2 & 2 \end{bmatrix}$

3. The proposed cryptosystem

This section described the proposed approach which uses the cycle graph, the complete graph of this cycle graph, Minimal Spanning Tree, the adjacency matrix of this Minimal Spanning Tree and the self-invertible key matrix.

Proposed encryption algorithm:

The following procedures are used to perform encoding:

Step 1: The consecutive characters in the provided unencrypted message units were connected to create the cycle graph.

Step 2: Using an encoded table (Table 1.0), the message units are translated into their corresponding numerical values.

Step 3: The numerical difference that exists between the corresponding two neighbouring vertices is used to assign the weights to each edge.

Step 4: Connect every vertex in the cycle graph to create a full network Kn. The weights

associated with these false nodes are simply the values of weights that follow the maximum in the encoded table (Table 1.0), so for example, 30, 31, 32,...

Step 5: To highlight the first letter of the original message, a unique add on character (Say A) was placed before the initial letter of the provided plaintext.

Step6: Build the complete graph's minimum spanning tree.

Step 7: The matching adjacency matrix for this minimum spanning tree was constructed after performing addition modulo 29.

Step 8: With the details provided, the self-invertible matrix was created using the methods outlined in Section 2.

Step 9: In order to obtain the encrypted version of the plaintext original message, the matrix of adjacency was multiplied by the self-invertible key matrix that was formed.

Step 10: This encoded matrix was sent to a different user via any type of medium, whether in a row-wise or column-wise format, along with the matrices' order, that is used to create the self-invertible key matrix.

Proposed decryption algorithm:

Step 1: By tracing back the information, the recipient can determine the matrix's order, its encryption, and an information matrix that aids in the creation of the self-invertible key matrix.

Step 2: Using the data provided in Section 2, the recipient must generate the self-invertible key matrix.

Step 3: The encoded matrix needs to be multiplied by the self-invertible matrix that was created.

Step 4: Lastly, the matrix representing the adjacency of the graph should be obtained by the beneficiary by adding modulo 29 to the resultant matrix.

Step 5: Tracing Backward the Graph: Using the nodes and the weights, the receiver can create the least spanning tree of the graph.

Step 6: Add the weights to determine the message. Vertex v1 is undoubtedly A, and its numerical equivalent is 1, and v2 is equal to the value of v1 plus weight e1.

4. Implementation example:

Example I: Assume that User A (sender) wishes to deliver the message "TIGER" to User B (receiver) via the method described in the previous section, utilizing the key matrix that was described in Section 2's first procedure.

User A (The sender): Encryption To perform encryption, follow these steps: Step 1: First, the sender (User A) needs to create a cycle graph by converting the provided message, "TIGER," into a graph with vertices. The successive letters in the provided message are connected to form the vertices of this cycle graph.

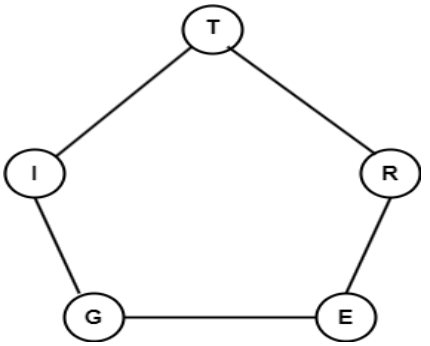

Figure 1.0. The cycle graph of original message

Step2: With the help of encoded table (Table 1.0) we get, $\boldsymbol{T \rightarrow 20}$, $\boldsymbol{I \rightarrow 9, G \rightarrow 7}$, $\boldsymbol{E \rightarrow 5}$, $\boldsymbol{R \rightarrow 18}$.

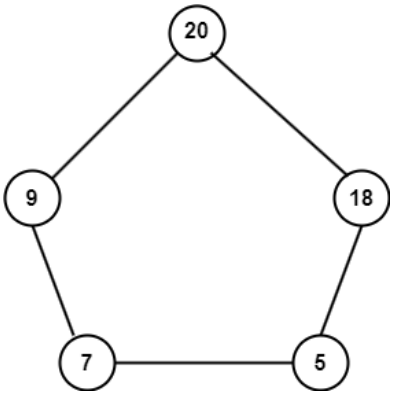

Figure 2.0. Encoded cycle graph

Step 3: The distance between the next two associated vertices is used to assign a weight to th e graph's edges (e.g., e1 = Code I – Code T, e2 = Code G – Code I, etc.).

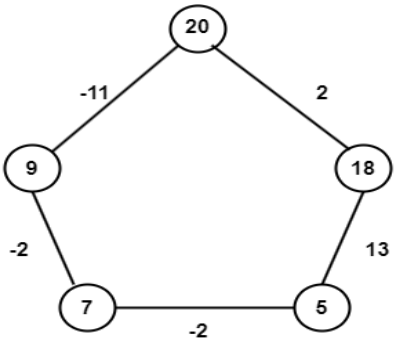

Figure 3.0. Weighted cycle graph

Step 4: Connect the cycle graph's unconnected nodes to create a complete graph Kn (the wei ghts associated with these false edges are 30, 31, 32,...).

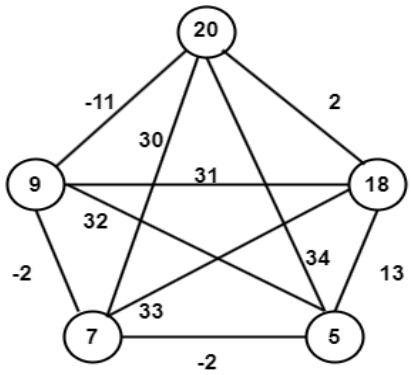

Figure 4.0. The Complete graph ($\boldsymbol{K_5}$)

Step 5: To indicate the first letter of the original message, a unique add on character (Usually an A) was placed before the initial letter for the original message unit.

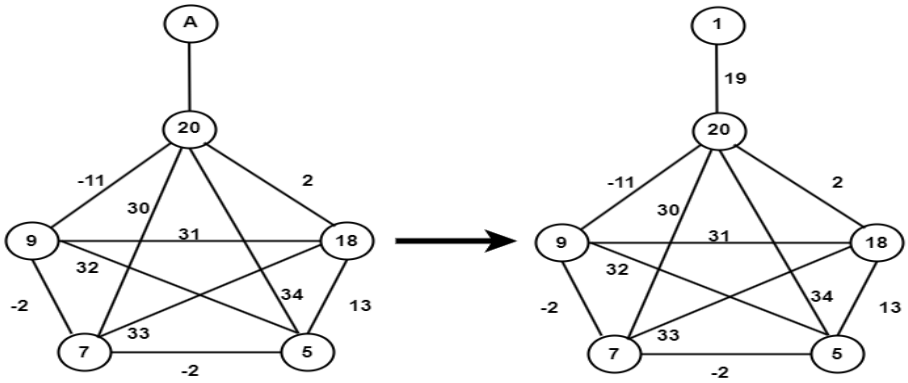

Figure 5.0. Complete graph $\boldsymbol{K_5}$ with a special character

Step 6: Using additions modulo 29 to create a minimal spanning tree of the above full graph

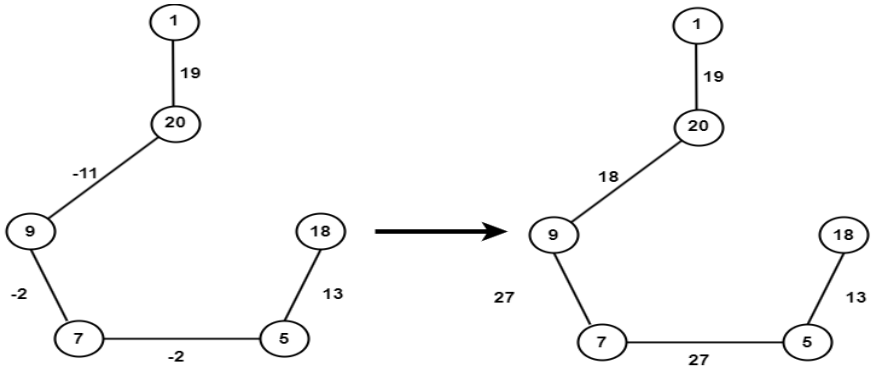

Figure 6.0. The minimum spanning tree of complete graph $\boldsymbol{K_5}$

Step 7: After computing an adjacency matrix of the matching minimum spanning tree, assign it the letter "M."

$$M = \begin{bmatrix} 0 & 19 & 0 & 0 & 0 & 0 \\ 19 & 0 & 18 & 0 & 0 & 0 \\ 0 & 18 & 0 & 27 & 0 & 0 \\ 0 & 0 & 27 & 0 & 27 & 0 \\ 0 & 0 & 0 & 27 & 0 & 13 \\ 0 & 0 & 0 & 0 & 13 & 0 \end{bmatrix}$$

Step 8: Now to compute the key matrix for that purpose we construct the self-invertible key matrix 'S' with the help of $\frac{n}{2} \times \frac{n}{2}$ matrix S_{22}.

Let $S_{22} = \begin{bmatrix} 2 & 1 & 1 \\ 3 & 2 & 1 \\ 2 & 1 & 2 \end{bmatrix}$ then $S_{11} = \begin{bmatrix} -2 & -1 & -1 \\ -3 & -2 & -1 \\ -2 & -1 & -2 \end{bmatrix} = \begin{bmatrix} 27 & 28 & 28 \\ 26 & 27 & 28 \\ 27 & 28 & 27 \end{bmatrix}$,

$$S_{12} = I - S_{11} = \begin{bmatrix} 3 & 1 & 1 \\ 3 & 3 & 1 \\ 2 & 1 & 3 \end{bmatrix}, \text{and } S_{21} = I + S_{11} = \begin{bmatrix} 28 & 28 & 28 \\ 26 & 28 & 28 \\ 27 & 28 & 28 \end{bmatrix}$$

$$\therefore S = \begin{bmatrix} S_{11} & S_{12} \\ S_{21} & S_{22} \end{bmatrix} = \begin{bmatrix} 27 & 28 & 28 & 3 & 1 & 1 \\ 26 & 27 & 28 & 3 & 3 & 1 \\ 27 & 28 & 27 & 2 & 1 & 3 \\ 28 & 28 & 28 & 2 & 1 & 1 \\ 26 & 28 & 28 & 3 & 2 & 1 \\ 27 & 28 & 28 & 2 & 1 & 2 \end{bmatrix}$$

Step 9: Finally, the encrypted matrix was computed by multiplying M and S

$$C = M \cdot S = \begin{bmatrix} 0 & 19 & 0 & 0 & 0 & 0 \\ 19 & 0 & 18 & 0 & 0 & 0 \\ 0 & 18 & 0 & 27 & 0 & 0 \\ 0 & 0 & 27 & 0 & 27 & 0 \\ 0 & 0 & 0 & 27 & 0 & 13 \\ 0 & 0 & 0 & 0 & 13 & 0 \end{bmatrix} \cdot \begin{bmatrix} 27 & 28 & 28 & 3 & 1 & 1 \\ 26 & 27 & 28 & 3 & 3 & 1 \\ 27 & 28 & 27 & 2 & 1 & 3 \\ 28 & 28 & 28 & 2 & 1 & 1 \\ 26 & 28 & 28 & 3 & 2 & 1 \\ 27 & 28 & 28 & 2 & 1 & 2 \end{bmatrix}$$

$$= \begin{bmatrix} 494 & 513 & 532 & 57 & 57 & 19 \\ 999 & 1036 & 1018 & 93 & 37 & 73 \\ 1224 & 1242 & 1260 & 108 & 81 & 108 \\ 1431 & 1512 & 1485 & 135 & 81 & 108 \\ 1107 & 1120 & 1120 & 80 & 40 & 53 \\ 338 & 364 & 364 & 39 & 26 & 13 \end{bmatrix}$$

Step 10: The encrypted matrix can be converted in the form of row or column matrix and sent it to the other user over any kind of median with specifying the order of the matrix, the matrix which helps to compute the self- invertible matrix.

[**6, 494, 513, 532, 57, 57, 19, 999, 1036, 1018, 93, 37, 73, 1224, 1242, 1260, 108, 81, 108, 1431**

81, 108, 1107, 1120, 1120, 80, 40, 53, 338, 364, 364, 39, 26, 13; 2, 1, 1, 3, 2, 1, 2, 1, 2].

Decryption- User B (The receiver): Decryption is done by the following steps

With the received information, the receiver is able to identify the order of the matrix, encrypted

matrix, the matrix which helps to generates the key matrix then the receiver separates the following matrix as follows

$$\boldsymbol{C = M \cdot S} = \begin{bmatrix} \mathbf{494} & \mathbf{513} & \mathbf{532} & \mathbf{57} & \mathbf{57} & \mathbf{19} \\ \mathbf{999} & \mathbf{1036} & \mathbf{1018} & \mathbf{93} & \mathbf{37} & \mathbf{73} \\ \mathbf{1224} & \mathbf{1242} & \mathbf{1260} & \mathbf{108} & \mathbf{81} & \mathbf{108} \\ \mathbf{1431} & \mathbf{1512} & \mathbf{1485} & \mathbf{135} & \mathbf{81} & \mathbf{108} \\ \mathbf{1107} & \mathbf{1120} & \mathbf{1120} & \mathbf{80} & \mathbf{40} & \mathbf{53} \\ \mathbf{338} & \mathbf{364} & \mathbf{364} & \mathbf{39} & \mathbf{26} & \mathbf{13} \end{bmatrix}$$

The receiver is also generating the self-invertible matrix as the procedure explained in Section 2(Procedure 1).

$$\therefore \boldsymbol{S} = \begin{bmatrix} \boldsymbol{S_{11}} & \boldsymbol{S_{12}} \\ \boldsymbol{S_{21}} & \boldsymbol{S_{22}} \end{bmatrix} = \begin{bmatrix} \mathbf{27} & \mathbf{28} & \mathbf{28} & \mathbf{3} & \mathbf{1} & \mathbf{1} \\ \mathbf{26} & \mathbf{27} & \mathbf{28} & \mathbf{3} & \mathbf{3} & \mathbf{1} \\ \mathbf{27} & \mathbf{28} & \mathbf{27} & \mathbf{2} & \mathbf{1} & \mathbf{3} \\ \mathbf{28} & \mathbf{28} & \mathbf{28} & \mathbf{2} & \mathbf{1} & \mathbf{1} \\ \mathbf{26} & \mathbf{28} & \mathbf{28} & \mathbf{3} & \mathbf{2} & \mathbf{1} \\ \mathbf{27} & \mathbf{28} & \mathbf{28} & \mathbf{2} & \mathbf{1} & \mathbf{2} \end{bmatrix}$$

$$\boldsymbol{C \cdot S = M \cdot S \cdot S} = \begin{bmatrix} \mathbf{494} & \mathbf{513} & \mathbf{532} & \mathbf{57} & \mathbf{57} & \mathbf{19} \\ \mathbf{999} & \mathbf{1036} & \mathbf{1018} & \mathbf{93} & \mathbf{37} & \mathbf{73} \\ \mathbf{1224} & \mathbf{1242} & \mathbf{1260} & \mathbf{108} & \mathbf{81} & \mathbf{108} \\ \mathbf{1431} & \mathbf{1512} & \mathbf{1485} & \mathbf{135} & \mathbf{81} & \mathbf{108} \\ \mathbf{1107} & \mathbf{1120} & \mathbf{1120} & \mathbf{80} & \mathbf{40} & \mathbf{53} \\ \mathbf{338} & \mathbf{364} & \mathbf{364} & \mathbf{39} & \mathbf{26} & \mathbf{13} \end{bmatrix} \cdot \begin{bmatrix} \mathbf{27} & \mathbf{28} & \mathbf{28} & \mathbf{3} & \mathbf{1} & \mathbf{1} \\ \mathbf{26} & \mathbf{27} & \mathbf{28} & \mathbf{3} & \mathbf{3} & \mathbf{1} \\ \mathbf{27} & \mathbf{28} & \mathbf{27} & \mathbf{2} & \mathbf{1} & \mathbf{3} \\ \mathbf{28} & \mathbf{28} & \mathbf{28} & \mathbf{2} & \mathbf{1} & \mathbf{1} \\ \mathbf{26} & \mathbf{28} & \mathbf{28} & \mathbf{3} & \mathbf{2} & \mathbf{1} \\ \mathbf{27} & \mathbf{28} & \mathbf{28} & \mathbf{2} & \mathbf{1} & \mathbf{2} \end{bmatrix}$$

$$= \begin{bmatrix} \mathbf{44631} & \mathbf{46303} & \mathbf{46284} & \mathbf{4408} & \mathbf{2755} & \mathbf{2755} \\ \mathbf{86932} & \mathbf{90132} & \mathbf{90150} & \mathbf{8584} & \mathbf{5365} & \mathbf{5365} \\ \mathbf{105705} & \mathbf{109638} & \mathbf{109620} & \mathbf{10467} & \mathbf{6525} & \mathbf{6525} \\ \mathbf{126846} & \mathbf{131544} & \mathbf{131571} & \mathbf{12528} & \mathbf{7857} & \mathbf{7830} \\ \mathbf{93960} & \mathbf{97440} & \mathbf{97440} & \mathbf{9307} & \mathbf{5800} & \mathbf{5813} \\ \mathbf{30537} & \mathbf{31668} & \mathbf{31668} & \mathbf{3016} & \mathbf{1898} & \mathbf{1885} \end{bmatrix}$$

Taking addition modulo $\mathbf{29}$, then we get, 44631(mod 29) = 0, 46303(mod 29) = 19, 46284(mod 29) = 0, …, $\mathbf{1885}$ (mod 29) = 0

$$\therefore \boldsymbol{C\,S} = \begin{bmatrix} \mathbf{0} & \mathbf{19} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{19} & \mathbf{0} & \mathbf{18} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{18} & \mathbf{0} & \mathbf{27} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{27} & \mathbf{0} & \mathbf{27} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{27} & \mathbf{0} & \mathbf{13} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{13} & \mathbf{0} \end{bmatrix} = \boldsymbol{M}$$

The Corresponding minimal spanning tree for the above adjacency matrix was formed

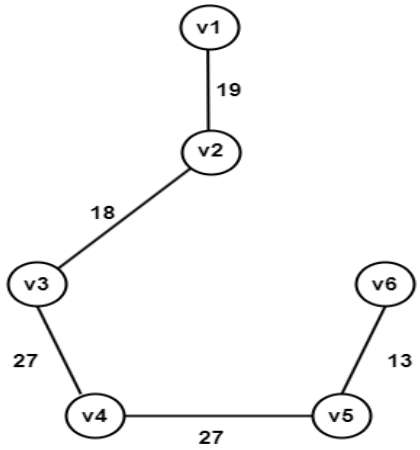

Figure 7.0. The minimum spanning tree of decrypted adjacency matrix

The vertices(nodes) of the above minimal spanning tree were constructed by adding numerical equivalent value of vertex with corresponding edge, since we are adding a special character A in the beginning so we know that the first vertex must be 1 so the remaining vertices are finding by let v1=1, so v2= 1 + 19 = 20, v3 = 20 + 18 =38 = 9, v4 = 9+ 27 = 36 = 7, v5 = 7 + 27 = 34 = 5, v6 = 5 + 13 = 18

∴ The vertices are $\mathbf{20}, \mathbf{9}, \mathbf{7}, \mathbf{5}, \mathbf{18}$.

∴The original message is $\mathbf{20} \rightarrow \boldsymbol{T}$, $\mathbf{9} \rightarrow \boldsymbol{I}, \mathbf{7} \rightarrow \boldsymbol{G}$, $\mathbf{5} \rightarrow \boldsymbol{E}$, $\mathbf{18} \rightarrow \boldsymbol{R}$ i.e., TIGER.

Example II. Suppose that User A(sender) wants to send the message "PEN" to another user (User B(receiver)) using the technique which is explained in section 3, using the key matrix that has been explained in procedure 2 of section 2.

Initially, the sender (User A) should convert the given message" PEN" as the vertices of a graph and make a cycle graph. The vertices of this cycle graph are joined by connecting sequential letters in the given message.

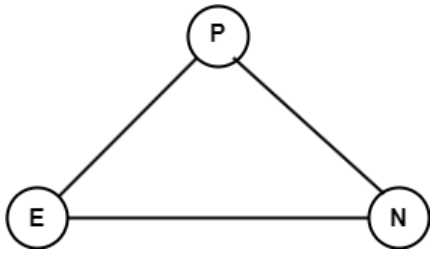

Figure 8.0

Using the encoded table (Table 1.0) we get, $\boldsymbol{P} \rightarrow \mathbf{16}$, $\boldsymbol{E} \rightarrow \mathbf{5}$, $\boldsymbol{N} \rightarrow \mathbf{14}$.

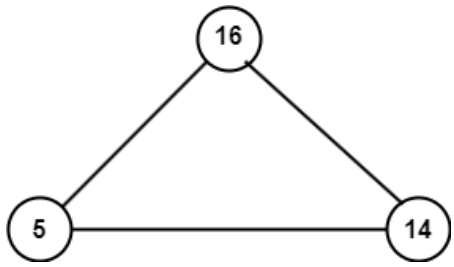

Figure 9.0. Encoded cycle graph

A special add on character (A) was added before the starting letter of the original message unit to specify the first letter of the original message.

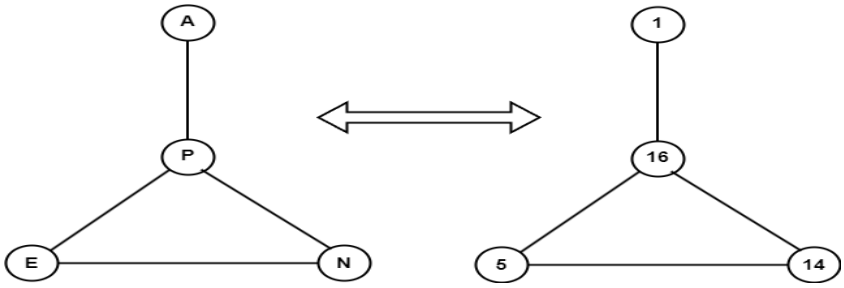

Figure 10.0. Complete graph $\boldsymbol{K_3}$ with a special character

Weights of the edges of this graph are assigned by finding distance between the consecutive two connected vertices (i.e., e1= Code E – Code P, e2 = Code N – Code E, …)

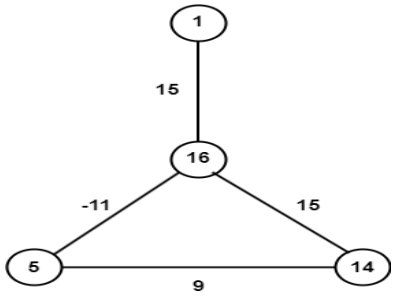

Figure 11.0. Weighted cycle graph

The Minimum spanning tree of the above was constructed, taking addition modulo 29

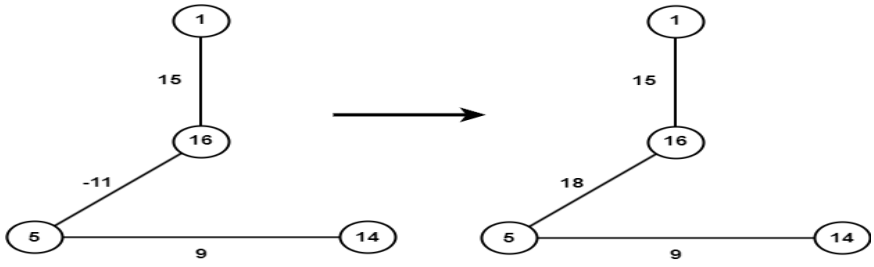

Figure 12.0. The minimum spanning tree of complete graph $\boldsymbol{K_3}$

The adjacency matrix of the corresponding minimum spanning tree was computed, name it as 'N'

$$\boldsymbol{N} = \begin{bmatrix} \mathbf{0} & \mathbf{15} & \mathbf{0} & \mathbf{0} \\ \mathbf{15} & \mathbf{0} & \mathbf{18} & \mathbf{0} \\ \mathbf{0} & \mathbf{18} & \mathbf{0} & \mathbf{9} \\ \mathbf{0} & \mathbf{0} & \mathbf{9} & \mathbf{0} \end{bmatrix}$$

The Self-invertible key matrix be $\boldsymbol{S} = \begin{bmatrix} \boldsymbol{S_{11}} & \boldsymbol{S_{12}} \\ \boldsymbol{S_{21}} & \boldsymbol{S_{22}} \end{bmatrix} = \begin{bmatrix} \mathbf{26} & \mathbf{28} & \mathbf{4} & \mathbf{1} \\ \mathbf{27} & \mathbf{27} & \mathbf{2} & \mathbf{3} \\ \mathbf{27} & \mathbf{28} & \mathbf{3} & \mathbf{1} \\ \mathbf{27} & \mathbf{28} & \mathbf{2} & \mathbf{2} \end{bmatrix}$

The encrypted matrix was computed by multiplying N and S

$$C = N \cdot S = \begin{bmatrix} 0 & 15 & 0 & 0 \\ 15 & 0 & 18 & 0 \\ 0 & 18 & 0 & 9 \\ 0 & 0 & 9 & 0 \end{bmatrix} \cdot \begin{bmatrix} 26 & 28 & 4 & 1 \\ 27 & 27 & 2 & 3 \\ 27 & 28 & 3 & 1 \\ 27 & 28 & 2 & 2 \end{bmatrix}$$

$$= \begin{bmatrix} 405 & 405 & 30 & 45 \\ 876 & 924 & 114 & 33 \\ 729 & 738 & 54 & 72 \\ 243 & 252 & 27 & 9 \end{bmatrix}$$

The encrypted matrix can be converted in the form of row or column matrix and sent is to the other user over any kind of median with specifying the order of the matrix, the matrix which helps to compute the self- invertible matrix.

$[\,4, 405, 405, 30, 45, 876, 924, 114, 33, 729, 738, 54, 72, 243, 252, 27, 9, 27, 2, 3, 28, 3, 1, 28, 2, 2]$.

Decryption- User B (The receiver): Decryption is done by the following steps

With the received information, the receiver is able to identify the order of the matrix, encrypted matrix, the matrix which helps to generates the key matrix then the receiver separates the following matrix as follows

$$C = N \cdot S = \begin{bmatrix} 405 & 405 & 30 & 45 \\ 876 & 924 & 114 & 33 \\ 729 & 738 & 54 & 72 \\ 243 & 252 & 27 & 9 \end{bmatrix}$$

The receiver is also generating the self-invertible matrix as procedure explained in section 2(Procedure 2)

$$\therefore S = \begin{bmatrix} S_{11} & S_{12} \\ S_{21} & S_{22} \end{bmatrix} = \begin{bmatrix} 26 & 28 & 4 & 1 \\ 27 & 27 & 2 & 3 \\ 27 & 28 & 3 & 1 \\ 27 & 28 & 2 & 2 \end{bmatrix}$$

$$C \cdot S = N \cdot S \cdot S = \begin{bmatrix} 405 & 405 & 30 & 45 \\ 876 & 924 & 114 & 33 \\ 729 & 738 & 54 & 72 \\ 243 & 252 & 27 & 9 \end{bmatrix} \cdot \begin{bmatrix} 26 & 28 & 4 & 1 \\ 27 & 27 & 2 & 3 \\ 27 & 28 & 3 & 1 \\ 27 & 28 & 2 & 2 \end{bmatrix}$$

$$= \begin{bmatrix} 23490 & 24375 & 2610 & 1740 \\ 51693 & 53592 & 5760 & 3828 \\ 42282 & 43866 & 4698 & 3141 \\ 14094 & 14616 & 1575 & 1044 \end{bmatrix}$$

Taking addition modulo 29, then we get, 23490(mod 29) = 0, 24375(mod 29) = 15, 2610(mod 29) = 0, …, 1044 (mod 29) = 0

$$\therefore C\,S = \begin{bmatrix} 0 & 15 & 0 & 0 \\ 15 & 0 & 18 & 0 \\ 0 & 18 & 0 & 9 \\ 0 & 0 & 9 & 0 \end{bmatrix} = N$$

The Corresponding minimal spanning tree for the above adjacency matrix was formed

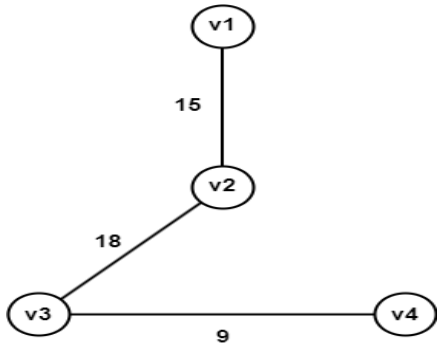

Figure 13.0. The minimum spanning tree of decrypted adjacency matrix

The vertices(nodes) of the above minimal spanning tree were constructed by adding numerical equivalent value of vertex with corresponding edge, since we are adding a special character A in the beginning so we know that the first vertex must 1 so the remaining vertices are finding by let v1=1, so v2= 1 + 15 = 16, v3 = 16 + 18 =34 = 5, v4 = 5 + 9 = 14.

∴ The vertices are $16, 5, 14$.

∴The original message is $16 \rightarrow P$, $5 \rightarrow E, 14 \rightarrow N$. i.e., PEN.

5. Conclusion:

In the modern world, security of information is critical. Numerous works use encryption methods such as the Hill cipher and graphic ways to guarantee the security of the interactions provided. To further improve security of information, this paper proposes a novel approach to encryption system encryption using complete graphs, the minimum spanning trees, and self-invertible matrices. The notions of undirected path, cycle graph, complete graph, minimal

spanning tree, and adjacency matrix are used in this methodology, along with a self-invertible matrix as the key matrix. The recommended approach outperforms the one that is intermediate and is more efficient. By using a self-invertible matrix as the key matrix, the suggested method uses a straightforward encryption/decryption mechanism with enhanced security. This eliminates the need to figure out the key matrix's inverse when decrypting the ciphertext and prevents the entire key matrix from being shared over an insecure channel. Several different kinds of graphs are used in this paper's text decoding and encryption process. This approach will be refined and extended to other graph theory concepts and more intricate graphs in the future. It will additionally be modified to incorporate various other encryption techniques, such decrypting and encrypting images, among others.

References

[1] Uma Dixit, Cryptography a Graph theory approach, International Journal of Advance Research in Science and Engineering, 6(01), 2017 http://www.ijarse.com/images/fullpdf/1504001715_BVCNSCS17072_Dr_Uma_Dixit.pdf

[2] Weal Mahmoud AI Etaiwi, Encryption algorithm using Graph theory, Journal of Scientific Research & Reports, 3(19): 2519-2527,2014, DOI;10.9734/JSRR/2014/11804

[3]Yamuna M, Meenal Gogia, Ashish Sikka, Md. Jazib Hayat Khan, Encryption Using Graph Theory and Linear Algebra, International Journal of Computer Application, ISSN:2250-1797, Issue 2 Vol 5, 2012. https://rspublication.com/ijca/OCT12/12.pdf

[4] Nandhini R, Maheswari V and Balaji V, A Graph Theory Approach on Cryptography, 2018, DOI: https://doi.org/10.26524/cm27

[5] Amudha P, Jayapriya P, Gowri J,An algorithmic approach for encryption using graph Labeling, ICMS-2020, 2021. https://doi.org/10.1088/1742-6596/1770/1/012072

[6] Sally Lin Pei Ching and Faridah Yunos, Effect of Self-Invertible Matrix on Cipher Hexagraphic Polyfunction, Cryptography 2019, 3, 15. DOI:10.3390/cryptography3020015.

[7] Acharya, B., Rath, G.S., Patra, S.K., Panigrahy, S.K, A Novel method of generating self-invertible matrix for Hill Cipher Algorithm, Int J. Secure,2007. https:doi=10.1.1.303.797&rep=rep1&type=pdf

[8] Mohan. P, Rajendran. K, Rajesh. A, An Encryption Technique using a Complete graph with a Self-invertible matrix, Journal of Algebraic statistics, Volume 13. No 3, p. 1821-1826, 2022. https://publishoa.com/index.php/journal/article/view/816.

[9] Mohan P, Rajendran K, Rajesh A. A Hamiltonian Path-Based Enciphering Technique with the use of a Self-Invertible Key Matrix, Indian Journal of Science and Technology, 15(44) (2022), pp.2351-2355. https://doi.org/10.17485/IIST/v15i44.1861

[10] Mohan P, Rajendran K, Rajesh A. An encryption Technique using the adjacency matrices of certain graphs with a self-invertible key matrix, E3S Web of Conf, Volume 376, 01108(2023) https://doi.org/10.1051/e3sconf/202337601108

[11] Mohan P, Rajendran K, Rajesh A. Enhancing Computational Performance of Minimal Spanning Tree of Certain Graphs Based Enciphering Technique Using Self-Invertible Key Matrix, "Journal of Aeronautical Materials(1005-5053)", May - 2023.

[12] 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).

[13] Invitation to Graph theory, S. Arumugam, S Ramachandran, Scitech Publications, 2015.

[14] Neal Koblitz, A course in Number Theory and Cryptography, second edition, Springer.