JOURNAL OF AERONAUTICAL MATERIALS
ISSN: 1005-5053

Vol. 43, Issue-01, 2023
pp. 359-371

ENHANCING COMPUTATIONAL PERFORMANCE OF MINIMAL SPANNING TREE OF CERTAIN GRAPHS BASED ENCIPHERING TECHNIQUE USING SELF INVERTIBLE KEY MATRIX

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

[1]Research Scholar, Department of Mathematics, Vels Institute of Science, Technology & Advanced Studies (VISTAS), India.
& Assistant Professor, Department of Mathematics, SRM Arts and Science College.
[1]mohan14palani@gmail.com, mohan.phd@velsuniv.ac.in
[2] Associate Professor, Department of Mathematics, Vels Institute of Science, Technology & Advanced Studies (VISTAS), India. [2] gkrajendra59@gmail.com,
[3] Associate Professor, Department of CSE, Vels Institute of Science, Technology & Advanced Studies (VISTAS), India. [3] arajesh.se@velsuniv.ac.in

ABSTRACT:

These days, message encryption techniques are the most crucial methods for protecting our communications and data. Utilizing the internet and network connections has accelerated the development of message encryption technologies. It is potential for an assault, theft, or hacking of the communications if sensitive, private messages are shared via insecure networks. Cryptographic techniques have been discovered to be crucial for reducing this term. There are various symmetric enciphering techniques; the Caesar Cipher, Hill Cipher, and other examples are a handful. The enciphering method described in this article uses a self-invertible key matrix and an adjacency matrix of the minimal spanning trees of some specific graphs, such as the Antenna graph, and Diamond graph to encrypt and decrypt the messages that are provided to it in order to produce a complex cipher text. We can decode the ciphertext without computing the inverse of the key matrix since we are employing the self-invertible matrix as a key matrix, whose inverse always exists. Our ability to find the inverse of a key matrix is made easier by the reduction in computing complexity.

Key Words: Graph Encryption, Antenna graph, Diamond graph, MST, Self-Invertible Matrix.

1. Introduction:

The mathematical technique of cryptography is employed to increase the security of data transfers and to safeguard communications, data, and images from hackers. Plain text and cipher text are both written in the framework of alphabets; however, they are not even the same alphabets. Sometimes letters or messages are written using certain characters, such as punctuation, numbers, blanks, or other unusual characters. The message units in this work 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	27	28	29

Table 1.0. Encoded Table

The concepts of graph theory provide a crucial foundation for cryptography and have several applications in mathematics and the study of mathematics [13]. In the area of cryptography, graph theory is applied extensively [13]. With the help of a lower triangular matrix acting as the key matrix, the concept of an encryption approach using a full graph and a

Hamiltonian walk was applied in [16]. The upper triangular matrix was used as a key matrix in both cases of a novel message encoding and decoding strategy using graph labelling that was described in [2]. In [14,16], the least spanning tree, full graph, and cycle graph symmetric encryption method was described. [10] used the upper triangular matrix as a key matrix to illustrate the connection between graph theory and cryptography. All of the symmetric encryption methods previously mentioned employed the same key, which is frequently lower and upper triangular, for both sender and recipient. Over any kind of medians, both users share these keys. It is easy to break the plan if the middlemen are aware of it. Similar difficulties arise when sharing the key matrix via an unsecured channel. To decrease this, reinforce the key, and increase security, we have proposed the new approach.

The approach that has been proposed in this work uses the self-invertible key matrix [1,7,8,9] as the key matrix. As a result, we can perform the decryption process without needing to figure the inverse of the key matrix. The sender must first determine the adjacency matrix of an A-graph [2] or Centipede [15] or Domino graph [15] using the supplied message units as the graph vertices. The produced self-invertible key matrix can then be multiplied by this adjacency matrix. The output was then transmitted to the recipient on an unprotected channel, and by using the reverse procedure, the recipient should be able to view the original message. This study's remaining section is characterised as follows: In Section 2, it was explained how to generate a self-inverting key matrix. Section 3 displays a few particular graphs, Section 4 explains the new suggested approach, and Section 5 displays an implementation example. The conclusion and a few suggestions for additional research are presented in Section 6.

2. Self-Invertible Key Matrix Generation:

If $G = G^{-1}$, or $G \cdot G^{-1} = G^{-1} \cdot G = I$ under modulo p then a matrix G is said to be self-invertible matrix, construct a self-invertible matrix by doing the actions listed below.

(i) Take any arbitrary $\frac{n}{2} \times \frac{n}{2}$ matrix G_{22}. With the help of G_{22} we may compute the other $\frac{n}{2} \times \frac{n}{2}$ matrices by the following properties:

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

Following the computation of $G_{11,}G_{12}, G_{21},$ and G_{22}, the self-invertible matrix G was produced by,

$$G = \begin{bmatrix} G_{11} & G_{12} \\ G_{21} & G_{22} \end{bmatrix} = \left[\begin{array}{ccc:cc} g_{11} & g_{12} & \cdots & \cdots & g_{1n} \\ g_{21} & g_{22} & \cdots & \cdots & g_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \hdashline \cdots & \cdots & \cdots & \cdots & \cdots \\ g_{n1} & g_{n2} & \cdots & \cdots & g_{nn} \end{array}\right]$$

(ii) Consider the random G_{22} matrix of order $(n-1) \times (n-1)$, where n being the order of adjacency matrix.

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

$G_{11} = -\lambda = -$[one of the eigen value of G_{22}], G_{12} and G_{21} are calculated by finding consistent solution of equation $G_{21} \cdot G_{12} = I - (G_{22})^2$

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

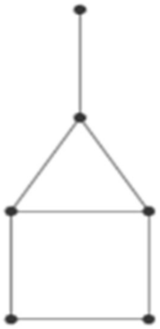
$$G = \begin{bmatrix} G_{11} & G_{12} \\ G_{21} & G_{22} \end{bmatrix} = \left[\begin{array}{ccc:cc} g_{11} & g_{12} & \cdots & \cdots & g_{1n} \\ \hdashline g_{21} & g_{22} & \cdots & \cdots & g_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ g_{n1} & g_{n2} & \cdots & \cdots & g_{nn} \end{array}\right]$$

3. Specific graphs:

Graph: An ordered pair (V, E), where V is a graph's vertices and E is its edges, is known as a graph and is nothing more than a collection of vertices and edges.

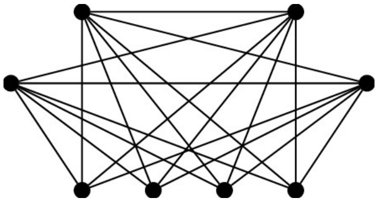
Antenna Graph:

The graph with 6 vertices and 7 edges illustrated below is known antenna graph.



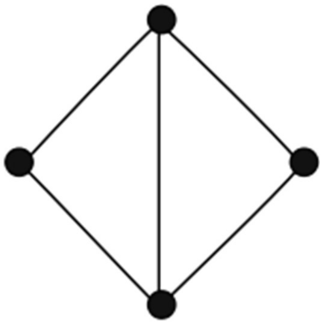
Complete Tripartite Graph:

Complete tripartite graph is the k=3 case of a complete *k*-partite graph. In other words, it is a tripartite graph (i.e., a set of graph vertices decomposed into three disjoint sets such that no two graph vertices within the same set are adjacent) such that every vertex of each set graph vertices is adjacent to every vertex in the other two sets. If there are p, q and r graph vertices in the three sets, the complete tripartite graph (sometimes also called a complete trigraph) is denoted $K_{p,q,r}$.



Diamond Graph:

The diamond graph is the simple graph on 4 vertices and 5 edges illustrated below. It is isomorphic to the complete tripartite graph $K_{1,1,2}$ and $K_4 - e$ where $K_4 - e$ is the tetrahedral graph with any edge removed. The diamond graph is also sometimes known as the double triangle graph



4. The proposed cryptosystem

The suggested approach was described in depth in this part, and it involves employing the self-invertible key matrix as the key matrix together with the adjacency matrices of the minimum spanning trees of Antenna Graph and Diamond graph.

Algorithm for proposed encryption technique: The steps listed below are used to perform encryption:

Step 1: The special character A is used to identify the letter that the specified message unit starts with. We generate the necessary Antenna graph, Diamond graph by linking the sequential letters in the provided plain text message units.

Step 2: Using an encoded table, the message units are translated into their numerical equivalents (Table1).

Step 3: To determine the weights of each edge in a graph, we compute the numerical difference between the two neighbouring vertices.

Step 4: For the associated graph, the Minimal Spanning Tree was calculated.

Step 5: After performing addition modulo p, the adjacency matrix for this graph was generated.

Step 6: The self-invertible matrix is constructed using the shared data and the methods described in Part 2.

Step 7: The encrypted information for the original plaintext message was obtained by multiplying the adjacency matrix by the created self-invertible key matrix.

Step 8: Lastly, these encrypted matrices, the adjacency matrix order, and the matrices that were used to construct the self-invertible matrices can all be shared with another user either in the form of row or column matrices.

Algorithm for proposed decryption technique:

Step 1: By going back over the information they have received, the receiver can ascertain the order of the matrix, the encrypted matrix, and the matrix that helps in the creation of the self-invertible key matrix.

Step 2: Using the details from Section 2, the receiver should produce the self-invertible key matrix.

Step 3: Multiply the self-invertible matrix created in step 2 by the encrypted matrix.

Step 4: The receiver should then add modulo p to the step 3 resultant matrix to produce the adjacency matrix of the appropriate graph.

Step 5: The receiver can generate the Minimum Spanning Tree of the specified graph with the nodes and the supplied weights after retracing the graph.

Step 6: The weights and associated vertices are added to calculate the message. Vertex v1 is identified by the letter A and has a value of 1, while v2 is defined as v1 + weight e1, among other things.

5. Implementation example:

5.1 Using Antenna graph: Suppose that User A(sender) wants to send the message "CAMEL" to another user (User B(receiver)) using the technique which is explained in the above section, MST of Antenna graph and its adjacency matrix, the key matrix that has been generated using Section 2.

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

Initially, we should add a special character A as the beginning letter of the given plaintext message units and then convert the given message "A CAMEL" as the vertices of an Antenna graph. The vertices are joined from bottom to top by connecting sequential letters in the given message units.

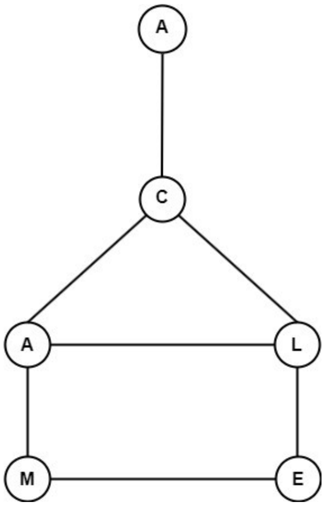
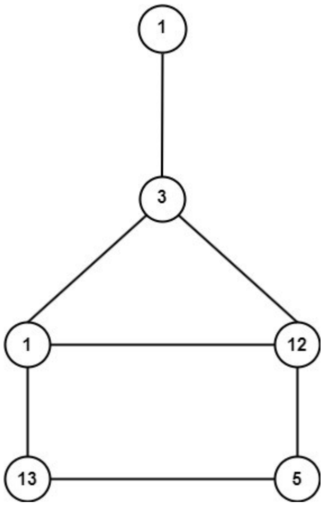


Figure 1. Antenna Graph for an original message unit

Using the encoded table (Table 1) we get, $A \rightarrow 1,\ C \rightarrow 3,\ A \rightarrow 1,\ M \rightarrow 13,\ E \rightarrow 5, O \rightarrow$



12.

Figure 2. Encoded Antenna Graph

Weights of the edges of this graph are assigned by finding the numerical distance between the consecutive two connected vertices and then take addition modulo 29 as we are using 29 characters in the given encoded table (e1= Code C– Code A, e2 = Code A – Code C, …)

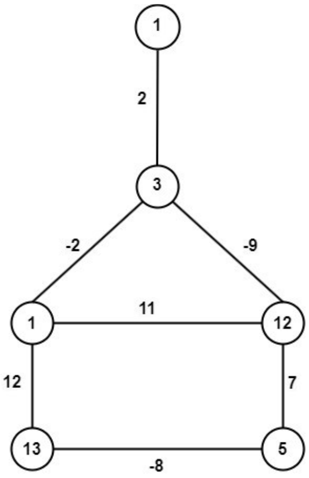


Figure 3. Encoded Antenna graph with edge weights

Minimum spanning tree for the above graph was computed.

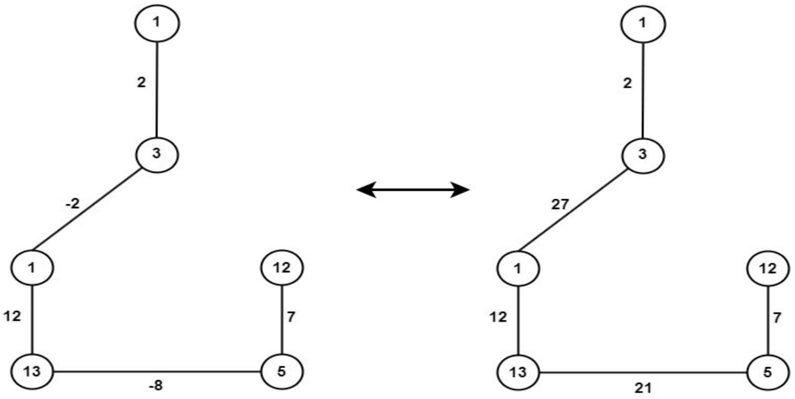


Figure 4. Minimum Spanning tree of an Antenna graph

The corresponding adjacency matrix of the above Minimum Spanning Tree was computed, name it as ‘M’

$$M = \begin{bmatrix} 0 & 2 & 0 & 0 & 0 & 0 \\ 2 & 0 & 27 & 0 & 0 & 0 \\ 0 & 27 & 0 & 12 & 0 & 0 \\ 0 & 0 & 12 & 0 & 21 & 0 \\ 0 & 0 & 0 & 21 & 0 & 7 \\ 0 & 0 & 0 & 0 & 7 & 0 \end{bmatrix}$$

Now that the key matrix needs to be calculated, we use the $\frac{n}{2} \times \frac{n}{2}$ matrix G_{22} to construct the self-invertible key matrix G.

$$\text{Let } G_{22} = \begin{bmatrix} 1 & 4 & 1 \\ 4 & 1 & 5 \\ 9 & 6 & 8 \end{bmatrix} \text{ then } G_{11} = \begin{bmatrix} 28 & 25 & 27 \\ 25 & 28 & 24 \\ 20 & 23 & 21 \end{bmatrix},$$

$$G_{12} = I - G_{11} = \begin{bmatrix} 2 & 4 & 2 \\ 4 & 2 & 5 \\ 9 & 6 & 9 \end{bmatrix}, \text{and } G_{21} = I + G_{11} = \begin{bmatrix} 0 & 25 & 27 \\ 25 & 0 & 24 \\ 20 & 23 & 22 \end{bmatrix}$$

$$\therefore G = \begin{bmatrix} G_{11} & G_{12} \\ G_{21} & G_{22} \end{bmatrix} = \begin{bmatrix} 28 & 25 & 27 & 2 & 4 & 2 \\ 25 & 28 & 24 & 4 & 2 & 5 \\ 20 & 23 & 21 & 9 & 6 & 9 \\ 0 & 25 & 27 & 1 & 4 & 2 \\ 25 & 0 & 24 & 4 & 1 & 5 \\ 20 & 23 & 22 & 9 & 6 & 8 \end{bmatrix}$$

Finally, the encrypted matrix was computed by multiplying M and G

$$C = M \cdot G = \begin{bmatrix} 0 & 2 & 0 & 0 & 0 & 0 \\ 2 & 0 & 27 & 0 & 0 & 0 \\ 0 & 27 & 0 & 12 & 0 & 0 \\ 0 & 0 & 12 & 0 & 21 & 0 \\ 0 & 0 & 0 & 21 & 0 & 7 \\ 0 & 0 & 0 & 0 & 7 & 0 \end{bmatrix} \cdot \begin{bmatrix} 28 & 25 & 27 & 2 & 4 & 2 \\ 25 & 28 & 24 & 4 & 2 & 5 \\ 20 & 23 & 21 & 9 & 6 & 9 \\ 0 & 25 & 27 & 1 & 4 & 2 \\ 25 & 0 & 24 & 4 & 1 & 5 \\ 20 & 23 & 22 & 9 & 6 & 8 \end{bmatrix}$$

$$C = \begin{bmatrix} 50 & 56 & 48 & 8 & 4 & 10 \\ 596 & 671 & 621 & 247 & 170 & 247 \\ 675 & 1056 & 972 & 120 & 102 & 159 \\ 765 & 276 & 756 & 192 & 93 & 213 \\ 140 & 686 & 721 & 84 & 126 & 98 \\ 175 & 0 & 168 & 28 & 7 & 35 \end{bmatrix}$$

The encrypted matrix can be transformed into a row or column matrix and delivered to another user over any type of median with specifying the order of the matrix, the matrix which aids in computing the self-invertible matrix.

[6, 50, 56, 48, 8, 4, 10, 596, 671, 621, 247, 170, 247, 675, 1056, 972, 120, 102, 159, 765, 276, 756, 192, 93, 140, 686, 721, 84, 126, 98, 175, 0, 168, 28, 7, 35; 1, 4, 2, 4, 1, 5, 9, 6,8].

Decryption- User B (The receiver): Decryption is done by using 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.

$$C = \begin{bmatrix} 50 & 56 & 48 & 8 & 4 & 10 \\ 596 & 671 & 621 & 247 & 170 & 247 \\ 675 & 1056 & 972 & 120 & 102 & 159 \\ 765 & 276 & 756 & 192 & 93 & 213 \\ 140 & 686 & 721 & 84 & 126 & 98 \\ 175 & 0 & 168 & 28 & 7 & 35 \end{bmatrix}$$

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

$$G = \begin{bmatrix} G_{11} & G_{12} \\ G_{21} & G_{22} \end{bmatrix} = \begin{bmatrix} 28 & 25 & 27 & 2 & 4 & 2 \\ 25 & 28 & 24 & 4 & 2 & 5 \\ 20 & 23 & 21 & 9 & 6 & 9 \\ 0 & 25 & 27 & 1 & 4 & 2 \\ 25 & 0 & 24 & 4 & 1 & 5 \\ 20 & 23 & 22 & 9 & 6 & 8 \end{bmatrix}$$

$$C \cdot G = \begin{bmatrix} 50 & 56 & 48 & 8 & 4 & 10 \\ 596 & 671 & 621 & 247 & 170 & 247 \\ 675 & 1056 & 972 & 120 & 102 & 159 \\ 765 & 276 & 756 & 192 & 93 & 213 \\ 140 & 686 & 721 & 84 & 126 & 98 \\ 175 & 0 & 168 & 28 & 7 & 35 \end{bmatrix} \cdot \begin{bmatrix} 28 & 25 & 27 & 2 & 4 & 2 \\ 25 & 28 & 24 & 4 & 2 & 5 \\ 20 & 23 & 21 & 9 & 6 & 9 \\ 0 & 25 & 27 & 1 & 4 & 2 \\ 25 & 0 & 24 & 4 & 1 & 5 \\ 20 & 23 & 22 & 9 & 6 & 8 \end{bmatrix}$$

$$= \begin{bmatrix} 4060 & 4352 & 4234 & 870 & 696 & 928 \\ 55073 & 59827 & 61420 & 12615 & 10092 & 13456 \\ 70470 & 75456 & 73167 & 16281 & 12180 & 17400 \\ 50025 & 53940 & 55257 & 11919 & 10287 & 12267 \\ 40600 & 43645 & 42833 & 10983 & 7308 & 11781 \\ 9135 & 9744 & 9947 & 2233 & 2037 & 2233 \end{bmatrix}$$

Taking addition modulo 29, we get, 4060(mod 29) = 0, 4352(mod 29) = 2, 4234(mod 29) = 0, …, 2233 (mod 29) = 0.

$$\therefore C \cdot G = \begin{bmatrix} 0 & 2 & 0 & 0 & 0 & 0 \\ 2 & 0 & 27 & 0 & 0 & 0 \\ 0 & 27 & 0 & 12 & 0 & 0 \\ 0 & 0 & 12 & 0 & 21 & 0 \\ 0 & 0 & 0 & 21 & 0 & 7 \\ 0 & 0 & 0 & 0 & 7 & 0 \end{bmatrix} = M$$

The Corresponding Minimum Spanning Tree for the above adjacency matrix was formed

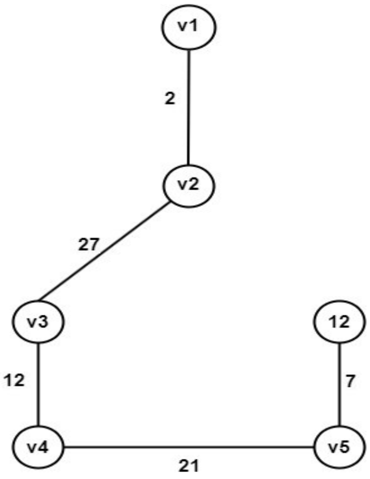


Figure 5. Antenna graph of decrypted adjacency matrix.

The vertices(nodes) of the above graph 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 + 2 = 3, v3 = 3 + 27 = 30 = 1, v4 = 1 + 12 = 13, v5 = 13 + 21 = 34 = 5, v6 = 5 + 7 = 12.

$\therefore$ The vertices are $1, 3, 1, 13, 5, 12.$

$\therefore$The message is $1 \rightarrow A$, $3 \rightarrow C, 1 \rightarrow A,$ $13 \rightarrow M,$ $5 \rightarrow E, 12 \rightarrow L$ i.e., A CAMEL.

5.2 Using Diamond graph: Suppose that the sender wants to send the message "PEN" to another user using the technique which is explained in Section 4, using Minimum Spanning Tree of Diamond graph and its corresponding adjacency matrix, the self-invertible key matrix that has been explained in Section 2.

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

Initially, we should add a special character A to the beginning letter of the given plaintext message units and then convert the given message "A PEN" as the vertices of Diamond graph. The vertices are joined from vertex1 to vertex 4 by putting sequential letters in the given message units as the vertices.

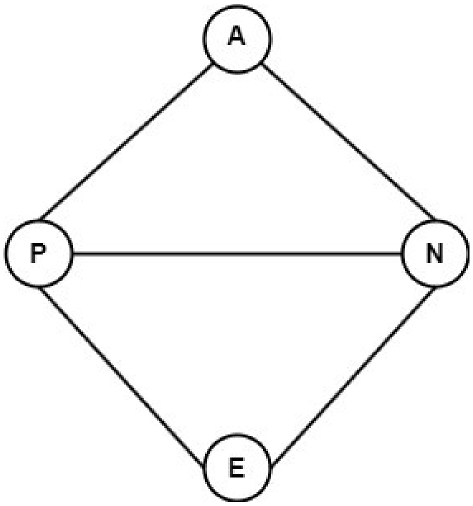


Figure 6. Diamond graph of original message

Using the encoded table (Table 1) we get, $A \to 1,\ P \to 16,\ \ E \to 5,\ N \to 14$.

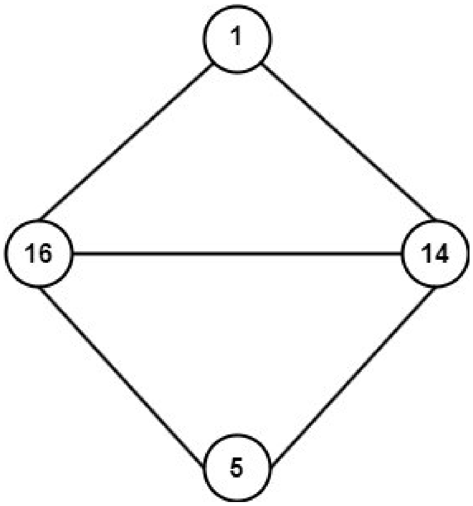


Figure 7. Encoded Diamond graph

Weights of the edges of this graph are assigned by finding the numerical distance between the consecutive two connected vertices and then take addition modulo 29 as we are utilising 29 character in the given encoded table(Table 1) (e1= Code P – Code A, e2 = Code E – CodeP ,…)

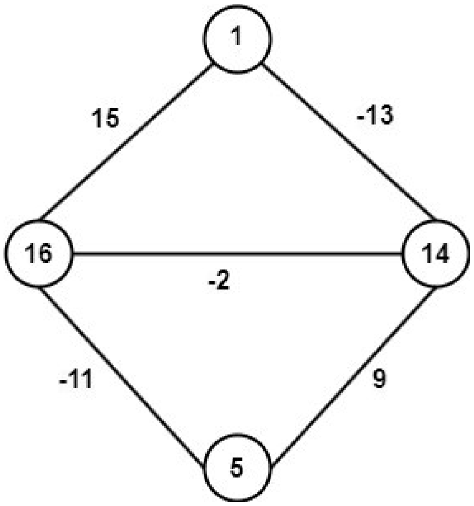


Figure 8. Diamond graph with weights

The Minimum Spanning Tree of the above graph was computed

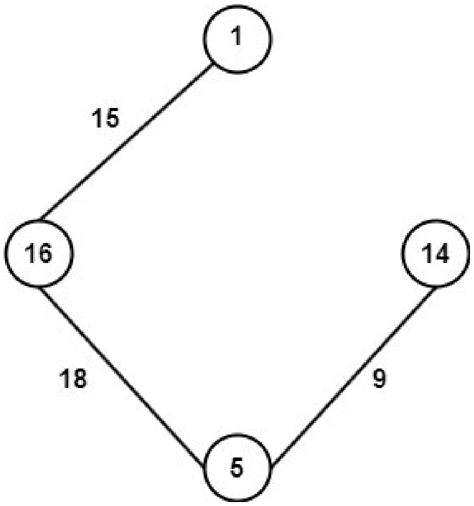


Figure 9. MST of Diamond graph

The corresponding adjacency matrix of the above graph was computed, name it as 'M'

$$M = \begin{bmatrix} 0 & 15 & 0 & 0 \\ 15 & 0 & 18 & 0 \\ 0 & 18 & 0 & 9 \\ 0 & 0 & 9 & 0 \end{bmatrix}$$

To compute the key matrix, we construct the self-invertible key matrix 'G'.

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

$$G_{22} = \begin{bmatrix} 28 & 0 & 2 \\ 23 & 2 & 6 \\ 0 & 0 & 1 \end{bmatrix}$$

The eigen values of G_{22} are $\lambda_1 = 1$, λ_2 =2, $\lambda_3 = 28$

The other matrices are $G_{11} = -\lambda_3 = -2 = 27(mod\ 29) \implies G_{11} = [27]$

The consistent solutions of $G_{21} \cdot G_{12} = I - (G_{22})^2$ are $G_{12} = [\ 23\ \ 3\ \ 6]$, $G_{21} = \begin{bmatrix} 0 \\ 28 \\ 0 \end{bmatrix}$

Hence the self-invertible key matrix is $G = \begin{bmatrix} G_{11} & G_{12} \\ G_{21} & G_{22} \end{bmatrix} = \begin{bmatrix} 27 & 23 & 3 & 6 \\ 0 & 28 & 0 & 2 \\ 28 & 23 & 2 & 6 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

Finally, the encrypted matrix was computed by multiplying M and G

$$C = M \cdot G = \begin{bmatrix} 0 & 15 & 0 & 0 \\ 15 & 0 & 18 & 0 \\ 0 & 18 & 0 & 9 \\ 0 & 0 & 9 & 0 \end{bmatrix} \cdot \begin{bmatrix} 27 & 23 & 3 & 6 \\ 0 & 28 & 0 & 2 \\ 28 & 23 & 2 & 6 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$C = \begin{bmatrix} 0 & 420 & 0 & 30 \\ 909 & 759 & 81 & 198 \\ 0 & 504 & 0 & 45 \\ 252 & 207 & 18 & 54 \end{bmatrix}$$

The encrypted matrix can be transformed into a row or column matrix and delivered to another user over any type of median with specifying the order of the matrix, the matrix which aids in computing the self-invertible matrix.

$[\,4, 0, 420, 0, 30, 909, 759, 81, 198, 0, 504, 0, 45, 252, 207, 18, 54; 28, 0, 2, 23, 2, 6, 0, 0, 1]$.

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

$$C = \begin{bmatrix} 0 & 420 & 0 & 30 \\ 909 & 759 & 81 & 198 \\ 0 & 504 & 0 & 45 \\ 252 & 207 & 18 & 54 \end{bmatrix}$$

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

$$G = \begin{bmatrix} G_{11} & G_{12} \\ G_{21} & G_{22} \end{bmatrix} = \begin{bmatrix} 27 & 23 & 3 & 6 \\ 0 & 28 & 0 & 2 \\ 28 & 23 & 2 & 6 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$C \cdot G = \begin{bmatrix} 0 & 420 & 0 & 30 \\ 909 & 759 & 81 & 198 \\ 0 & 504 & 0 & 45 \\ 252 & 207 & 18 & 54 \end{bmatrix} \cdot \begin{bmatrix} 27 & 23 & 3 & 6 \\ 0 & 28 & 0 & 2 \\ 28 & 23 & 2 & 6 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 11760 & 0 & 870 \\ 26811 & 44022 & 2889 & 7656 \\ 0 & 14112 & 0 & 1053 \\ 7308 & 12006 & 792 & 2088 \end{bmatrix}$$

Taking addition modulo 29 we get, 0(mod 29) = 0, 11760(mod 29) = 12, 0(mod 29) = 0, …, 2088 (mod 29) = 0.

$$\therefore C \cdot G = \begin{bmatrix} 0 & 15 & 0 & 0 \\ 15 & 0 & 18 & 0 \\ 0 & 18 & 0 & 9 \\ 0 & 0 & 9 & 0 \end{bmatrix} = M$$

The Corresponding MST of the above adjacency matrix was formed

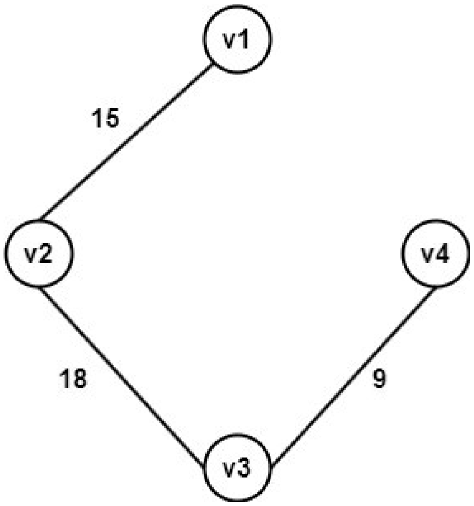


Figure 10. MST of decrypted adjacency matrix.

The vertices(nodes) of the above graph 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 + 15 = 16, v3 = 16 + 18 = 34=5(mod 29), v4 = 5 + 9 = 14.

∴ The vertices are $1, 16, 5, 14$.

∴The message is $1 \rightarrow A\ ,\ 16 \rightarrow P, 5 \rightarrow E,\ 14 \rightarrow N.$ i.e., A PEN.

6. Conclusion:

Nowadays, protecting the security of our information is essential. To do this, many publications make use of symmetric encryption methods like the Caesar cypher, the Hill cypher, graphical methods, and others. For the purpose of enhancing the security of our data, this study suggests a new method for cryptosystem encryption, it uses a self-invertible matrix as the key matrix together with adjacency matrices of MST for numerous graphs, including the Antenna graph and Diamond Graph. This suggested strategy can avoid the intermediate and is more effective; any simple graph may make use of the suggested method. We just exchange a $\frac{n}{2} \times \frac{n}{2}$ or $(n-1) \times (n-1)$ matrix that aids in creating the self-invertible matrix in the recommended way, which employs a straightforward encryption and decryption mechanism with higher security. It improves the security of the key against hacking by reducing the complexity necessary in sharing the shared key. As a result of utilising a self-invertible matrix as the key matrix, it is not necessary to determine the key matrix's inverse in order to decode the ciphertext. In this research, this approach of message encryption and decryption is used together with a few graph theory concepts. This technology will be enhanced in the future and used to a range of other challenging graph theory ideas and more encryption techniques, including image and video encryption, among others.

References:

1. Acharya, B., Rath, G.S., Patra, S.K., Panigrahy, S.K., A Novel methods of generating self-invertible matrix for Hill Cipher Algorithm, International Journal of Security(2007), pp.14-21.
2. Alastair Farrugia, Self-complementary graphs and generalisations: a comprehensive reference manual, University of Malta, 1999.

3. Amudha P, Jayapriya J, Gowri J, An algorithmic approach for encryption using graph Labeling, Journal of physcis,1770(1): 012072, (2021), pp. 375-384, https://iopscience.iop.org/article/10.1088/1742-6596/1770/1/012072.
4. Arumugam S, Ramachandran S, Invitation to Graph theory, Scitech Publications, (2015).
5. Brandstädt, Andreas and Le, Van Bang and Spinrad, Jeremy P, Graph Classes: A Survey, Society for Industrial and Applied Mathematics (1999) https://epubs.siam.org/doi/book/10.1137/1.9780898719796
6. Diffie, W., Hellman, M., New directions in Cryptography, IEEE Trans. Inf. Theory 22 (6), (1976), pp.644-654.
7. 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, (2022), https://publishoa.com/index.php/journal/article/view/816 , pp.1821-1826.
8. 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/IJST/v15i44.1861
9. 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
10. Nandhini R, Maheswari V and Balaji V, A Graph Theory Approach on Cryptography, Journal of Computational Mathematics,2(1), (2018), pp.97-104 https://doi.org/10.26524/jcm32.
11. Neal Koblitz, A course in Number Theory and Cryptography, second edition, Springer.
12. Saniah Sulaiman Zurina Mohd Hanpi, Extensive analysis on Images Encryption using Hybrid Elliptic Curve Cryptosystem and Hill cipher, Journal of Computer Science,17(3),(2021), pp.221-320, https://doi.org/10.3844/jcssp.2021.221.230.
13. Uma Dixit, Cryptography a Graph theory approach, International journal of Advance Research in Science and Engineering,6(01),(2017), pp.218-221, http://www.ijarse.com/images/fullpdf/1504001715_BVCNSCS17072_Dr_Uma_Dixit.pdf
14. Weal Mahmoud AI Etaiwi, Encryption algorithm using Graph theory, Journal of Scientific Research and Reports, 3(19), (2014), pp. 2519-2527.
15. Weisstein, Eric W., Graph Theory, Math World.
16. 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), pp.102-107.
17. Ziad E. Dawahdeh, Shahrul N. Yaakob, Rozmie Razif bin Othman, A new image encryption technique combining Elliptic Curve Cryptosystem with Hill Cipher, Journal of King Saud University - Computer and Information Sciences,30(3),(2018), pp.349-355.