A Novel Encoding Technique Using a Self Invertible Key Matrix and the Adjacency Matrices of Pan Graphs

Mr Mohan P (mohan14palani@gmail.com)
Vels Institute of Science, Technology & Advanced Studies (VISTAS)
Dr Rajendran K
Vels Institute of Science, Technology & Advanced Studies (VISTAS)
Dr Rajesh A
Vels Institute of Science, Technology & Advanced Studies (VISTAS)

Research Article

Keywords: Symmetric encryption, Graph encryption, Pan Graph, Self-Invertible Matrix, Adjacency Matrix

Posted Date: August 10th, 2023

DOI: https://doi.org/10.21203/rs.3.rs-3236543/v1

Additional Declarations: No competing interests reported.

A NOVEL ENCODING TECHNIQUE USING A SELF INVERTIBLE KEY MATRIX AND THE ADJACENCY MATRICES OF PAN GRAPHS

[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.

[2]Assistant Professor, Department of Mathematics, SRM Arts and Science College.

[1]mohan14palani@gmail.com, [2]mohanmat@srmasc.ac.in

[3] Associate Professor, Department of Mathematics, Vels Institute of Science, Technology & Advanced Studies (VISTAS), India. [3] gkrajendra59@gmail.com,

[4] Associate Professor, Department of CSE, Vels Institute of Science, Technology & Advanced Studies (VISTAS), India. [4] arajesh.se@velsuniv.ac.in

ABSTRACT:

Message encryption techniques are now the most important safeguards for our data and communications. The use of networks and the internet has sped up the development of message encryption technology. If sensitive, private messages are shared over unsecured networks, there is a possibility of an attack, theft, or hacking of the communications. It has been revealed that using cryptographic techniques is essential for shortening this period. The Caesar Cipher, Hill Cipher, and others are a few examples of the symmetric enciphering methods. The enciphering method given in this article encrypts and decrypts the input messages to generate a complex cipher using a self-invertible key matrix and an adjacency matrix of the pan graphs. Since the key matrix we are using is the self-invertible matrix, whose inverse always exists, we can decode the cipher without having to compute the inverse of the key matrix. The reduction in computational complexity facilitates our capacity to determine the inverse of a key matrix.

Key Words: Symmetric encryption, Graph encryption, Pan Graph, Self-Invertible Matrix, Adjacency Matrix.

1. Introduction:

The mathematical technique of cryptography is used to improve data transmission security and protect conversations, data, and images from attackers. Although alphabets are used to write both plain text and encrypted text. Letters or communications occasionally contain unusual characters, such as punctuation, digits, blanks, or other symbols. The message units in this work are encrypted using the encoded table below.

A	B	C	D	E	F	G	H	I	J	K	L	M	…	…	…	V	W	X	Y	Z		.	?
1	2	3	4	5	6	7	8	9	10	11	12	13	…	…	…	22	23	24	25	26	27	28	29

Table 1.0. Encoded Table

The use of graph labelling in a novel message encoding and decoding method was disclosed in [3]. [11] used the upper triangular matrix as a key matrix to show how graph theory and cryptography are related. Graph theory concepts have many applications in both mathematics and the study of mathematics [14]. They also form the foundation for cryptography. In the subject of cryptography, graph theory is widely used [14]. The complete graph, cycle graph, and symmetric minimum spanning tree encryption techniques were described in [14,15]. The upper triangular matrix was utilized as a key matrix in [17], which presented the concept of an encryption approach utilizing a complete graph and a Hamiltonian path. Each of the symmetric encryption methods previously covered employed the same key, which is frequently either a

lower triangular or upper triangular, for sender and the end user. Both users utilize these keys for all median kinds. This tactic can be easily defeated if the intermediates are aware of it. The key matrix is difficult to share via an unsecured connection.

We devised a unique approach to alleviate this, to strengthen the key, and increase security for the supplied information in order to eliminate this terminology, generate more security, and strengthen the key. We have put forth a novel method that encrypts and decrypts data using the adjacency matrix of a complete graph of a cycle graph and the key matrix as a self-invertible matrix [1,7,8,9,10]. Since the key matrix is self-invertible, the computation of the inverse is not necessary to decode the cipher. It aids in making the process of discovering the inverse less difficult. Additionally, we are not sharing the whole key matrix. This enhances data security and lessens the chance that the key matrix may be compromised.

The approach proposed in this work is implemented using the notion of a minimal spanning tree of a complete graph and its corresponding adjacency matrix. Here, the self-invertible matrix is utilized as the key to encrypt and decode the original message units in order to improve security and provide a new and effective approach. Retrieving the original message is quite challenging unless the intermediaries are aware of this procedure. This work's remaining portions are specified as follows: The procedure for creating a self-invertible key matrix was covered in Section II of the article. Section III details the proposed technique. An implementation example will be provided in Section IV. The conclusion is presented in Section V, along with recommendations for more research.

2. Self-Invertible Key Matrix Generation:

If $S = S^{-1}$, or $S \cdot S^{-1} = S^{-1} \cdot S = I$, then the matrix S is said to be self-invertible matrix under addition modulo p, the self-invertible matrix was generated by using the following procedures,

2.1 Generating Procedure-I of Self-Invertible key matrix of even order:

Let us consider any random S_{22} matrix of order $\frac{n}{2} \times \frac{n}{2}$, where n being the order of adjacency matrix, n being even.

The remaining $\frac{n}{2} \times \frac{n}{2}$ matrices are calculated with the help of S_{22}, by applying the following characteristics,

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

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

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

2.2 Generating Procedure-II of Self-Invertible key matrix for any order:

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,

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

2.3 Generating Procedure III of Self-Invertible key matrix of any order:

Let us select any random non-singular square matrix G, find the Inverse of the matrix G, choose a diagonal matrix D whose elements are ± 1 but not all them are equal.

The self-invertible matrix was computed by using $G \cdot D \cdot G^{-1} = S$. Under modulo p.

3. Pan graph based enciphering technique

The suggested approach, which was explained in this section, combines the adjacency matrices of the Pan graphs with the self-invertible key matrix as the key matrix.

Algorithm for proposed encryption technique: To perform encryption, follow the procedures given below:

Step 1: To determine the initial letter of a given message unit, we start by linking the sequential letters in the supplied plain text message units to form the necessary pan graphs, starting with the special character A as the first vertex of the given pan graph.

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

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

Step 4: After taking addition modulo p, the adjacency matrix for this pan graph was created.

Step 5: The self-invertible matrix was created using the shared data and the methods described in Sections 2.1 and 2.3.

Step 6: The encrypted data for the original plaintext message was calculated by multiplying the adjacency matrix by the generated self-invertible key matrix. A user can transmit these encrypted matrices, the adjacency matrix's order, and the matrix that was used to generates the self-invertible matrix. These matrices can be sent as either row matrices or column matrices.

Algorithm for proposed decryption technique:

Step 1: By going back over the information they have received, the receiver may 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: The receiver should use the knowledge provided in Sections 2.1 and 2.3 to construct the self-invertible key matrix.

Step 3: Multiply the self-invertible matrix produced 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 necessary graph.

Step 5: The receiver can construct the necessary pan graph with the necessary nodes and weights after retracing the network.

Step 6: The weights and matching 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.

4. Implementation examples

4.1.1 Using Pan Graph (P_n for n=3):

Assume that the sender intends to communicate the word "GOD" to another user using the method described in the above Algorithm, which makes use of Pan graph P_3 and its adjacency matrix as well as the self-invertible key matrix described in Section 2.1.

Encryption- The following techniques are used to encrypt data:

The first vertex of the supplied plaintext message units should be added as an add-on character A, and the message "$A\ GOD$" should then be converted into the vertices of Pan graph P_3. The specified message units' consecutive letters are used as the vertices to connect the vertices from vertex 1 to vertex 4.

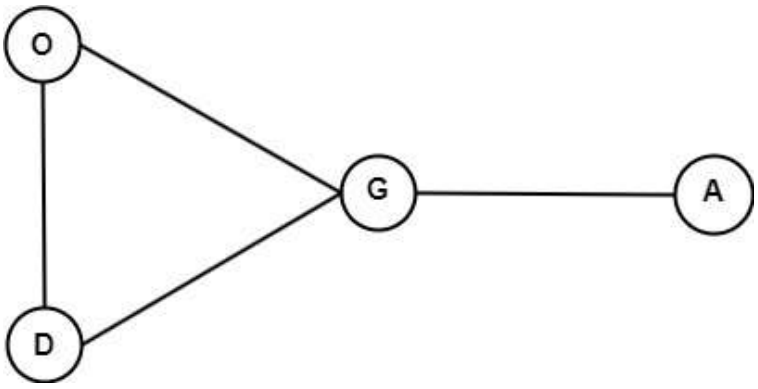

Figure 4.1 Pan graph P_3 of original message

We obtain, $A \to 1,\ G \to 7,\ \ O \to 15,\ D \to 4$ by using the provided encoded table (Table 1.0)

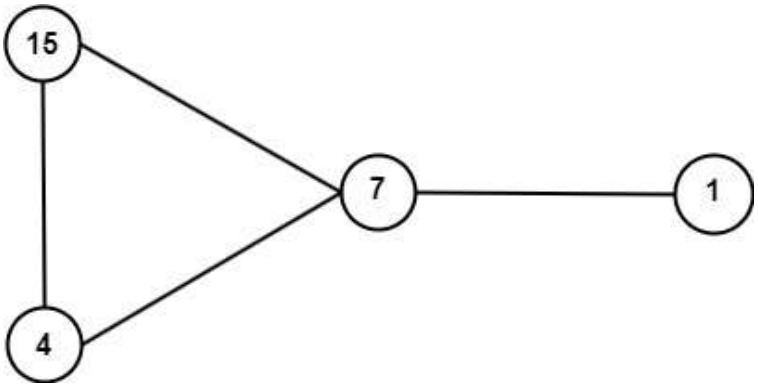

Figure 4.2. Encoded Pan graph P_3

The weights of the edges in the Pan graph are determined by calculating the numerical distance between the consecutive two linked vertices and adding them $modulo$ 29, as we are using 29 characters in the encoded table provided, (Table 1.0).

$$(e1 = \ Code\ G - Code\ A, e2 \ = \ Code\ O - Code\ G\ , \dots)$$

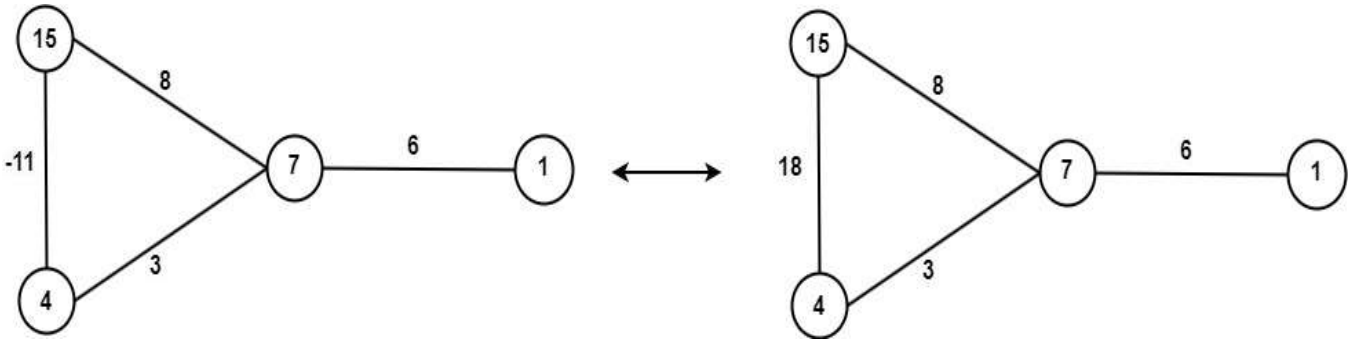

Figure 4.3. Pan graph P_3 with edge weights

The above graph's associated adjacency matrix, designated by the letter "M," has been calculated.

$$M = \begin{bmatrix} 0 & 6 & 0 & 0 \\ 6 & 0 & 8 & 3 \\ 0 & 8 & 0 & 18 \\ 0 & 3 & 18 & 0 \end{bmatrix}$$

Let the commonly shared $\frac{n}{2} \times \frac{n}{2}$ matrix $S_{22} = \begin{bmatrix} 2 & 6 \\ 0 & 1 \end{bmatrix}$. Then the remaining $\frac{n}{2} \times \frac{n}{2}$ matrices are,

$$S_{11} = \begin{bmatrix} 27 & 23 \\ 0 & 28 \end{bmatrix}, S_{12} = I - S_{11} = \begin{bmatrix} 3 & 6 \\ 0 & 2 \end{bmatrix}, S_{21} = I + S_{11} = \begin{bmatrix} 28 & 23 \\ 0 & 0 \end{bmatrix}$$

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

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

$$C = M \cdot S = \begin{bmatrix} 0 & 6 & 0 & 0 \\ 6 & 0 & 8 & 3 \\ 0 & 8 & 0 & 18 \\ 0 & 3 & 18 & 0 \end{bmatrix} \cdot \begin{bmatrix} 27 & 23 & 3 & 6 \\ 0 & 28 & 0 & 2 \\ 28 & 23 & 2 & 6 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$C = \begin{bmatrix} 0 & 168 & 0 & 12 \\ 386 & 322 & 34 & 87 \\ 0 & 224 & 0 & 34 \\ 504 & 498 & 36 & 114 \end{bmatrix}$$

The encrypted matrix, the matrix which assists in constructing the self-invertible matrix, are converted into a row or column matrices and transmitted to the end user over any type of median.

$$[\,4,0,168,0,12,386,322,34,87,0,224,0,34,504,498,36,114;2,6,0,1].$$

Decryption: The procedures below are used for decryption.

The receiver may determine the order of the matrix, the encrypted matrix, and the matrix that aids in creating the self-invertible key matrix using the information they have received.

$$C = \begin{bmatrix} 0 & 168 & 0 & 12 \\ 386 & 322 & 34 & 87 \\ 0 & 224 & 0 & 34 \\ 504 & 498 & 36 & 114 \end{bmatrix}$$

With the process explained in Section 2.1, the receiver is also producing the self-invertible matrix.

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

$$C \cdot S = \begin{bmatrix} 0 & 168 & 0 & 12 \\ 386 & 322 & 34 & 87 \\ 0 & 224 & 0 & 34 \\ 504 & 498 & 36 & 114 \end{bmatrix} \cdot \begin{bmatrix} 27 & 23 & 3 & 6 \\ 0 & 28 & 0 & 2 \\ 28 & 23 & 2 & 6 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 4704 & 0 & 348 \\ 11374 & 18676 & 1226 & 3251 \\ 0 & 6272 & 0 & 482 \\ 14616 & 26364 & 1584 & 4350 \end{bmatrix}$$

After taking addition $modulo\ 29$ we obtain,

$0(\text{mod } 29) = 0$, $4704(\text{mod } 29) = 6$, $0(\text{mod } 29) = 0$, …, $4350\ (\text{mod } 29) = 0$.

$$\therefore C \cdot S = \begin{bmatrix} 0 & 6 & 0 & 0 \\ 6 & 0 & 8 & 3 \\ 0 & 8 & 0 & 18 \\ 0 & 3 & 18 & 0 \end{bmatrix} = M$$

For the aforementioned adjacency matrix, the corresponding Pan graph P_3 was formed

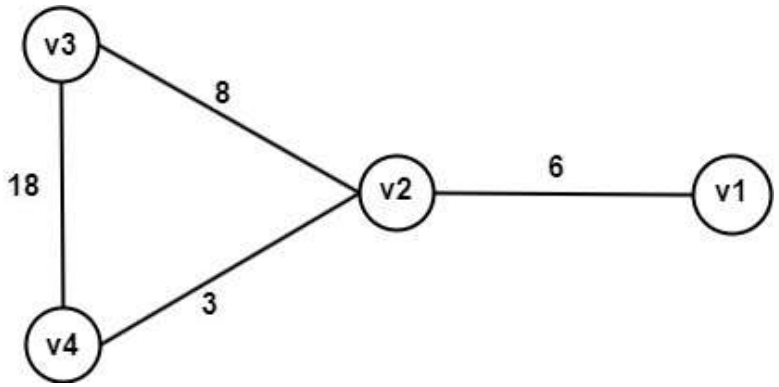

Figure 4.4. Pan graph P_3 of decrypted adjacency matrix.

The vertices of the above graph were constructed by adding the numerical equivalent values of vertex with corresponding edge. Since we are starting with an additional character A, we know that the first vertex must be 1, so the remaining vertices are found by letting $v_1 = 1$, so $v_2 = 1 + 6 = 7, v_3 = 7 + 8 = 15, v_4 = 15 + 18 = 33 = 4$.

$\therefore$ The vertices are $1, 7, 15, 4$.

$\therefore$The original message is $1 \rightarrow A$, $7 \rightarrow G, 15 \rightarrow O$, $4 \rightarrow D$. i.e., $A\ GOD$.

4.2.2. Using Pan Graph (P_n for n = 4):

Assume that the sender intends to communicate the word "NEWS" to another user using the method described in Proposed Algorithm 3, which makes use of Pan graph P_4 and its adjacency matrix as well as the self-invertible key matrix described in Section 2.3.

Encryption- The following techniques are used to encrypt data:

The first vertex of the supplied plaintext message units should be added as an add-on character A, and the message "$A\ NEWS$" should then be converted into the vertices of Pan graph P_4. The specified message units' consecutive letters are used as the vertices to connect the vertices from vertex 1 to vertex 5.

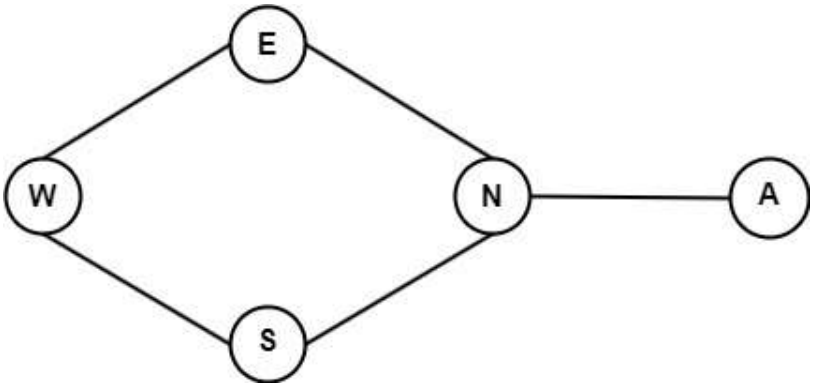

Figure 4.5. Pan graph P_4 for an original message unit

We get, $A \rightarrow 1$, $N \rightarrow 14$, $E \rightarrow 5$, $W \rightarrow 23, S \rightarrow 19$ by using the encoded table ($Table$ 1.0)

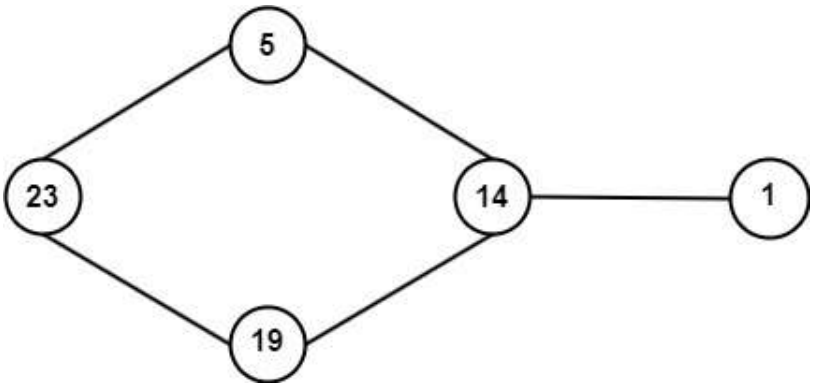

Figure 4.6. Encoded Pan graph P_4

The weights of the edges in the Pan graph are determined by calculating the numerical distance between the consecutive two linked vertices and adding them $modulo$ 29, as we are using 29 characters in the encoded table provided, (Table 1.0).

$$(e1 = Code\ N - Code\ A, e2 = Code\ E - Code\ N, \dots)$$

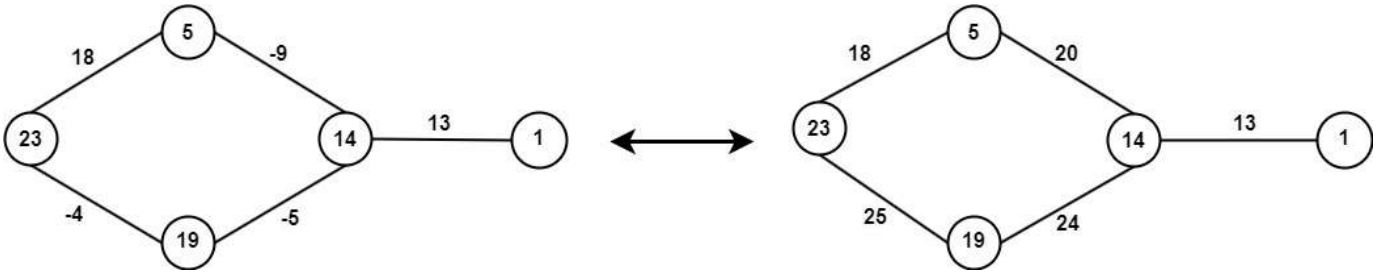

Figure 4.7. Encoded Pan graph P_4 with edge weights

The above graph's associated adjacency matrix, designated by the letter "M," has been calculated.

$$M = \begin{bmatrix} 0 & 13 & 0 & 0 & 0 \\ 13 & 0 & 20 & 0 & 24 \\ 0 & 20 & 0 & 18 & 0 \\ 0 & 0 & 18 & 0 & 25 \\ 0 & 24 & 0 & 25 & 0 \end{bmatrix}$$

The key matrix must now be computed,

Let us choose the random non-singular matrix G, $G = \begin{bmatrix} 1 & 5 & 1 & 4 & 9 \\ 2 & 3 & 6 & 1 & 2 \\ 1 & 4 & 1 & 2 & 6 \\ 2 & 5 & 1 & 1 & 3 \\ 9 & 2 & 0 & 4 & 7 \end{bmatrix}$

And take the diagonal matrix D, the entries of D are ± 1 but all the values are not equal,

$$D = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 28 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\therefore GDG^{-1} = S = \begin{bmatrix} 17 & 28 & 4 & 13 & 8 \\ 9 & 24 & 24 & 20 & 9 \\ 16 & 28 & 5 & 13 & 8 \\ 16 & 28 & 4 & 14 & 8 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Finally, by multiplying M and S, we compute the encrypted matrix.

$$C = M \cdot S = \begin{bmatrix} 0 & 13 & 0 & 0 & 0 \\ 13 & 0 & 20 & 0 & 24 \\ 0 & 20 & 0 & 18 & 0 \\ 0 & 0 & 18 & 0 & 25 \\ 0 & 24 & 0 & 25 & 0 \end{bmatrix} \cdot \begin{bmatrix} 17 & 28 & 4 & 13 & 8 \\ 9 & 24 & 24 & 20 & 9 \\ 16 & 28 & 5 & 13 & 8 \\ 16 & 28 & 4 & 14 & 8 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$C = \begin{bmatrix} 117 & 312 & 312 & 260 & 247 \\ 541 & 924 & 152 & 429 & 288 \\ 468 & 984 & 552 & 652 & 524 \\ 288 & 504 & 90 & 234 & 169 \\ 616 & 1276 & 676 & 830 & 656 \end{bmatrix}$$

The encrypted matrix, with the order of the matrix, the matrix G and the entries of diagonal Matrix D which assists in constructing the self-invertible matrix, are converted into a row or column matrices and transmitted to the end user over any type of median.

[5, 117, 312, 312, 260, 247, 541, 924, 152, 429, 288, 468, 984, 552, 652, 524, 288, 504, 90, 234, 169, 616, 1276, 676, 830, 656 ; 1, 5, 1, 4, 9, 2, 3, 6, 1, 2, 1, 4, 1, 2, 6, 2, 5, 1, 1, 3, 9, 2, 0, 4, 7;

1, 1, 28, 0, 0].

Decryption:

The receiver may determine the order of the matrix, the encrypted matrix, and the matrix that aids in creating the self-invertible key matrix using the information they have received.

$$C = \begin{bmatrix} 117 & 312 & 312 & 260 & 247 \\ 541 & 924 & 152 & 429 & 288 \\ 468 & 984 & 552 & 652 & 524 \\ 288 & 504 & 90 & 234 & 169 \\ 616 & 1276 & 676 & 830 & 656 \end{bmatrix}$$

With the process explained in Section 2.3, the receiver is also producing the self-invertible matrix.

$$S = \begin{bmatrix} 17 & 28 & 4 & 13 & 8 \\ 9 & 24 & 24 & 20 & 9 \\ 16 & 28 & 5 & 13 & 8 \\ 16 & 28 & 4 & 14 & 8 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$C \cdot S = \begin{bmatrix} 117 & 312 & 312 & 260 & 247 \\ 541 & 924 & 152 & 429 & 288 \\ 468 & 984 & 552 & 652 & 524 \\ 288 & 504 & 90 & 234 & 169 \\ 616 & 1276 & 676 & 830 & 656 \end{bmatrix} \cdot \begin{bmatrix} 17 & 28 & 4 & 13 & 8 \\ 9 & 24 & 24 & 20 & 9 \\ 16 & 28 & 5 & 13 & 8 \\ 16 & 28 & 4 & 14 & 8 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 13949 & 26780 & 10556 & 15457 & 11687 \\ 26809 & 53592 & 26816 & 33495 & 26820 \\ 36076 & 70432 & 30856 & 42068 & 32596 \\ 14616 & 29232 & 14634 & 18270 & 14641 \\ 46052 & 90040 & 39788 & 53936 & 41876 \end{bmatrix}$$

After taking addition $modulo$ 29 we obtain,

$$13949(mod\ 29) = 0, 26780(mod\ 29) = 13, 10556(mod\ 29) = 0, \dots, 41876\ (mod\ 29) = 0.$$

$$\therefore C \cdot S = \begin{bmatrix} 0 & 13 & 0 & 0 & 0 \\ 13 & 0 & 20 & 0 & 24 \\ 0 & 20 & 0 & 18 & 0 \\ 0 & 0 & 18 & 0 & 25 \\ 0 & 24 & 0 & 25 & 0 \end{bmatrix} = M$$

For the aforementioned adjacency matrix, the corresponding Pan graph P_4 was formed

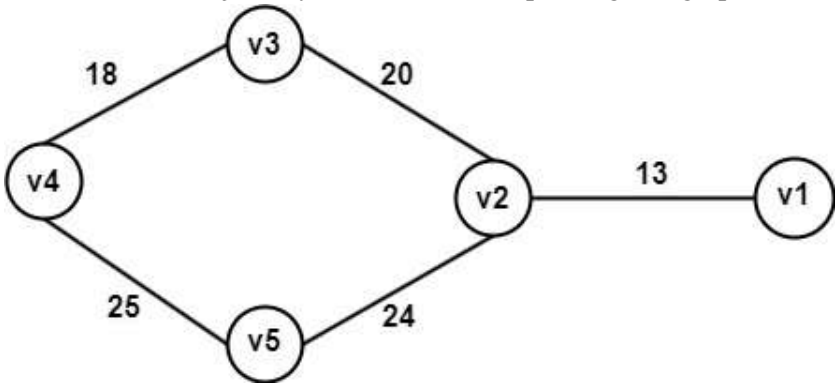

Figure 4.8. Pan graph P_4 of decrypted adjacency matrix.

The vertices of the above graph were constructed by adding the numerical equivalent values of vertex with corresponding edge. Since we are starting with an additional character A, we know that the first vertex must be 1, so the remaining vertices are found by letting v1=1, so v2= 1 + 13 = 14, v3 = 14 + 20 = 34 = 5, v4 = 5 + 18 = 23, v5 = 23 + 25 = 48 = 19.

$$\therefore \text{The vertices are } 1, 14, 5, 23, 19.$$

$$\therefore \text{The original message is } 1 \rightarrow A,\ 14 \rightarrow N,\ 5 \rightarrow E,\ 23 \rightarrow W,\ 19 \rightarrow S. \text{ i.e., } A\ NEWS.$$

4.3.3. Using Pan Graph (P_n for n = 5):

Suppose that User A(sender) wants to send the message "WORLD" to another user (User B(receiver)) using the technique using the adjacency matrix of pan graph P_5, the key matrix that has been generated using Section 2.1.

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

Initially, we should add an add-on character A as the beginning letter of the given plaintext message units and then convert the given message "A WORLD" as the vertices of a pan graph P_5. The vertices are joined by connecting sequential letters in the given message units.

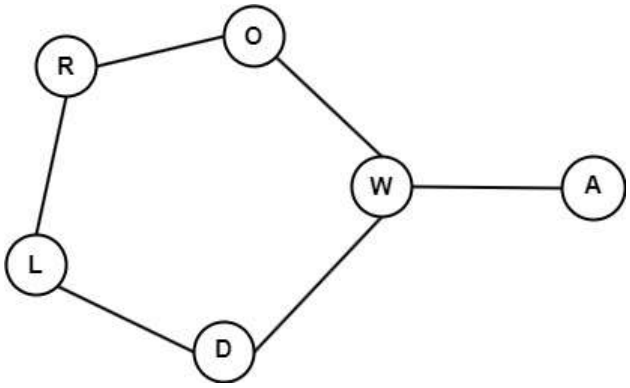

Figure 4.9 Pan graph P_5 for an original message unit

Using the encoded table (Table 1.0) we get, $A \to 1, W \to 23, O \to 15, R \to 18,\ \ L \to 12, D \to 4.$

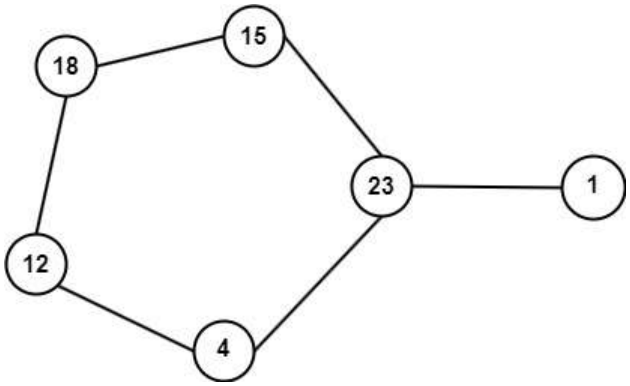

Figure 4.10. Encoded Pan graph P_5

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

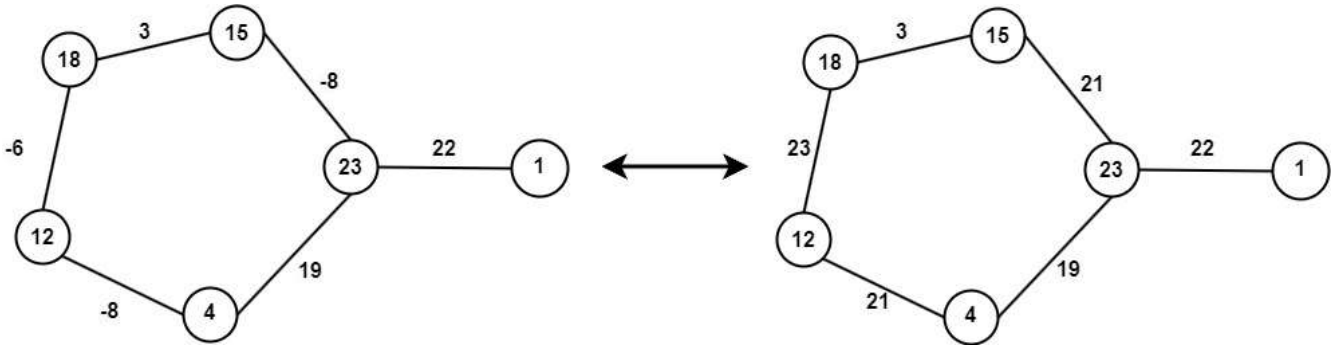

Figure 4.11. Encoded Pan graph P_5 with edge weights

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

$$M = \begin{bmatrix} 0 & 22 & 0 & 0 & 0 & 0 \\ 22 & 0 & 21 & 0 & 0 & 19 \\ 0 & 21 & 0 & 3 & 0 & 0 \\ 0 & 0 & 3 & 0 & 23 & 0 \\ 0 & 0 & 0 & 23 & 0 & 21 \\ 0 & 19 & 0 & 0 & 21 & 0 \end{bmatrix}$$

Now that the key matrix needs to be calculated, we choose the random $\frac{n}{2} \times \frac{n}{2}$ matrix S_{22} to construct the self-invertible key matrix S.

$$\text{Let } S_{22} = \begin{bmatrix} 2 & 6 & 1 \\ 7 & 1 & 5 \\ 1 & 4 & 3 \end{bmatrix} \text{ then } S_{11} = \begin{bmatrix} 27 & 23 & 28 \\ 22 & 28 & 24 \\ 28 & 25 & 26 \end{bmatrix},$$

$$S_{12} = I - S_{11} = \begin{bmatrix} 3 & 6 & 1 \\ 7 & 2 & 5 \\ 1 & 4 & 4 \end{bmatrix}, \text{ and } S_{21} = I + S_{11} = \begin{bmatrix} 28 & 23 & 28 \\ 22 & 0 & 24 \\ 28 & 25 & 27 \end{bmatrix}$$

$$\therefore S = \begin{bmatrix} S_{11} & S_{12} \\ S_{21} & S_{22} \end{bmatrix} = \begin{bmatrix} 27 & 23 & 28 & 3 & 6 & 1 \\ 22 & 28 & 24 & 7 & 2 & 5 \\ 28 & 25 & 26 & 1 & 4 & 4 \\ 28 & 23 & 28 & 2 & 6 & 1 \\ 22 & 0 & 24 & 7 & 1 & 5 \\ 28 & 25 & 27 & 1 & 4 & 3 \end{bmatrix}$$

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

$$C = M \cdot S = \begin{bmatrix} 0 & 22 & 0 & 0 & 0 & 0 \\ 22 & 0 & 21 & 0 & 0 & 19 \\ 0 & 21 & 0 & 3 & 0 & 0 \\ 0 & 0 & 3 & 0 & 23 & 0 \\ 0 & 0 & 0 & 23 & 0 & 21 \\ 0 & 19 & 0 & 0 & 21 & 0 \end{bmatrix} \cdot \begin{bmatrix} 27 & 23 & 28 & 3 & 6 & 1 \\ 22 & 28 & 24 & 7 & 2 & 5 \\ 28 & 25 & 26 & 1 & 4 & 4 \\ 28 & 23 & 28 & 2 & 6 & 1 \\ 22 & 0 & 24 & 7 & 1 & 5 \\ 28 & 25 & 27 & 1 & 4 & 3 \end{bmatrix}$$

$$C = \begin{bmatrix} 484 & 616 & 528 & 154 & 44 & 110 \\ 1714 & 1506 & 1675 & 106 & 292 & 163 \\ 546 & 657 & 588 & 153 & 60 & 108 \\ 590 & 75 & 630 & 164 & 35 & 127 \\ 1232 & 1054 & 1211 & 67 & 222 & 86 \\ 880 & 532 & 960 & 280 & 59 & 200 \end{bmatrix}$$

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.

$$[\,6, 484, 616, 528, 154, 44, 110, 1714, 1506, 1675, 106, 292, 163, 546, 657, 588, 153, 60, 108, 590, 75,$$

$$630, 164, 35, 127, 1232, 1054, 1211, 67, 222, 86, 880, 532, 960, 280, 59, 200\,;\, 2, 6, 1, 7,$$

$$1, 5, 1, 4, 3].$$

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.

$$C = \begin{bmatrix} 484 & 616 & 528 & 154 & 44 & 110 \\ 1714 & 1506 & 1675 & 106 & 292 & 163 \\ 546 & 657 & 588 & 153 & 60 & 108 \\ 590 & 75 & 630 & 164 & 35 & 127 \\ 1232 & 1054 & 1211 & 67 & 222 & 86 \\ 880 & 532 & 960 & 280 & 59 & 200 \end{bmatrix}$$

The receiver is also generating the self-invertible matrix as the procedure explained in Section 2.1.

$$S = \begin{bmatrix} S_{11} & S_{12} \\ S_{21} & S_{22} \end{bmatrix} = \begin{bmatrix} 27 & 23 & 28 & 3 & 6 & 1 \\ 22 & 28 & 24 & 7 & 2 & 5 \\ 28 & 25 & 26 & 1 & 4 & 4 \\ 28 & 23 & 28 & 2 & 6 & 1 \\ 22 & 0 & 24 & 7 & 1 & 5 \\ 28 & 25 & 27 & 1 & 4 & 3 \end{bmatrix}$$

$$C \cdot G = \begin{bmatrix} 484 & 616 & 528 & 154 & 44 & 110 \\ 1714 & 1506 & 1675 & 106 & 292 & 163 \\ 546 & 657 & 588 & 153 & 60 & 108 \\ 590 & 75 & 630 & 164 & 35 & 127 \\ 1232 & 1054 & 1211 & 67 & 222 & 86 \\ 880 & 532 & 960 & 280 & 59 & 200 \end{bmatrix} \cdot \begin{bmatrix} 27 & 23 & 28 & 3 & 6 & 1 \\ 22 & 28 & 24 & 7 & 2 & 5 \\ 28 & 25 & 26 & 1 & 4 & 4 \\ 28 & 23 & 28 & 2 & 6 & 1 \\ 22 & 0 & 24 & 7 & 1 & 5 \\ 28 & 25 & 27 & 1 & 4 & 3 \end{bmatrix}$$

$$= \begin{bmatrix} 49764 & 47872 & 50402 & 7018 & 7656 & 6380 \\ 140266 & 129978 & 142063 & 19778 & 21576 & 17999 \\ 54288 & 51873 & 54984 & 7659 & 8352 & 6960 \\ 44138 & 38367 & 43561 & 3625 & 7737 & 4205 \\ 99528 & 91814 & 100804 & 14059 & 15312 & 12781 \\ 77082 & 70576 & 77024 & 8497 & 12723 & 8555 \end{bmatrix}$$

Taking addition modulo 29, we get, 49764(mod 29) = 0, 47872(mod 29) = 22, 50402(mod 29) = 0, …, 8555 (mod 29) = 0.

$$\therefore C \cdot S = \begin{bmatrix} 0 & 22 & 0 & 0 & 0 & 0 \\ 22 & 0 & 21 & 0 & 0 & 19 \\ 0 & 21 & 0 & 3 & 0 & 0 \\ 0 & 0 & 3 & 0 & 23 & 0 \\ 0 & 0 & 0 & 23 & 0 & 21 \\ 0 & 19 & 0 & 0 & 21 & 0 \end{bmatrix} = M$$

The Corresponding Pan graph P_5 for the above adjacency matrix was formed

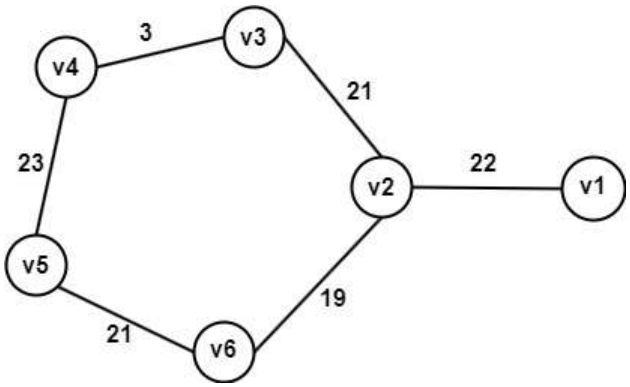

Figure 4.12. Pan graph P_5 of decrypted adjacency matrix.

The vertices(nodes) of the above graph were constructed by adding numerical equivalent value of vertex with corresponding edge weights,

Since we are adding an add-on 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 + 22 = 23, v3 = 23 + 21 = 44 = 15, v4 = 15 + 3 = 18, v5 = 18 + 23 = 41 = 12, v6 = 12 + 21 = 33 = 4.

$\therefore$ The vertices are $1, 23, 15, 18, 12, 4$.

$\therefore$The message is $1 \rightarrow A,\ 23 \rightarrow W,\ 15 \rightarrow O,\ 18 \rightarrow R,\ 12 \rightarrow L, 4 \rightarrow D.$ i.e., A WORLD.

5. Conclusion:

Information security needs to be safeguarded in the current world. To do this, a number of publications use symmetric encryption methods including the Caesar cipher, the Hill cipher, graphical approaches, and others. To strengthen the security of our data, this study offers a novel method for symmetric encryption. It uses a self-invertible matrix as the key matrix together with adjacency matrices of the pan graphs. The suggested approach may be advantageous for the pan graph for any value of n and it can bypass the intermediate and is more efficient. The recommended approach, which uses a straightforward encryption and decryption method with greater security, we are not sharing the whole key matrix, it makes the shared key exchange process less complicated, it makes the key more secure against hackers. Additionally, because the key matrix is a self-invertible matrix, it is not necessary to discover its inverse in order to decode the cipher. In this study, a simple pan graph is used for message encryption and decryption. This approach will be enhanced in the future and used to a wide range of other challenging graph theory ideas and new 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.
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. 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), Vol 43, Issue-01(2023), pp 359-371, https://www.hkclxb.cn/article/view/2023/359.html.
11. 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.
12. Neal Koblitz, A course in Number Theory and Cryptography, second edition, Springer.
13. 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.
14. 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
15. Weisstein, Eric W., Bull Graph, Math World.
16. Weal Mahmoud AI Etaiwi, Encryption algorithm using Graph theory, Journal of Scientific Research and Reports, 3(19), (2014), pp. 2519-2527.
17. 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.
18. 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.