

Synergistic Cryptography: Implementing K_6 Graphs and Hamiltonian Cycles for Reliable Encryption and Decryption

S.Renuga Devi

Department of Mathematics
Hindusthan College of Arts & Science,
Coimbatore, Tamilnadu, India

P.Rekha

Department of Mathematics
Hindusthan College of Arts & Science,
Coimbatore, Tamilnadu, India

L.Dhivya Prabha

Department of Mathematics
Hindusthan College of Arts & Science,
Coimbatore, Tamilnadu, India

Abstract— In today's digital era, encrypting messages is essential for ensuring secure communications. As internet and network technologies advance, encryption methods are becoming more sophisticated. Transmitting information, personal messages, images, or data over unsecured channels exposes them to potential attacks or hacking. To counter these threats and enhance security, cryptographic techniques are vital. Once ciphertext is produced and transmitted, it can be decrypted back to plaintext using the same key and a decryption algorithm. This paper describes an encryption method that employs a Complete K_6 Graph and a Cycle to generate ciphertext using two keys, one of which is derived from a Hamiltonian Circuit. It also provides the corresponding decryption algorithm.

Keywords— Complete Graph, Cycle, Hamiltonian Cycle, Encryption, Decryption, Cipher text.

I. INTRODUCTION

Cryptography is vital in any area requiring secure data transmission and storage, safeguarding the confidentiality, integrity, and authenticity of information across various applications. In computer science, cryptography underpins data security, identity authentication, and privacy across numerous applications. From securing web communications and online transactions to protecting cloud data and IoT devices, cryptographic techniques are essential for preserving the integrity, confidentiality, and authenticity of digital information in our increasingly interconnected world. [4] provides some ideas for discovering how to use labeled graphs. The inner magic and inner antimagic labelings introduced in [1] were utilized in [5] for secure data transfer in a cryptographic application of the inner magic and inner antimagic graphs. [3] describes the use of super mean and magic graph labelings in cryptography. [6] provides concepts on graph based cryptography, and certain specific graphs have been employed for cryptographic purposes in [7]. The relationship between randomness and cryptography is explained in [8], while [9] provides encryption and decryption techniques based on Graph Theory for symmetric keys. In [9], a Graph Theory-based encryption algorithm and bipartite graph approach for message encryption are discussed.

This study introduces an encryption mechanism founded on Graph Theory concepts to safeguard messages. The technique encodes the initial data (Plain Text) as a complete graph, employing an encryption table for labeling. To enhance the Cycle Matrix complexity, an Alphabet Encoding Table is used. The approach uses an upper triangular matrix as a shared key, while the Hamiltonian Circuit generates the second key, thereby increasing the ciphertext's complexity. Section 2 covers definitions and fundamental principles, and Section 3 of Main Results outlines encryption instructions, alphabet encoding, and graph labeling.

II. FUNDAMENTAL CONCEPTS

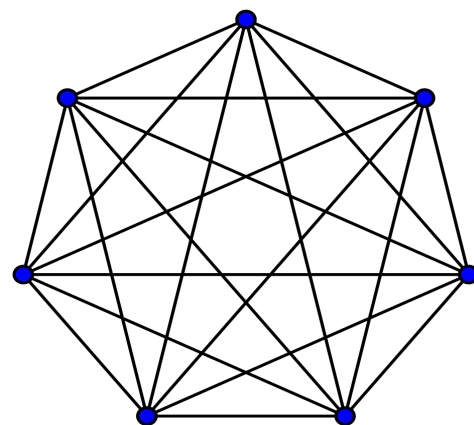
In this section, we outline the fundamental concepts of Graph Theory and Cryptography essential for the proposed encryption technique.

A. Graph

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

B. Complete Graph

In graph theory, a complete graph is a simple, undirected graph where every pair of distinct vertices is connected by a unique edge.



C. Directed/Undirected Graphs:

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

D. Path

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

E. Hamiltonian Path

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

F. Hamiltonian cycle

A Hamiltonian cycle (or Hamiltonian circuit) is a cycle that visits each vertex exactly once. A Hamiltonian path that starts and ends at adjacent vertices can be completed by adding one more edge to form a Hamiltonian cycle, and removing any edge from a Hamiltonian cycle produces a Hamiltonian path.

G. Nearest Neighbor Algorithm:

The Nearest Neighbor Algorithm traverses a graph starting at one vertex, and then it travels to the next vertex following the edge with the shortest distance (lightest weight) between them.

H. Cryptography and Cryptanalysis

Cryptography is the technique of converting readable data into unreadable data, ensuring message security. Cryptanalysis is the process of decoding a communication from a non-readable scheme to a readable scheme without understanding how it was originally encoded. Cryptology refers to a mix of cryptography and cryptanalysis.

I. Plain text

The plain text means Original readable data in its natural form.

J. Ciphertext

Ciphertext is encrypted text that is created by applying an encryption algorithm on plaintext.

K. Encryption and Decryption

Encryption is the process of transforming a standard message (plain text) into a meaningless message (ciphertext). Decryption is the process of transforming a meaningless message (ciphertext) back to its original form (plaintext).

III. MAIN RESULTS

i) Encryption Algorithm

STEP 1:

Encryption Table Construction

Encode the message using encoding chart.

A	B	C	D	E	F	G	H	I	J	K	L	M
65	66	67	68	69	70	71	72	73	74	75	76	77
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
78	79	80	81	82	83	84	85	86	87	88	89	90

Table 1: ASCII Encryption Table

STEP 2:

Apply the encoded information in the graph.

The graph's vertices reflect the original data (Plain Text). We use a complete graph K_n , where 'n' is the total number of characters in the original message. Let A be the original message with length n that is to be encrypted. Table 1 is used to translate each character of message A into the relevant numerical values, which are then assigned to the vertices of the full graph K_n . Label the edges by calculating the modulus of differences in labeling of the linked vertices.

STEP 3:

Create the newly generated Complete Graph Matrix 'P' using Labelled Complete Graph K_n . Create a new Cycle Matrix 'T' for the cycle derived from the full Graph K_n by deleting inner edges.

STEP 4:

Store the diagonal entries in Matrix 'B' by the respective number values of characters in original message M from the Alphabet Encoding table as given in Table 2 to obtain new modified matrix 'T*'.

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Table 2: Alphabet Encoding Table

STEP 4:

To create a new matrix 'M', multiply matrix P with matrix T^* .

STEP 5:

To obtain the first Cipher Matrix 'S', we multiply matrix M with the Key 'U'. Figure 1 depicts the top triangular key matrix U, which has an order of $n \times n$. where 'n' denotes the number of characters in the original message

$$U = \begin{pmatrix} 1 & 2 & \dots & \dots & n-1 & n \\ 0 & 1 & 2 & \dots & \dots & n-1 \\ 0 & 0 & 1 & 2 & \dots & \dots \\ 0 & 0 & 0 & 1 & 2 & \dots \\ 0 & 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

STEP 6:

Select a Hamiltonian Cycle from the complete graph. Because any Complete graph includes total $(n-1)!$ Hamiltonian Cycles: We will utilize the Nearest-Neighbor Algorithm to select the appropriate Hamiltonian Cycle.

STEP 7:

Nearest-Neighbor Algorithm

- As a starting point, select a vertex that contains the original message's beginning character.
- Go to the next vertex, which has an edge with the smallest labeling.
- If the labels on two or more edges are the same, select a random vertex; otherwise, proceed to the next.
- Repeat until the Hamiltonian Cycle is achieved.

STEP 8:

Add the edge labeling acquired while going along the Hamiltonian Cycle. Assume the total is "W". It serves as a secondary key.

STEP 9:

To create a new final Cipher Matrix 'R', apply mod W to each element of the previous Cipher Matrix 'S'.

Decryption Algorithm

- Use Matrix Form R to write the linear message.
- Use key W to extract matrix S from matrix R.
- To calculate Matrix 'M', use Cipher Matrix 'S' and the inverse of Key Matrix 'U' ($M = S \times U^{-1}$).
- Using P^{-1} and M, calculate T^* ($T^* = P^{-1} \times M$).
- Use the Alphabet Encoding Table to decode the diagonal entries from matrix T^* and calculate the original message.
- The original Plain Text is acquired.

Encryption:

Consider the case where the original message is "GENIUS". Because it contains six characters, we will create a K_6 Complete Graph and allocate these characters to the vertices of graphs, as illustrated in Figure 2. Use Table 1 to determine the number value for each character. We will get G = 71, E = 69, N = 78, I = 73, U = 85 and S = 83. Label the vertices with the corresponding numerical values. We set V_1 to 71, V_2 to 69, V_3 to 78, V_4 to 73, V_5 to 85 and V_6 to 83. Edge labels can be found as

$$\begin{aligned} E_1 &= |V_1 - V_2| = |71 - 69| = 2 \\ E_2 &= |V_2 - V_3| = |69 - 78| = 9 \\ E_3 &= |V_3 - V_4| = |78 - 73| = 5 \\ E_4 &= |V_4 - V_5| = |73 - 85| = 12 \\ E_5 &= |V_5 - V_6| = |85 - 83| = 2 \\ E_6 &= |V_6 - V_1| = |83 - 71| = 12 \\ E_7 &= |V_1 - V_3| = |71 - 78| = 7 \\ E_8 &= |V_1 - V_4| = |71 - 73| = 2 \\ E_9 &= |V_1 - V_5| = |71 - 85| = 14 \\ E_{10} &= |V_2 - V_6| = |69 - 83| = 14 \\ E_{11} &= |V_2 - V_5| = |69 - 85| = 16 \\ E_{12} &= |V_2 - V_4| = |69 - 73| = 4 \\ E_{13} &= |V_3 - V_6| = |78 - 83| = 5 \\ E_{14} &= |V_3 - V_5| = |78 - 85| = 7 \\ E_{15} &= |V_6 - V_4| = |83 - 73| = 10 \end{aligned}$$

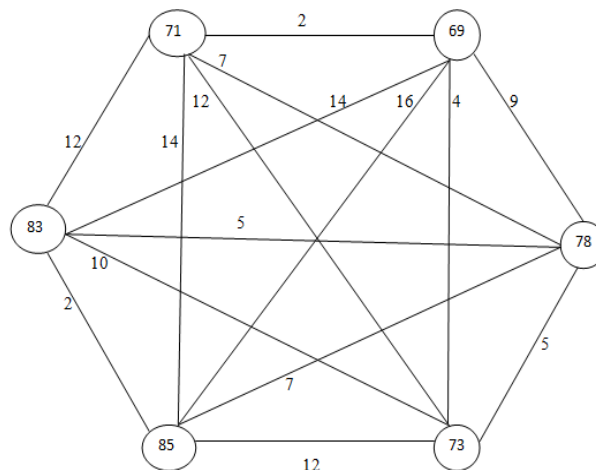


Figure 1 a): Complete Graph K_6

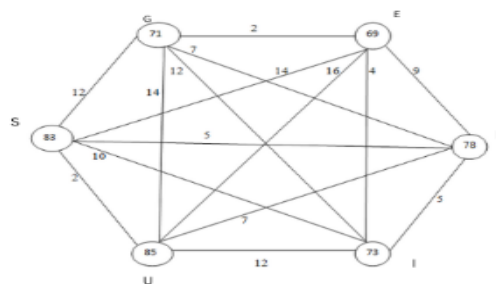


Figure 1 b): Complete Graph K_6

Obtain a freshly labeled Complete Graph Matrix from figure 1, indicated by 'P'.

$$P = \begin{matrix} & \begin{matrix} G & E & N & I & U & S \end{matrix} \\ \begin{matrix} G \\ E \\ N \\ I \\ U \\ S \end{matrix} & \begin{bmatrix} 0 & 2 & 7 & 2 & 14 & 12 \\ 2 & 0 & 9 & 4 & 16 & 14 \\ 7 & 9 & 0 & 5 & 7 & 5 \\ 2 & 4 & 5 & 0 & 12 & 10 \\ 14 & 16 & 7 & 12 & 0 & 2 \\ 12 & 14 & 5 & 10 & 2 & 0 \end{bmatrix} \end{matrix}$$

Using the aforementioned Complete Graph K_6 in figure 1 b), create a 6-length cycle.

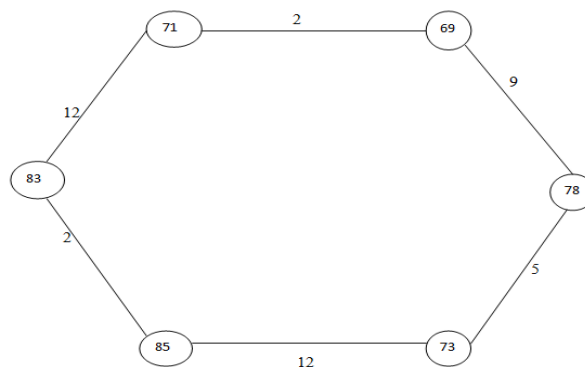


Figure 2: Cycle of length 6

The cycle yields a matrix 'T'. The Cycle Matrix is created in the same way as the Complete Graph Matrix, with the Cycle shown in figure 2.

$$T = \begin{matrix} & \begin{matrix} G & E & N & I & U & S \end{matrix} \\ \begin{matrix} G \\ E \\ N \\ I \\ U \\ S \end{matrix} & \begin{pmatrix} 0 & 2 & 0 & 0 & 0 & 12 \\ 2 & 0 & 9 & 0 & 0 & 0 \\ 0 & 9 & 0 & 5 & 0 & 0 \\ 0 & 0 & 5 & 0 & 12 & 0 \\ 0 & 0 & 0 & 12 & 0 & 2 \\ 12 & 0 & 0 & 0 & 2 & 0 \end{pmatrix} \end{matrix}$$

To replace the 0's in matrix 'T', use the Alphabet Encoding Table (Table 2) to assign new integer values to the characters in the original message. Table 2 yields the following English alphabet position numbers: G = 7; E = 5; N = 14; I = 9; U = 21; S = 19. By assigning these values to matrix 'T's' diagonal entries, we get a new matrix 'T*' (updated Cycle Matrix), as shown below.

$$T^* = \begin{matrix} & \begin{matrix} G & E & N & I & U & S \end{matrix} \\ \begin{matrix} G \\ E \\ N \\ I \\ U \\ S \end{matrix} & \begin{pmatrix} 7 & 2 & 0 & 0 & 0 & 12 \\ 2 & 5 & 9 & 0 & 0 & 0 \\ 0 & 9 & 14 & 5 & 0 & 0 \\ 0 & 0 & 5 & 9 & 12 & 0 \\ 0 & 0 & 0 & 12 & 21 & 2 \\ 12 & 0 & 0 & 0 & 2 & 19 \end{pmatrix} \end{matrix}$$

Obtain New Matrix "M" as follows

$$M = P \times T^*$$

$$M = \begin{pmatrix} 0 & 2 & 7 & 2 & 14 & 12 \\ 2 & 0 & 9 & 4 & 16 & 14 \\ 7 & 9 & 0 & 5 & 7 & 5 \\ 2 & 4 & 5 & 0 & 12 & 10 \\ 14 & 16 & 7 & 12 & 0 & 2 \\ 12 & 14 & 5 & 10 & 2 & 0 \end{pmatrix} \times \begin{pmatrix} 7 & 2 & 0 & 0 & 0 & 12 \\ 2 & 5 & 9 & 0 & 0 & 0 \\ 0 & 9 & 14 & 5 & 0 & 0 \\ 0 & 0 & 5 & 9 & 12 & 0 \\ 0 & 0 & 0 & 12 & 21 & 2 \\ 12 & 0 & 0 & 0 & 2 & 19 \end{pmatrix}$$

$$M = \begin{pmatrix} 148 & 73 & 126 & 221 & 342 & 256 \\ 182 & 85 & 146 & 273 & 412 & 322 \\ 127 & 59 & 106 & 129 & 217 & 193 \\ 142 & 69 & 106 & 169 & 272 & 238 \\ 154 & 171 & 302 & 143 & 148 & 206 \\ 112 & 139 & 246 & 139 & 162 & 148 \end{pmatrix}$$

Create Key Matrix 'U'. As the original message has 6 characters, the Key Matrix will be 6x6 as indicated below:

$$U = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 0 & 1 & 2 & 3 & 4 \\ 0 & 0 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Multiply the Key Matrix 'U' by the matrix 'M' to obtain the First Cipher Matrix 'S'.

$$S = M \times U$$

$$S = \begin{pmatrix} 148 & 73 & 126 & 221 & 342 & 256 \\ 182 & 85 & 146 & 273 & 412 & 322 \\ 127 & 59 & 106 & 129 & 217 & 193 \\ 142 & 69 & 106 & 169 & 272 & 238 \\ 154 & 171 & 302 & 143 & 148 & 206 \\ 112 & 139 & 246 & 139 & 162 & 148 \end{pmatrix} \times \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 0 & 1 & 2 & 3 & 4 \\ 0 & 0 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Using the Nearest-Neighbor Algorithm, we can determine the needed Hamiltonian Cycle as shown below: We'll start with the vertex that contains the first character of the original message, 'G'. Next, we will select a vertex with 'E' as an edge linking to it that has the least weight (the edge label is comparable to the weight of an edge here) than others. Continuing this process yields the needed Hamiltonian Cycle: G→E→I→N→U→S→G, with edge labels 2, 4, 5, 7, and 2,12, respectively. The Hamiltonian Cycle is represented in Figure 3.

Find second Key 'W'.

$$W = 2+4+5+7+2+12 = 32.$$

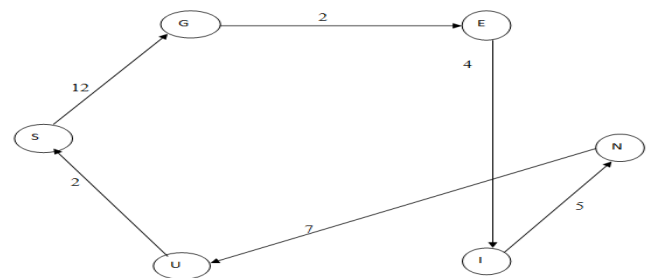


Figure 3: Hamiltonian Cycle

To generate a new Final Cipher Matrix, apply mod 32 to each element of the initial Cipher Matrix S. As a result, the final Cipher Matrix is 'R'.

Thus, the R matrix contains the remainders after each entry in S is divided by 32, which is as follows:

$$R = \begin{pmatrix} 20 & 17 & 12 & 4 & 18 & 0 \\ 22 & 1 & 30 & 12 & 22 & 2 \\ 31 & 25 & 29 & 2 & 0 & 31 \\ 14 & 1 & 30 & 4 & 26 & 30 \\ 26 & 31 & 18 & 20 & 10 & 14 \\ 16 & 11 & 28 & 24 & 22 & 8 \end{pmatrix}$$

The Quotient matrix Q records the outcomes of the division (quotients) after each element in S is divided by 32, which is as follows:

$$Q = \begin{pmatrix} 4 & 11 & 22 & 40 & 68 & 105 \\ 5 & 14 & 26 & 48 & 82 & 127 \end{pmatrix}$$

$$Q = \begin{pmatrix} 3 & 9 & 18 & 32 & 52 & 77 \\ 4 & 11 & 20 & 36 & 59 & 90 \\ 4 & 14 & 34 & 58 & 87 & 122 \\ 3 & 11 & 26 & 46 & 71 & 101 \end{pmatrix}$$

Hence the plain text "GENIUS" the Cipher text will be right to left

$$\begin{pmatrix} 8 & 22 & 24 & 28 & 11 & 16 & 14 & 10 & 20 & 18 & 31 & 26 \\ 30 & 26 & 4 & 30 & 1 & 14 & 31 & 0 & 2 & 29 & 25 & 31 \\ 2 & 22 & 12 & 30 & 1 & 22 & 0 & 18 & 4 & 12 & 17 & 20 \end{pmatrix}$$

ii) Decryption Algorithm

STEP 1:

The decryption inputs are as follows:: R (Final Cipher Text), Q (Quotient Matrix), W (second key) = 32 using Hamiltonian Cycle , U (Key Matrix), P (Complete Graph Matrix)

STEP 2:

Write the Cipher text 8 22 24 28 11 16 14 10 20 18 31 26 30 26 4 30 1 14 31 0 2 29 25 31 2 22 12 30 1 22 0 18 4 12 17 20 (Right to Left) in the Final Cipher Matrix R form as:

$$R = \begin{pmatrix} 20 & 17 & 12 & 4 & 18 & 0 \\ 22 & 1 & 30 & 12 & 22 & 2 \\ 31 & 25 & 29 & 2 & 0 & 31 \\ 14 & 1 & 30 & 4 & 26 & 30 \\ 26 & 31 & 18 & 20 & 10 & 14 \\ 16 & 11 & 28 & 24 & 22 & 8 \end{pmatrix}$$

STEP 3:

Obtain the First Cipher Matrix S with the use of second Key 'W' = 32 as follows $[Q]_{ij} \times 32 + [R]_{ij} = [S]_{ij}$ where $[Q]_{ij}$, $[R]_{ij}$ and $[S]_{ij}$ are entries of matrices Q, R and S respectively at the ith row and jth column.

$$[Q]_{ij} \times 32 = \begin{pmatrix} 128 & 352 & 704 & 1280 & 2176 & 3360 \\ 160 & 448 & 832 & 1536 & 2624 & 4064 \\ 96 & 288 & 576 & 1024 & 1664 & 2464 \\ 128 & 352 & 640 & 1152 & 1888 & 2880 \\ 128 & 448 & 1088 & 1856 & 2784 & 3904 \\ 96 & 352 & 832 & 1472 & 2272 & 3232 \end{pmatrix}$$

$$[Q]_{ij} \times 32 + [R]_{ij} = \begin{pmatrix} 148 & 369 & 716 & 1284 & 2194 & 3360 \\ 182 & 449 & 862 & 1548 & 2646 & 4066 \\ 127 & 313 & 605 & 1026 & 1664 & 2495 \\ 142 & 353 & 670 & 1156 & 1914 & 2910 \\ 154 & 479 & 1106 & 1876 & 2794 & 3918 \\ 112 & 363 & 860 & 1496 & 2294 & 3240 \end{pmatrix}$$

STEP 4: Compute inverse of matrix 'U'

$$U^{-1} = \begin{pmatrix} 1 & -2 & 1 & 0 & 0 & 0 \\ 0 & 1 & -2 & 1 & 0 & 0 \\ 0 & 0 & 1 & -2 & 1 & 0 \\ 0 & 0 & 0 & 1 & -2 & 1 \\ 0 & 0 & 0 & 0 & 1 & -2 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

STEP 5: Compute with Matrix M with $M = S \times U^{-1}$

$$M = S \times U^{-1} = \begin{pmatrix} 148 & 73 & 126 & 221 & 342 & 256 \\ 182 & 85 & 146 & 273 & 412 & 322 \\ 127 & 59 & 106 & 129 & 217 & 193 \\ 142 & 69 & 106 & 169 & 272 & 238 \\ 154 & 171 & 302 & 143 & 148 & 206 \\ 112 & 139 & 246 & 139 & 162 & 148 \end{pmatrix}$$

STEP 6: Compute inverse matrix of 'A'

$$P^{-1} = \begin{pmatrix} -1/2 & 1/4 & 0 & 1/4 & 0 & 0 \\ 1/4 & -7/32 & 0 & 0 & 1/32 & 0 \\ 0 & 0 & -1/5 & 1/10 & 0 & 1/10 \\ 1/4 & 0 & 1/10 & -7/20 & 0 & 0 \\ 0 & 1/32 & 0 & 0 & -7/32 & 1/4 \\ 0 & 0 & 1/10 & 0 & 1/4 & -7/20 \end{pmatrix}$$

STEP 7: Locate T* with help of $T^* = P^{-1} \times M$

$$T^* = P^{-1} \times M$$

$$= \begin{pmatrix} -1/2 & 1/4 & 0 & 1/4 & 0 & 0 \\ 1/4 & -7/32 & 0 & 0 & 1/32 & 0 \\ 0 & 0 & -1/5 & 1/10 & 0 & 1/10 \\ 1/4 & 0 & 1/10 & -7/20 & 0 & 0 \\ 0 & 1/32 & 0 & 0 & -7/32 & 1/4 \\ 0 & 0 & 1/10 & 0 & 1/4 & -7/20 \end{pmatrix} \times \begin{pmatrix} 148 & 73 & 126 & 221 & 342 & 256 \\ 182 & 85 & 146 & 273 & 412 & 322 \\ 127 & 59 & 106 & 129 & 217 & 193 \\ 142 & 69 & 106 & 169 & 272 & 238 \\ 154 & 171 & 302 & 143 & 148 & 206 \end{pmatrix}$$

$$T^* = \begin{pmatrix} 7 & 2 & 0 & 0 & 0 & 12 \\ 2 & 5 & 9 & 0 & 0 & 0 \\ 0 & 9 & 14 & 5 & 0 & 0 \\ 0 & 0 & 5 & 9 & 12 & 0 \\ 0 & 0 & 0 & 12 & 21 & 2 \\ 12 & 0 & 0 & 0 & 2 & 19 \end{pmatrix}$$

STEP 8:

Now we have the diagonal entries of the matrix T* as 7 5 14 9 21 19 which are when decoded with the help of Table 2 (Alphabet Encoding Table), we get 7 = G, 5 = E, 14 = N, 9 = I, 21 = U, 19 = S.

STEP 9:

As a result, the original text is: "GENIUS"

REFERENCES

- [1] Krishnaa A. and Dulawat M.S., Algorithms for Inner Magic and Inner Antimagic Labelings for Some Planar Graphs, Informatica (Lithuania), 17(3) (2006) 393-406.
- [2] Krishnaa A., Some Applications of Labelled Graphs, International Journal of Mathematics Trends and Technology, 37(3) (2016).
- [3] I.W. Sudarsana, S.A. Suryanto, D. Lucianti and N P A P S Putri, An application of super mean and mean graphs labeling in cryptography system, J. of Physics, Conference Series, 1763, The 2nd International Seminar on Science and Technology, Palu, Indonesia. Published under license by IOP Publishing Ltd (2020).
- [4] Krishnaa A., An Example Usage of Graph Theory in Other Scientific Fields: On Graph Labeling, Possibilities and Role of Mind/Consciousness, Chapter in the book titled Graph Theory : Advanced Algorithms and Applications, IntechOpen, London, UK (2018).
- [5] Krishnaa A., Inner magic and inner antimagic graphs in cryptography Journal of Discrete Mathematical Sciences and Cryptography, 22(6) (2019) 1057- 1066.
- [6] Ustimenko V.A., On graph based cryptography and symbolic computations, Serdica Journal of Computing I, (2007) 131-156.
- [7] Krishnaa A., Certain specific graphs in cryptography, Advances and Applications in Discrete Mathematics, 26(2) (2021) 157-177.
- [8] Perera P.A.S. and Wijesiri G.S., Encryption and decryption in symmetric key cryptography using graph theory, (2021).
- [9] Etaiwi W. M. A., Encryption Algorithm using Graph Theory. Journal of Scientific Research and Reports. 3(19) (2014) 2519-2527.