International Journal of Mathematics Trends and Technology
ISSN: 2231 – 5373/doi:10.14445/22315373/IJMTT-V67I12P507

Volume 67 Issue 12, 62-71, December, 2021

Complete Graph and Hamiltonian Cycle in Encryption and Decryption

Dharmendra Kumar Gurjar[1], Auparajita Krishnaa[2]

[1]*Research Scholar*, [2]*Supervisor*
[1]*Department of Mathematics and Statistics, University College of Science*
[2]*Mohan Lal Sukhadia University, Udaipur (Rajasthan) INDIA*

Abstract - *In recent times, Cryptography has becomes a significant area for research due to the vast transfer of information including the need for maintaining secrecy. Various encryption techniques are developed and used for securing the transferred data between two or more sources to hide the messages being sent. This paper involves an encryption technique for encrypting the message with the use of Complete Graph and a Cycle to generate a Cipher text using 2 keys, one of them is formed by the use of Hamiltonian Circuit. The decryption algorithm is also provided for the same.*

Keywords - *Complete Graph, Cycle, Hamiltonian Cycle, Encryption, Decryption, Cipher text, Complete Graph Matrix.*

I. INTRODUCTION

Discrete Mathematics has emerged as a very important and useful way to explore to find solutions in different disciplines such as Linear-programming, Coding theory, Theory of Computing, Computer Security, Electronic Banking, Number Theory, Cryptography etc. In recent times, interest has been aroused in using Graphs and concepts of Graph Theory in Cryptography. Cryptography is the discipline of achieving security by encoding message to make them un-readable for unwanted party. Modern cryptography is highly connected with Discrete Mathematics. Many cryptographic Algorithms such as RSA, ELGamal, Elliptic Curve methods, AES, CAST etc are directly based on discrete mathematical results. Ciphers can be converted into Graphs for secret communication. Some of the works on the basis of use of Graph Theory concepts in Cryptography are as follows:

Some ideas for discovering use of labeled graphs are given in [1]. The *inner magic* and *inner antimagic* labelings discovered and presented in [2], have been used in [3] for safe data transfer in a cryptographic application of the *inner magic* and *inner antimagic* graphs. [4] gives application of *super mean* and *magic* graph labelings in cryptography. [5] gives concepts on graph based cryptography whereas some particular graphs have been used for cryptographic applications in [6]. Relationship between randomness and cryptography is given in [8] and [9] gives the encryption and decryption algorithms using the concepts of Graph Theory for the symmetric key of cryptography. [9] discusses about an encryption algorithm using Graph Theory and a method for message encryption using bipartite graph has been introduced in [10]. [11] has give certain applications of labeled graphs including cryptography.

In this paper, an encryption technique is proposed for securing the message, which is based on Graph Theory concepts. In this technique, the initial data (Plain Text) is stored in a complete Graph. For the labeling, an encryption table is used. An Alphabet Encoding Table has been used for more complexity in Cycle Matrix. An upper triangular matrix is used as a shared key $\boldsymbol{K}$ and Hamiltonian Circuit is used to generate second key $\boldsymbol{S}$. Use of two keys enhance the complexity of the Cipher text. Section 2 gives the definitions and fundamental concepts whereas instructions for encryption table, Alphabet Encoding Table and Labelling of Graph are given in the Section 3 of Main Results.

A. DEFINITIONS AND FUNDAMENTAL CONCEPTS

In this section we provide the basic concepts of Graph Theory and Cryptography which are required for the proposed encryption technique.

a) Graph

A graph G is a mathematical structure consisting of vertices and edges. Each edge joins two vertices. The sets of vertices and edges are represented as V(G) and E(G) respectively.

b) Complete Graph

It is a simple graph in which each pair of distinct vertices is connected by an edge. A complete graph is denoted by K_n, where n is the number of vertices. Here a complete graph K_5 is used for encryption.

c) Complete Graph Matrix

Let G be a complete graph with n vertices labeled as 1, 2, 3, …, n. The complete Graph Matrix is the n×n matrix in which the entry in i^{th} row and j^{th} column is the edge weight on the edge joining two vertices i and j. Defined as:

$$[a_{i,j}] = \begin{cases} weight\ on\ edge\ label\ joining\ the\ vertex\ i\ to\ vertex\ j; & i \neq j \\ 0; & i = j \end{cases}$$

d) Hamiltonian Cycle

A cycle of a graph G containing every vertex of G is called a Hamiltonian cycle. A graph containing a Hamiltonian cycle is a Hamiltonian Graph.

e) Cryptography and Cryptanalysis

Cryptography is basically a process to convert a readable data to unreadable data so that one can not easily read that, which makes the message/data secure. The technique of decoding message from a non-readable scheme to a readable scheme without knowing how they before converted from readable scheme to non-readable scheme, is known as **Cryptanalysis**. The combination of *cryptography* and *cryptanalysis* is called **Cryptology**.

f) Plain Text and Cipher Text

The *clear text* or ***plain text*** means a message that can be understood by the sender, the recipient, and also by anyone else who gets access to that message. '***Cipher***' means a code or a secret message. Hence, we can say that when a plain text message is codified using any suitable schemes, the resulting message is called *cipher text*.

g) Encryption and Decryption

The process of encoding a plain text message into cipher text message is called ***encryption***. The process of transforming cipher text message into plain text message back is called ***decryption***. Decryption is exactly reverse process of Encryption.

h) Algorithm and Key

Every encryption and decryption process has two aspects: the **algorithm** and the **key** used for encryption and decryption. In general, the algorithm used for encryption and decryption processes is usually known to everybody. However, the key used for encryption and decryption is main aspect of security system that makes the process of cryptography secure.

II. MAIN RESULTS

Encryption Algorithm:

STEP 1. (Encryption Table Construction):

We Assign the numbers 0,1,2,…,m to the columns and the numbers m+1, m+2, m+3, …, n to the rows. Assign the characters in S randomly in the table. Where S is the set of characters from which the characters are used in the original message. Here we use set S containing elements {26 alphabets, blank space, dot (.)}. A model Table is given in **Table 1**.

Table 1: Encryption Table

	0	**1**	**2**	**3**	**4**	**5**	**6**
7	A	B	C	D	E	F	G
8	H	I	J	K	L	M	N
9	O	P	Q	R	S	T	U
10	V	W	X	Y	Z	SPACE	DOT

Here in this table each character receives a number value. For assigning the number value we have two groups: First group containing all the vowels, SPACE and DOT. The second group includes all the consonant characters in it. For Group 2, the first character represents the column number, remaining the row number. For Group 1, the last character represents the column number and the remaining initial number represents the row number.

For example, A = 70, F = 57, R = 39, X = 210, O = 90, U = 96, SPACE = 105, DOT = 106.

STEP 2. (Construction of Graph and Labelling of Graph)**:**

In the second step the initial data (Plain Text) is represented as vertices in the graph. We take a complete Graph $\mathbf{K_n}$ where 'n' is the total number of characters in the original message. Let M be the original message having length n, which is to be encrypted. After converting each character of message M into the corresponding number values with the help of Table 1, assign these values to the vertices of complete Graph $\mathbf{K_n}$. Label the edges with taking the modulus of differences of labeling of respective connecting vertices.

STEP 3. Construct the Newly developed Complete Graph Matrix '**A**' with the help of Labelled Complete Graph $\mathbf{K_n}$. Also construct a new Cycle Matrix '**B**' for the Cycle obtained from the complete Graph $\mathbf{K_n}$ by removing inside 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 '**B***'.

Table 2: Alphabet Encoding Table

A	B	C	D	…	…	…	X	Y	Z
1	2	3	4	…	…	…	24	25	26

STEP 5. Multiply matrix A with matrix B* to obtain a new matrix 'N'.

STEP 6. After that we multiply matrix N with a Key '$\boldsymbol{K}$' to get First Cipher Matrix '$\mathbf{C_1}$'. The key matrix $\boldsymbol{K}$ is an ***upper triangular matrix*** of order $\boldsymbol{n \times n}$ as shown below in **figure 1**. Where 'n' is the number of characters in the original message.

$$\boldsymbol{K} = \begin{bmatrix} 1 & 2 & \dots & \dots & n-1 & n \\ 0 & 1 & 2 & \dots & \dots & n-1 \\ 0 & 0 & 1 & 2 & \dots & \dots \\ 0 & 0 & 0 & 1 & 2 & \dots \\ 0 & 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Figure 1: Key Matrix

STEP 7. Choose a Hamiltonian Cycle from the complete graph. Since any Complete graph contains total **(n-1)!** Hamiltonian Cycles, for choosing the required Hamiltonian Cycle, we will use **Nearest-Neighbor Algorithm**.

(Nearest-Neighbor Algorithm)

- Choose a vertex having initial character of the original message as starting point.
- Go to the next vertex, which is having an edge with smallest labelling on it.
- If labeling on two or more edges are same, choose random vertex, otherwise go to next.
- Repeat, till the Hamiltonian Cycle is obtained.

STEP 8. Add the edge labeling obtained while moving on Hamiltonian Cycle. Let sum be "**S**". It is used as second key.

STEP 9. Apply ***mod S*** on every element of first Cipher Matrix **'C_1'** to obtain a new final Cipher Matrix **'C_2'.**

The Cipher Text contains Matrix **C_2** in a linear format.

Decryption Algorithm:

- Write the linear message in Matrix Form **C_2**.
- Obtain matrix **C_1** from matrix **C_2** with the use of key **S**.
- Compute Matrix 'N' with the help of Cipher Matrix 'C_1' and inverse of Key Matrix 'K' (i.e. $N = C_1 \times K^{-1}$).
- Compute B* with the help of A^{-1} and N (i.e. $B^* = A^{-1} \times N$).
- Write the diagonal entries from the matrix B* to compute the original message by decoding these values with the help of Alphabet Encoding Table.
- Original Plain Text is obtained.

Illustration:

Encryption:

Suppose the Original Message is "**GRAPH**". Since it has 5 characters in it so, we will form a K_5 Complete Graph and assign these characters to the vertices of Graphs as shown in **figure 2**.

Now find out the number value for each character with the help of Table 1. We will get G = 67, R = 39, A = 70, P = 19, H = 08.

Label the vertices with these corresponding number values. We assign V1 = 67, V2 = 39, V3 = 70, V4 = 19, V5 = 08.

Edge labels are found as:

e1 = |v1-v2| = |67-39| = 28.

e2 = |v2-v3| = |39-70| = 31.

e3 = |v3-v4| = |70-19| = 51.

e4 = |v4-v5| = |19-08| = 11.

e5 = |v5-v1| = |08-67| = 59.

e6 = |v1-v3| = |67-70| = 03.

e7 = |v1-v4| = |67-19| = 48.

e8 = |v2-v4| = |39-19| = 20.

e9 = |v2-v5| = |39-08| = 31.

e10 = |v3-v5| = |70-08| = 62.

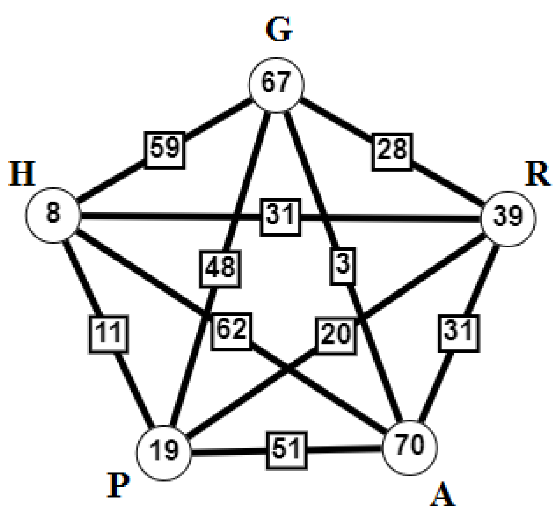

Figure 2: **Complete Graph K_5**

Obtain a newly labeled Complete Graph Matrix from figure 2 and denoted by ‘A’.

$$A = \begin{array}{c} \\ G \\ R \\ A \\ P \\ H \end{array} \begin{array}{c} \begin{array}{ccccc} G & R & A & P & H \end{array} \\ \begin{bmatrix} 0 & 28 & 3 & 48 & 59 \\ 28 & 0 & 31 & 20 & 31 \\ 3 & 31 & 0 & 51 & 62 \\ 48 & 20 & 51 & 0 & 11 \\ 59 & 31 & 62 & 11 & 0 \end{bmatrix} \end{array}$$

Figure 3: **Complete Graph Matrix**

Obtain a Cycle of length 5 with the help of above Complete Graph K_5 in **figure 2**.

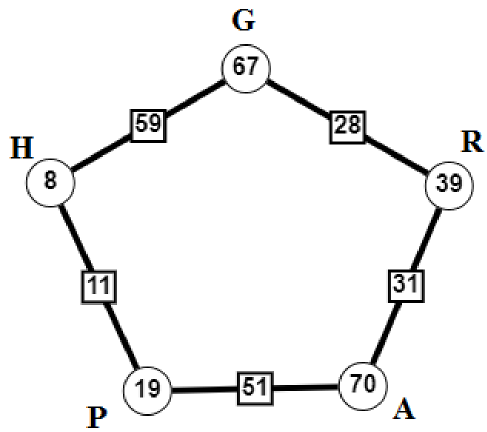

Figure 4: **Cycle of length 5.**

Obtain a matrix 'B' from the cycle. The Cycle Matrix is prepared in a similar manner to the Complete Graph Matrix with the Cycle in figure 4.

$$B = \begin{array}{cc} & \begin{matrix} \mathbf{G} & \mathbf{R} & \mathbf{A} & \mathbf{P} & \mathbf{H} \end{matrix} \\ \begin{matrix} \mathbf{G} \\ \mathbf{R} \\ \mathbf{A} \\ \mathbf{P} \\ \mathbf{H} \end{matrix} & \begin{bmatrix} 0 & 28 & 0 & 0 & 59 \\ 28 & 0 & 31 & 0 & 0 \\ 0 & 31 & 0 & 51 & 0 \\ 0 & 0 & 51 & 0 & 11 \\ 59 & 0 & 0 & 11 & 0 \end{bmatrix} \end{array}$$

Figure 5: **Cycle Matrix**

Replace the diagonal entries in matrix 'B' from 0's to new assigned number values to characters of original message from the Alphabet Encoding Table (Table 2) i.e., we get the position numbers of the letters in the English alphabet from Table 2 as follows : G = 7, R = 18, A = 1, P = 16, H = 8. After assigning these values to diagonal entries of matrix 'B', we obtain a new matrix '**B***' (updated Cycle Matrix) as shown below:

$$B^* = \begin{bmatrix} \mathbf{7} & 28 & 0 & 0 & 59 \\ 28 & \mathbf{18} & 31 & 0 & 0 \\ 0 & 31 & \mathbf{1} & 51 & 0 \\ 0 & 0 & 51 & \mathbf{16} & 11 \\ 59 & 0 & 0 & 11 & \mathbf{8} \end{bmatrix}$$

Obtain new matrix 'N' as follows:

$$\mathrm{N} = \mathrm{A} \times \mathrm{B}^* = \begin{bmatrix} 0 & 28 & 3 & 48 & 59 \\ 28 & 0 & 31 & 20 & 31 \\ 3 & 31 & 0 & 51 & 62 \\ 48 & 20 & 51 & 0 & 11 \\ 59 & 31 & 62 & 11 & 0 \end{bmatrix} \times \begin{bmatrix} 7 & 28 & 0 & 0 & 59 \\ 28 & 18 & 31 & 0 & 0 \\ 0 & 31 & 1 & 51 & 0 \\ 0 & 0 & 51 & 16 & 11 \\ 59 & 0 & 0 & 11 & 8 \end{bmatrix}$$

$$N = \begin{bmatrix} 4265 & 597 & 3319 & 1570 & 1000 \\ 2025 & 1745 & 1051 & 2242 & 2120 \\ 4547 & 642 & 3562 & 1498 & 1234 \\ 1545 & 3285 & 671 & 2722 & 2920 \\ 1281 & 4132 & 1584 & 3338 & 3602 \end{bmatrix}$$

Construct **Key Matrix** 'K'. As the original message has 5 characters in it, the size of Key Matrix will be 5×5 as shown below:

$$\mathbf{K} = \begin{bmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} & \mathbf{5} \\ \mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{3} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{2} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} \end{bmatrix}$$

Obtain the First Cipher Matrix '$\mathbf{C_1}$' by multiplying Key Matrix 'K' with matrix 'N'.

$$\boldsymbol{C_1} = N \times K = \begin{bmatrix} 4265 & 597 & 3319 & 1570 & 1000 \\ 2025 & 1745 & 1051 & 2242 & 2120 \\ 4547 & 642 & 3562 & 1498 & 1234 \\ 1545 & 3285 & 671 & 2722 & 2920 \\ 1281 & 4132 & 1584 & 3338 & 3602 \end{bmatrix} \times \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\boldsymbol{C_1} = \begin{bmatrix} \mathbf{4265} & \mathbf{9127} & \mathbf{17308} & \mathbf{27059} & \mathbf{37810} \\ \mathbf{2025} & \mathbf{5795} & \mathbf{10616} & \mathbf{17679} & \mathbf{26862} \\ \mathbf{4547} & \mathbf{9736} & \mathbf{18487} & \mathbf{28736} & \mathbf{40219} \\ \mathbf{1545} & \mathbf{6375} & \mathbf{11876} & \mathbf{20099} & \mathbf{31242} \\ \mathbf{1281} & \mathbf{6694} & \mathbf{13691} & \mathbf{24026} & \mathbf{37963} \end{bmatrix}$$

By Use of **Nearest-Neighbor Algorithm** we find the required **Hamiltonian Cycle** as given under:

We will start from vertex that is containing the initial character of original message that is 'G'. For next, we will choose vertex having 'A' as edge connecting to it has minimum weight (the *edge labe*l is equivalent to the *weight* of an edge here) on it than others. Continue this process and we get required Hamiltonian Cycle as **G→A→R→P→H→G** and edge labels on these are 3, 31, 20, 11, 59 respectively. The Hamiltonian Cycle is shown in **figure 6**.

Find second Key '**S**'. **S = 3+31+20+11+59 = 124**.

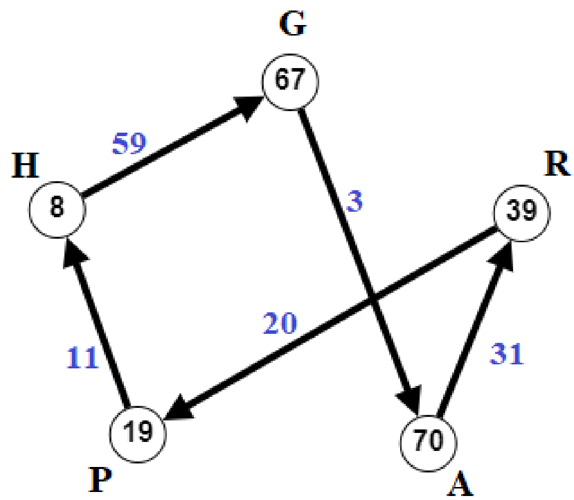

Figure 6: **Hamiltonian Cycle**

Apply ***mod 124*** on every element of the first Cipher Matrix $\mathbf{C_1}$ to get new Final Cipher Matrix. Hence the Final Cipher Matrix '$\mathbf{C_2}$' is:

$C_2 = C_1$ *multiplication* mod 124

$$C_2 = \begin{bmatrix} 4265 & 9127 & 17308 & 27059 & 37810 \\ 2025 & 5795 & 10616 & 17679 & 26862 \\ 4547 & 9736 & 18487 & 28736 & 40219 \\ 1545 & 6375 & 11876 & 20099 & 31242 \\ 1281 & 6694 & 13691 & 24026 & 37963 \end{bmatrix} multiplication\ \ mod\ 124$$

Thus, C_2 matrix stores the remainders after each entry of C_1 is divided by 124 which is as follows **:**

$$\boldsymbol{C_2} = \begin{bmatrix} \mathbf{49} & \mathbf{75} & \mathbf{72} & \mathbf{27} & \mathbf{114} \\ \mathbf{41} & \mathbf{91} & \mathbf{76} & \mathbf{71} & \mathbf{78} \\ \mathbf{83} & \mathbf{64} & \mathbf{11} & \mathbf{92} & \mathbf{43} \\ \mathbf{57} & \mathbf{51} & \mathbf{96} & \mathbf{11} & \mathbf{118} \\ \mathbf{41} & \mathbf{122} & \mathbf{51} & \mathbf{94} & \mathbf{19} \end{bmatrix}$$

The Quotient matrix Q stores the results of the division (quotients) after each entry of C_1 is divided by 124 which is as follows :

$$\boldsymbol{Q} = \begin{bmatrix} \mathbf{34} & \mathbf{73} & \mathbf{139} & \mathbf{218} & \mathbf{304} \\ \mathbf{16} & \mathbf{46} & \mathbf{85} & \mathbf{142} & \mathbf{216} \\ \mathbf{36} & \mathbf{78} & \mathbf{149} & \mathbf{231} & \mathbf{324} \\ \mathbf{12} & \mathbf{51} & \mathbf{95} & \mathbf{162} & \mathbf{251} \\ \mathbf{10} & \mathbf{53} & \mathbf{110} & \mathbf{193} & \mathbf{306} \end{bmatrix}$$

Hence, For the Plain text "**GRAPH**", the **Cipher text** will be (the entries of C_2 from left to right):

49 75 72 27 114 41 91 76 71 78 83 64 11 92 43 57 51 96 11 118 41 122 51 94 19

Decryption Algorithm:

1. The input for decryption are as follows **: $\mathbf{C_2}$ (Final Cipher Text), Q (Quotient Matrix), S (second key) = 124 using Hamiltonian Cycle , K (Key Matrix), A (Complete Graph Matrix)**
2. Write the Cipher text **49 75 72 27 114 41 91 76 71 78 83 64 11 92 43 57 51 96 11 118 41 122 51 94 19** in the Final Cipher Matrix $\boldsymbol{C_2}$ form as:

$$C_2 = \begin{bmatrix} 49 & 75 & 72 & 27 & 114 \\ 41 & 91 & 76 & 71 & 78 \\ 83 & 64 & 11 & 92 & 43 \\ 57 & 51 & 96 & 11 & 118 \\ 41 & 122 & 51 & 94 & 19 \end{bmatrix}$$

3. Obtain the First Cipher Matrix C_1 with the use of second Key 'S' = 124 as follows :

   $[Q]_{ij} \times 124 + [C_2]_{ij} = [C_1]_{ij}$ where $[Q]_{ij}$, $[C_2]_{ij}$ and $[C_1]_{ij}$ are entries of matrices Q, C_2 and C_1 respectively at the i^{th} row and j^{th} column.
   For instance, 4265 = 34 x 124 + 49

$$C_1 = \begin{bmatrix} 4265 & 9127 & 17308 & 27059 & 37810 \\ 2025 & 5795 & 10616 & 17679 & 26862 \\ 4547 & 9736 & 18487 & 28736 & 40219 \\ 1545 & 6375 & 11876 & 20099 & 31242 \\ 1281 & 6694 & 13691 & 24026 & 37963 \end{bmatrix}$$

4. Compute inverse of matrix ‘K’; $K^{-1} = \begin{bmatrix} 1 & -2 & 1 & 0 & 0 \\ 0 & 1 & -2 & 1 & 0 \\ 0 & 0 & 1 & -2 & 1 \\ 0 & 0 & 0 & 1 & -2 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$

5. Compute matrix ‘N’ with $\boxed{N = C_1 \times K^{-1}}$

$$N = \begin{bmatrix} 4265 & 9127 & 17308 & 27059 & 37810 \\ 2025 & 5795 & 10616 & 17679 & 26862 \\ 4547 & 9736 & 18487 & 28736 & 40219 \\ 1545 & 6375 & 11876 & 20099 & 31242 \\ 1281 & 6694 & 13691 & 24026 & 37963 \end{bmatrix} \times \begin{bmatrix} 1 & -2 & 1 & 0 & 0 \\ 0 & 1 & -2 & 1 & 0 \\ 0 & 0 & 1 & -2 & 1 \\ 0 & 0 & 0 & 1 & -2 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$N = \begin{bmatrix} 4265 & 597 & 3319 & 1570 & 1000 \\ 2025 & 1745 & 1051 & 2242 & 2120 \\ 4547 & 642 & 3562 & 1498 & 1234 \\ 1545 & 3285 & 671 & 2722 & 2920 \\ 1281 & 4132 & 1584 & 3338 & 3602 \end{bmatrix}$$

6. Compute inverse matrix of ‘A’;

$$A^{-1} = \begin{bmatrix} \frac{-31}{168} & \frac{1}{56} & \frac{1}{6} & 0 & 0 \\ \frac{1}{56} & \frac{-3}{70} & 0 & \frac{1}{40} & 0 \\ \frac{1}{6} & 0 & \frac{-59}{372} & 0 & \frac{1}{124} \\ 0 & \frac{1}{40} & 0 & \frac{-31}{440} & \frac{1}{22} \\ 0 & 0 & \frac{1}{124} & \frac{1}{22} & \frac{-51}{1364} \end{bmatrix}$$

7. Now find B* with help of $\boxed{B^* = A^{-1} * N}$

$$B^* = \begin{bmatrix} \frac{-31}{168} & \frac{1}{56} & \frac{1}{6} & 0 & 0 \\ \frac{1}{56} & \frac{-3}{70} & 0 & \frac{1}{40} & 0 \\ \frac{1}{6} & 0 & \frac{-59}{372} & 0 & \frac{1}{124} \\ 0 & \frac{1}{40} & 0 & \frac{-31}{440} & \frac{1}{22} \\ 0 & 0 & \frac{1}{124} & \frac{1}{22} & \frac{-51}{1364} \end{bmatrix} \times \begin{bmatrix} 4265 & 597 & 3319 & 1570 & 1000 \\ 2025 & 1745 & 1051 & 2242 & 2120 \\ 4547 & 642 & 3562 & 1498 & 1234 \\ 1545 & 3285 & 671 & 2722 & 2920 \\ 1281 & 4132 & 1584 & 3338 & 3602 \end{bmatrix}$$

$$B^* = \begin{bmatrix} \mathbf{7} & 28 & 0 & 0 & 59 \\ 28 & \mathbf{18} & 31 & 0 & 0 \\ 0 & 31 & \mathbf{1} & 51 & 0 \\ 0 & 0 & 51 & \mathbf{16} & 11 \\ 59 & 0 & 0 & 11 & \mathbf{8} \end{bmatrix}$$

8. Now we got diagonal entries of matrix B* as 7 18 1 16 8 which are when decoded with the help of Table 2(Alphabet Encoding Table), we get 7 = G, 18 = R, 1 = A, 16 = P, 8 = H.
9. Hence the original text is: **GRAPH**.

III. CONCLUSIONS

In this work we have studied an encryption technique for hiding the Plain Text message. For this, we used a Complete Graph and Cycle of the length of size of the message and also made use of the Hamiltonian Cycle. We develop a Complete Graph Matrix and Cycle Matrix based on the edge labeling done using the Encryption Table (Table 1). We modified the Cycle Matrix with the use of Alphabet Encoding Table (Table 2) and applied matrix operations on these two (Complete Graph Matrix A and updated Cycle Matrix B*) matrices with the use of a shared key K (Upper Triangular Matrix), used the Hamiltonian Cycle to get a second key S which helped us to get a new Final Cipher Matrix C_2 to yield the Final Cipher text which is not easily predictable. The decryption process involves calculating the following matrices in the order : C_2 (Final Cipher Matrix), C_1 (First Cipher Matrix) using S (second key), K^{-1} (inverse of Key Matrix), N ($N = C_1 \times K^{-1}$), A, B* ($B = A^{-1} \times N$) and the diagonal entries of B* with the Alphabet Encoding Table (Table 2), which gives the original plain text.

Therefore, a multilayered hiding of the original plain text is obtained using the concepts from Graph Theory which gives a much hidden cipher text serving the purpose of a highly safe data transfer.

ACKNOWLEDGEMENT

INSPIRE Fellowship provided to the first author to carry out his Ph.D. work under the supervision of the Corresponding and second author by the Department of Science and Technology (DST), Ministry of Science and Technology, Government of India.

REFERENCES

[1] Krishnaa A., An Example Usage of Graph Theory in Other Scientific Fields: On Graph Labeling, Possibilities and Role of Mind/C onsciousness, Chapter in the book titled Graph Theory : Advanced Algorithms and Applications, IntechOpen, London, UK (2018).
[2] 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.
[3] Krishnaa A., Inner magic and inner antimagic graphs in cryptography Journal of Discrete Mathematical Sciences and Cryptography, 22(6) (2019) 1057-1066.
[4] 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 Sciencce and Technology, Palu, Indonesia. Published under license by IOP Publishing Ltd (2020).
[5] Ustimenko V.A., On graph based cryptography and symbolic computations, Serdica Journal of Computing I, (2007) 131-156.
[6] Krishnaa A., Certain specific graphs in cryptography, Advances and Applications in Discrete Mathematics, 26(2) (2021) 157-177.
[7] Shamir Adi, Random graphs in cryptography, The Weizman Institute, Israel, The Onassis Foundation Science Lecture Series, 28 (2010).
[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.
[10] Yamuna M. and Karthika K**.,** Data transfer using bipartite Graphs. International Journal of Advance Research in Science and Engineering (IJARSE), 4(2) (2015).
[11] Krishnaa A., Some Applications of Labelled Graphs, International Journal of Mathematics Trends and Technology, 37(3) (2016).