LouisSaveinDupuisJournalofMultidisciplinaryResearch2024,3: 170-177 Doi.: 10.21839/lsdjmr.2024.v3.126

Research Article

GRAPH THEORETIC APPROACHES IN CRYPTOGRAPHY: EXPLORING CONNECTIONS AND APPLICATIONS

Ms. P. Geetha,
Assistant Professor for mathematic
Immaculate College for Women, Cuddalore

R. Nivethini,
II M.sc, mathematic,
Immaculate College for Women, Cuddalore

Abstract

Cryptography is one among the most important techniques used for securing the transmission of **messages and the protection of data and Graph Theory is one of the techniques used to protect the data.** Cryptography is especially used to make the text unintelligible and non-readable through the encrypt and decrypt process. In this paper, we use graph theory to encrypt and decrypt the message

Keywords: *Complete graph, Spanning tree, Encryption, Decryption, Public key, Sharing key*

Introduction

Complete Graph

A simple graph in which each pair of distinct vertices is adjacent is called a complete graph. It is an undirected graph. A complete graph is denoted as k_n, where n is the number of vertices.

Spanning Tree

A spanning tree T a graph G is a subgraph containing all the vertices of G. It is a minimal set of edges that connects all the vertices of G without creating any cycles or loops. The minimum spanning tree is one with the least weight.

Weighted Graph

A weighted graph is a graph in which each branch is given a numerical weight. A weighted graph is a special type of labeled graph in which the labels are numbers.

Cryptography

Cryptography is a method of protecting information and communications through the use of codes so that only those for whom the information is intended can read and process it. It is associated with the process of converting plain text into cipher text. The prefix "crypt" means "hidden" or "vault" and the suffix "graphy" stands for "writing".

Problem

We proceed to encrypt the text or data, such as "C O M P L E T E", before transmitting it securely to the receiver on the other end. This ensures that the information remains confidential during transmission.

Each letter is represented as a vertex in the graph, and the connection between vertices forms edges in the graph.

Figure: Letter into vertex (node)

Here's the cycle graph formed by linking each two characters in alternating lines.

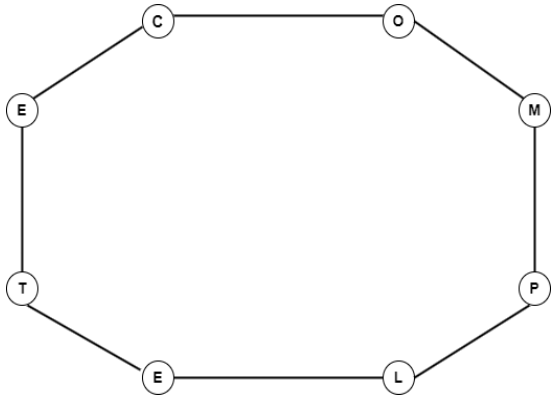

Figure: Cycle graph

Moreover, we use the encoding table to mark each edge.

Encoding table													
A	B	c	D	.	.	.	.	W	X	y	Z		
1	2	3	4	.	.	.	.	23	24	25	26		

Figure: Encoding Table

Distance of CO = Code (O) – Code (C)

= 15-3 = 12.

We may infer the lengths of the other edges in a similar manner. Next, we name the graph that includes every letter in plain text, and the result is a weighted graph.

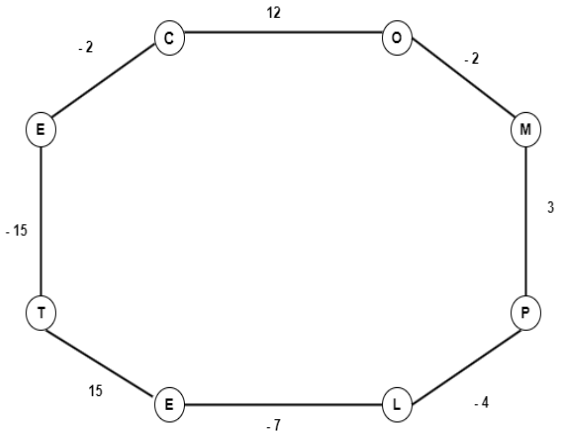

Figure weighted graph

Then, in order to create a full graph, we continue to add edges. Each new edge has a sequential weight that begins at the maximum weight of 26, which is found in the encoding table. Thus, we can add 27, 28, and furthermore.

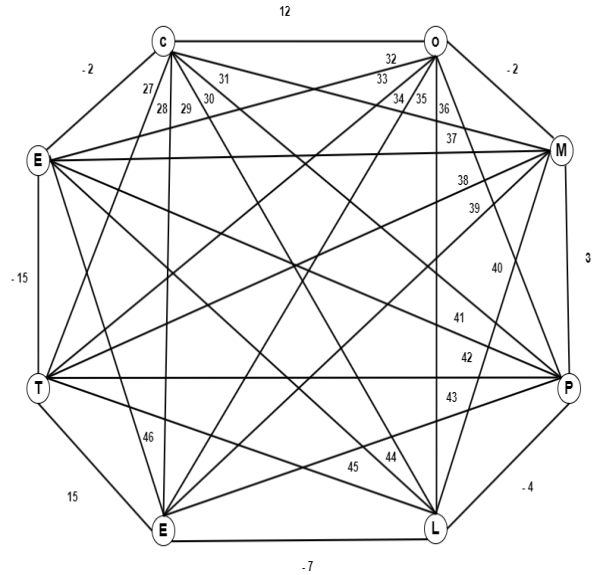

Figure Complete graph

Therefore, we can take,

Distance of CM = 31; CP = 30; CL = 29; CE = 28; CT = 27;

Distance of OP = 36; OL = 35; OE = 34; OT = 33; OE = 32;

Distance of MC = 31; ML = 40; ME = 39; MT = 38; ME = 37;

Distance of PC = 30; PO = 36; PE = 43; PT = 42; PE = 41;

Distance of LC = 29; LO = 35; LM = 40; LT = 45; LE = 44;

Distance of EC = 28; EO = 34; EM = 39; EP = 43; EE = 46;

Distance of TC = 27; TO = 33; TM = 38; TP = 42; TL = 45;

Distance of EO = 32; EM = 37; EP = 41; EL = 44; EE = 46;

$$A = \begin{array}{c} \\ C \\ O \\ M \\ P \\ L \\ E \\ T \\ E \end{array} \begin{array}{c} \begin{array}{cccccccc} C & O & M & P & L & E & T & E \end{array} \\ \begin{bmatrix} 0 & 12 & 31 & 30 & 29 & 28 & 27 & -2 \\ 12 & 0 & -2 & 36 & 35 & 34 & 33 & 32 \\ 31 & -2 & 0 & 3 & 40 & 39 & 38 & 37 \\ 30 & 36 & 3 & 0 & -4 & 43 & 42 & 41 \\ 29 & 35 & 40 & -4 & 0 & -7 & 45 & 44 \\ 28 & 34 & 39 & 43 & -7 & 0 & 15 & 46 \\ 27 & 33 & 38 & 42 & 45 & 15 & 0 & -15 \\ -2 & 32 & 37 & 41 & 44 & 46 & -15 & 0 \end{bmatrix} \end{array}$$

Next, insert a special letter A before the first character to indicate that it is the first one. This way forms the complete graph with special character

Distance of AC = Code (C) – Code (A)

= 3 – 1

= 2

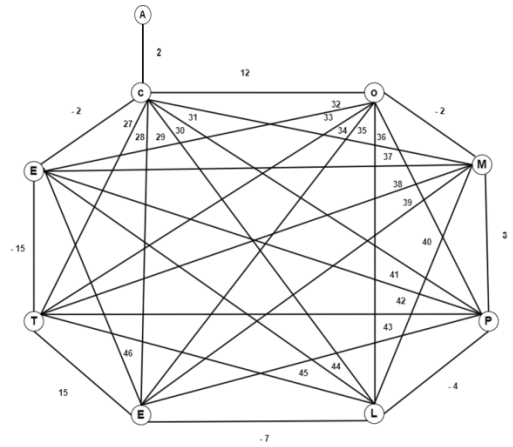

Figure complete graphs with special characters

Then, create a matrix representation of the above graph.

$$
\begin{array}{c} \\ A \\ C \\ O \\ M \\ P \\ L \\ E \\ T \\ E \end{array}
\begin{array}{c}
\begin{array}{ccccccccc} A & C & O & M & P & L & E & T & E \end{array} \\
\left[\begin{array}{ccccccccc}
0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 12 & 31 & 30 & 29 & 28 & 27 & -2 \\
0 & 12 & 0 & -2 & 36 & 35 & 34 & 33 & 32 \\
0 & 31 & -2 & 0 & 3 & 40 & 39 & 38 & 37 \\
0 & 30 & 36 & 3 & 0 & -4 & 43 & 42 & 41 \\
0 & 29 & 35 & 40 & -43 & 0 & -7 & 45 & 44 \\
0 & 28 & 34 & 39 & 4 & -7 & 0 & 15 & 46 \\
0 & 27 & 33 & 38 & 42 & 45 & 15 & 0 & -15 \\
0 & -2 & 32 & 37 & 41 & 44 & 46 & -15 & 0
\end{array}\right]
\end{array}
$$

. Now, we build a spanning tree in the graph above.

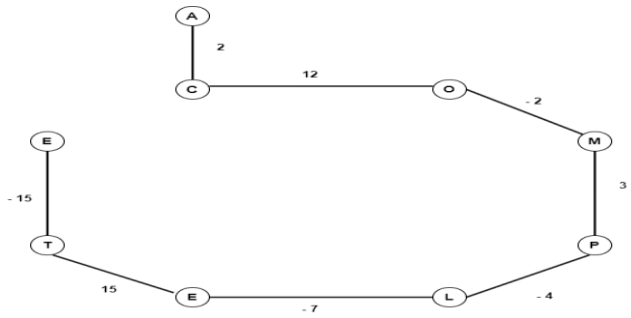

Figure: Spanning tree

$$
\begin{array}{c} \\ A \\ C \\ O \\ M \\ P \\ L \\ E \\ T \\ E \end{array}
\begin{array}{c}
\begin{array}{ccccccccc} A & C & O & M & P & L & E & T & E \end{array} \\
\left[\begin{array}{ccccccccc}
0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 0 & 12 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 12 & 0 & -2 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & -2 & 0 & 3 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 3 & 0 & -4 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & -4 & 0 & -7 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & -7 & 0 & 15 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 15 & 0 & -15 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & -15 & 0
\end{array}\right]
\end{array}
$$

Encryption Process

Certainly, you can store the character order in the diagonal instead of zeros as follows:

Character	A	c	o	M	P	L	E	T	E
Order	0	1	2	3	4	5	6	7	8

Then,

The modified B is B' = $\begin{bmatrix} 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 1 & 12 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 12 & 2 & -2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -2 & 3 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 4 & -4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -4 & 5 & -7 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -7 & 6 & 15 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 15 & 7 & -15 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -15 & 8 \end{bmatrix}$

We multiply matrix A by B to form C. C = A*B'

$$C = \begin{bmatrix} 4 & 2 & 24 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 148 & -38 & 159 & 97 & -171 & 370 & 639 & -421 \\ 64 & 12 & 148 & 102 & -2 & -207 & 454 & 261 & -239 \\ 62 & 7 & 368 & 13 & -148 & -85 & 524 & 296 & -274 \\ 60 & 462 & 426 & -63 & 25 & -321 & 916 & 324 & -302 \\ 58 & 449 & 338 & 38 & 104 & 65 & 633 & -450 & -323 \\ 56 & 436 & 326 & 178 & 317 & -207 & 274 & -585 & 143 \\ 54 & 423 & 314 & 174 & 102 & -48 & -225 & 450 & -120 \\ -4 & 382 & -34 & 170 & 99 & -266 & -257 & 585 & 225 \end{bmatrix}$$

Then, use a public key K to form the final cipher text C_t

$$K = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

So, cipher textC_t = K* C

C_t = $\begin{bmatrix} 314 & 2321 & 1872 & 771 & 594 & -1240 & 2689 & 1520 & -1311 \\ 310 & 2319 & 1848 & 771 & 594 & -1240 & 2689 & 1520 & -1311 \\ 310 & 2171 & 1886 & 612 & 497 & -1069 & 2319 & 881 & -890 \\ 286 & 2159 & 1738 & 510 & 499 & -862 & 1865 & 620 & -651 \\ 224 & 2152 & 1370 & 497 & 647 & -777 & 1341 & 324 & -377 \\ 164 & 1690 & 944 & 560 & 622 & -456 & 425 & 0 & -75 \\ 106 & 1241 & 606 & 522 & 518 & -521 & -208 & 450 & 248 \\ 50 & 805 & 280 & 344 & 201 & -314 & -482 & 1035 & 105 \\ -4 & 382 & -34 & 170 & 99 & -266 & -257 & 585 & 225 \end{bmatrix}$

We now send the encryption data C_t to the receiver.

314 2321 1872 771 594 -1240 2689 1520 -1311

310 2319 1848 771 594 -1240 2089 1520 -1311

310 2171 1886 612 497 -1069 2319 881 -890

286 2159 1738 510 499 -862 1865 620 -651

224 2152 1370 497 647 -777 1341 324 -377

164 1690 944 560 622 -456 425 0 -75

106 1241606 522 518 -521 -208 450 248

50 805 280 344 201 -314 -482 1035 105

-4 382 -34 170 99 -266 -257 585 225

Decryption Process

On the receiver side, C is obtained by multiplying the cipher text received with the inverse of shared key k^{-1}. Then calculate B by multiplying C by A^{-1}

Since $K^{-1}=$
$$\begin{bmatrix} 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$C_t =$
$$\begin{bmatrix} 314 & 2321 & 1872 & 771 & 594 & -1240 & 2689 & 1520 & -1311 \\ 310 & 2319 & 1848 & 771 & 594 & -1240 & 2689 & 1520 & -1311 \\ 310 & 2171 & 1886 & 612 & 497 & -1069 & 2319 & 881 & -890 \\ 286 & 2159 & 1738 & 510 & 499 & -862 & 1865 & 620 & -651 \\ 224 & 2152 & 1370 & 497 & 647 & -777 & 1341 & 324 & -377 \\ 164 & 1690 & 944 & 560 & 622 & -456 & 425 & 0 & -75 \\ 106 & 1241 & 606 & 522 & 518 & -521 & -208 & 450 & 248 \\ 50 & 805 & 280 & 344 & 201 & -314 & -482 & 1035 & 105 \\ -4 & 382 & -34 & 170 & 99 & -266 & -257 & 585 & 225 \end{bmatrix}$$

$k^{-1}*C_t=$
$$\begin{bmatrix} 4 & 2 & 24 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 148 & -38 & 159 & 97 & -171 & 370 & 639 & -421 \\ 64 & 12 & 148 & 102 & -2 & -207 & 454 & 261 & -239 \\ 62 & 7 & 368 & 13 & -148 & -85 & 524 & 296 & -274 \\ 60 & 462 & 426 & -63 & 25 & -321 & 916 & 324 & -302 \\ 58 & 449 & 338 & 38 & 104 & 65 & 633 & -450 & -323 \\ 56 & 436 & 326 & 178 & 317 & -207 & 274 & -585 & 143 \\ 54 & 423 & 314 & 174 & 102 & -48 & -225 & 450 & -120 \\ -4 & 382 & -34 & 170 & 99 & -266 & -257 & 585 & 225 \end{bmatrix} = C$$

Therefore $B = C*A^{-1}$

$$C = \begin{bmatrix} 4 & 2 & 24 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 148 & -38 & 159 & 97 & -171 & 370 & 639 & -421 \\ 64 & 12 & 148 & 102 & -2 & -207 & 454 & 261 & -239 \\ 62 & 7 & 368 & 13 & -148 & -85 & 524 & 296 & -274 \\ 60 & 462 & 426 & -63 & 25 & -321 & 916 & 324 & -302 \\ 58 & 449 & 338 & 38 & 104 & 65 & 633 & -450 & -323 \\ 56 & 436 & 326 & 178 & 317 & -207 & 274 & -585 & 143 \\ 54 & 423 & 314 & 174 & 102 & -48 & -225 & 450 & -120 \\ -4 & 382 & -34 & 170 & 99 & -266 & -257 & 585 & 225 \end{bmatrix}$$

Then,

Find the inverse of A

$A^{-1} = \frac{1}{|A|}\ \text{adj}(A)$

$$A^{-1} = \begin{bmatrix} \frac{-17515}{24399} & \frac{1}{2} & \frac{-14498}{36599} & \frac{47430}{12199} & \frac{24368}{36599} & \frac{-91463}{30499} & \frac{32159}{12199} & \frac{19942}{91499} & \frac{-75091}{30499} \\ \frac{1}{2} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \frac{-14498}{36599} & 0 & \frac{-10358}{54899} & \frac{10936}{60999} & \frac{27805}{54899} & \frac{-10330}{91499} & \frac{22230}{18299} & \frac{36483}{27449} & \frac{-38091}{30499} \\ \frac{47430}{12199} & 0 & \frac{10936}{60999} & \frac{-11407}{60999} & \frac{-28510}{60999} & \frac{47935}{30499} & \frac{-76429}{60999} & \frac{-39591}{30499} & \frac{41474}{30499} \\ \frac{24368}{36599} & 0 & \frac{27805}{54899} & \frac{-28510}{60999} & \frac{-29943}{54899} & \frac{15489}{91499} & \frac{-25286}{18299} & \frac{-40813}{27449} & \frac{44878}{30499} \\ \frac{-91463}{30499} & 0 & \frac{-13030}{91499} & \frac{47935}{30499} & \frac{15489}{91499} & \frac{-31919}{30499} & \frac{27397}{30499} & \frac{90233}{91499} & \frac{-28027}{30499} \\ \frac{32159}{12199} & 0 & \frac{22230}{18299} & \frac{-76429}{60999} & \frac{-25286}{18299} & \frac{27397}{30499} & \frac{-52825}{60999} & \frac{-82122}{91499} & \frac{28679}{30499} \\ \frac{19942}{91499} & 0 & \frac{36483}{27449} & \frac{-39591}{30499} & \frac{-40813}{27449} & \frac{90233}{91499} & \frac{-82122}{91499} & \frac{-17364}{27449} & \frac{18711}{30499} \\ \frac{-75091}{30399} & 0 & \frac{-38091}{30499} & \frac{41474}{30499} & \frac{44878}{30499} & \frac{-28027}{30499} & \frac{28679}{30499} & \frac{18711}{30499} & \frac{-21570}{30499} \end{bmatrix}$$

For finding matrix inverse, Python provides a sophisticated coding method. By using programming in Python,

$$C*A^{-1} = \begin{bmatrix} 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 1 & 12 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 12 & 2 & -2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -2 & 3 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 4 & -4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -4 & 5 & -7 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -7 & 6 & 15 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 15 & 7 & -15 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -15 & 8 \end{bmatrix} = B'$$

Where $C*A^{-1} = B'$, By using Figure 2.2.1. The modified B

Character	A	c	o	M	P	L	E	T	E
Order	0	1	2	3	4	5	6	7	8

$$B = \begin{bmatrix} 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 12 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 12 & 0 & -2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & -4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -4 & 0 & -7 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -7 & 0 & 15 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 15 & 0 & -15 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -15 & 0 \end{bmatrix}$$

Then, B indicates the below graph figure regardless of the diagonal, we use it to retrieve the original text.

Suppose, we take vertex 0 is A, and by using the encoding table

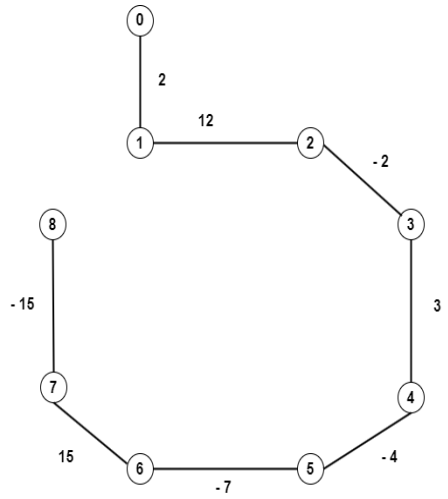

Figure: Decrypted graph

Node (1) = Code A + 2 = 3 which is Character C

Node (2) = Code C +12 = 15 which is Character O

Node (3) = Code O -2 = 13 which is Character M

Node (4) =Code M + 3 = 16 which is Character P

Node (5) = Code P - 4 = 12 which is character L

Node (6) = Code L – 7 = 5 which is character E

Node (7) = Code E + 15 = 20 which is character T

Node (8) = Code T -15 = 5 which is character E

Which gives original text Complete

Conclusion

In this paper work, we have studied an encryption technique for hiding the plain text message and for decryption technique for recovering the hidden text into the original text. We used a complete graph and spanning tree of the length of size of the message and also made use of the weighted graph. We develop a complete graph matrix and spanning tree matrix based on edge labeling using the encoding table .We modified the spanning tree with the use of a special character and applied matrix operations on these two complete matrices A and modified spanning tree Matrix B to get the First cipher text C matrix. Multiply the public key K matrix and C matrix to form the final cipher text C_t. In the decryption process, recover the encrypted data into the matrix by the use of shared key K^{-1}. The product of complete graph $A^{-1}$and first cipher text C matrix ($A^{-1}C$) to form the B matrix and the diagonal entries of B with Special character which gives the original text. Therefore, a multilayered hiding of the original plain text is obtained using the concept from Graph Theory which gives much-hidden cipher text cipher text serving the purpose of highly safe data transfer.

Reference

"Complete Graph and Hamiltonian Cycle in Encryption and Decryption"

Dharmendra Kumar Gurjar, Auparajita Krishnaa Supervisor Department of Mathematics and Statistics, University College of Science, Mohan Lal Sukhadai University, Udaipur INDIA.

Corman TH, Leiserson CE, Rivest RL, Stein C.

Introduction to the algorithm

McGraw-Hill, 2nd edition.

"Encryption Approach on Graph Theory Dharani,

Maheswari and Balaji PG and Research Department of Mathematics, Sacred Heart College, Tirupattur, Vellore District – 635 601. Tamil Nadu, S.India. Department of

Mathematics, Vels University, Chennai – 600 117.

Etaiwi W. M. A., Encryption Algorithm using Graph Theory.

Journal of Scientific Research and Reports. 3(19) (2014) 2519-2527

1) 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 Limited.

2) 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 (2015)

3) Krishnaa A. and Dulawat M.S., Algorithms for Inner Magic and Inner AntimagicLabelings for Some Planar Graphs, Informatica (Lithuania), 17(3) (2006) 393-406.

4) Krishnaa A., Inner magic and inner antimagic graphs in cryptography Journal of Discrete Mathematical Sciences and Cryptography, 22(6) (2019) 1057-1066.

5) Krishnaa A., Certain specific graphs in cryptography, Advances and Applications in Discrete Mathematics, 26(2) (2021) 157-177.

6) Perera P.A.S. and Wijesiri G.S., Encryption and decryption in symmetric key cryptography using graph theory, (2021).

7) Shamir Adi, Random graphs in cryptography, The Weizman Institute, Israel, The Onassis Foundation Science Lecture Series, 28 (2010).

8) Some Applications of Labelled Graphs, International Journal of Mathematics Trends and Technology, 37(3) (2016).

9) Ustimenko VA. On graph-based cryptography and symbolic computations, Serdica, Journal of Computing, 2007, 131-156.

10) Uma Dixi, CRYPTOGRAPHY A GRAPH THEORY APPROACH, International Journal of Advance Research in Science and Engineering 6(01), September 2017, BVCNCS 2017.

11) Wael Mahmoud Al Etaiwi, Encryption Algorithm Using Graph Theory, Journal of Scientific Research and Reports,3(19), 2004 2519-2527; Article number JSSRR. 2014.19.004.

12) Yamuna M. and Karthika K**.,** Data transfer using bipartite Graphs. International Journal of Advance Research in Science and Engineering (IJARSE), 4(2)

13) Yammuna M. Meenal Gogia Ashish Sikka, Md. Jazih Hayat Khan Encryption using graph theory and linear algebra, International Journal of Computer Application 2012, 2250-1797.