iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 Issue: III Month of publication: March 2026

DOI: https://doi.org/10.22214/ijraset.2026.79150

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

A Graph-Theory Based Encryption Model Utilizing Spanning Tree Transformations

Vidhya S[1], Sivashankari R[2]
[1]*Associate Professor, PG and Research Department of Mathematics, Cauvery College for Women (Autonomous), (Afflicated to Bharathidasan University), Tiruchirapalli - 18, Tamilnadu, India*
[2]*PG Student, PG and Research Department of Mathematics, Cauvery college for Women (Autonomous), (Afflicated to Bharathidasan University), Tiruchirapalli - 18, Tamilnadu, India*

Abstract: We will examine how the messages can be encrypted and decrypted using the complete graph and spanning tree principles from graph theory.
Keywords: Encryption, Decryption, Spanning tree, Complete graph.

I. INTRODUCTION

Cryptography plays an important role in securing digital communication and protecting information and ensuring secure communication in modern digital systems. With the rapid growth of the internet and digital data exchange, the need for efficient and reliable encryption techniques has become increasingly important. Encryption converts readable information into an encoded form so that only authorized users can access the original messages. Mathematical concepts are widely used in cryptography to design secure and systematic encryption methods. Graph theory is an important branch of mathematics that studies the relationships between objects using vertices and edges. Many graph structures have practical application in computer science, network security, and communication systems. Among these structures, the spanning tree is a fundamental concept that connects all vertices of a graph without forming cycles while maintaining minimum edges. Due to its structured and organized nature, the spanning tree concept can be effectively utilized in designing encryption techniques. Graph-based cryptographic techniques have gained the attention because of their simplicity and strong mathematical foundation. In particular, the spanning tree structure provides an efficient way to represent relationships between vertices while maintaining connectivity without cycles. This property makes spanning trees suitable for constructing unique paths within a graph, which can be used to encode information in a systematic manner. By assigning numerical values or symbols to vertices and edges, messages can be transformed into encrypted forms through graph traversal methods. Furthermore, the use of spanning trees in message encryption offers advantages such as structural clarity, reduced complexity, and flexibility in designing encoding schemes. Since a spanning tree connects all vertices with the minimum number of edges, it provides an organized framework for representing and transmitting information securely. The integration of graph theory with cryptography not only enhances the understanding of mathematical applications but also contributes to the development of innovative techniques for secure communication. In this paper, we explore the use of spanning trees for encrypting and decrypting messages. The proposed approach represents characters of a message using graph vertices and constructs a spanning tree to determine the path used for encoding the message. By following the structure of the spanning tree, the original message can be transformed into an encrypted form and later decoded using the same method.

II. METHOD OF ANALYSIS

A. Section 2.1

We will encrypt the data DACE**,** which we will be sending to the receiver on other hand. Now, we change this text into graph by converting each letter to vertices of graph.

STEP 1:

Draw each letter as node of graph.

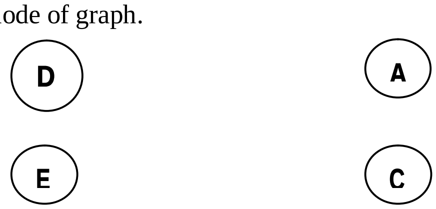

Figure 2.1: Convert the letter into vertex (node)

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

We encrypt the message using graph theory's spanning tree notion.

A	B	C	-	-	-	W	X	Y	Z
1	2	3	-	-	-	23	24	25	26

STEP 2:
Form a cycle graph, we link two characters which is denoted as vertex.

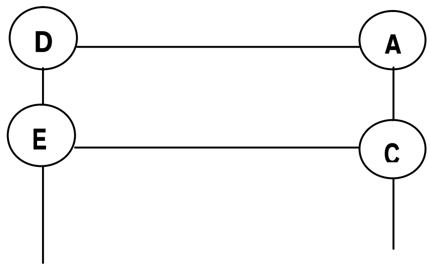

Figure 2.2: Cycle graph

STEP 3:
In this step we create the encoding table

This encoding table represent each character by the numerical values. By using Encoding table, we can find the distance between two vertices. Each edge represents the distance between two vertices. To find the distance between the connected two vertices. We have

Distance = code (A) – code (D) = 1 – 4 = -3.

By continuing this process, we can find the distance of other edges in the graph. Then we label the graph containing all the plain text letters and we get weighted graph.

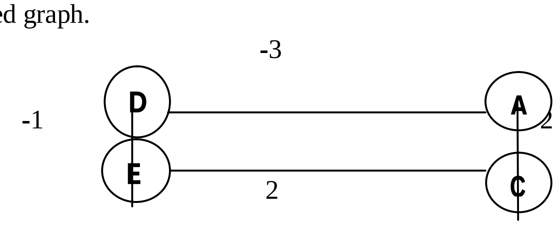

Figure 2.3: Weighted Graph

STEP 4
Then we add the edges to form complete graph. Each new added edge has a sequential weight starting from maximum weight in the encoding table which the maximum weight is 26. The new added edge has weight 27, 28 and so on.

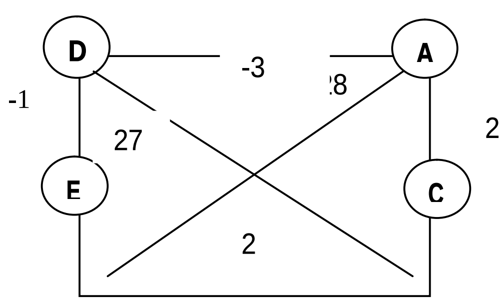

Figure 2.4: Complete weighted graph

STEP 5:

Then add a special character before the first character. The special character is "A".

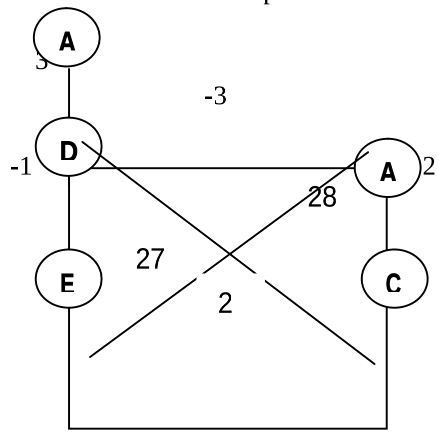

Figure 2.5: Complete graph with special character

Represent the above graph in the matrix form.

$$A_1 = \begin{bmatrix} 0 & 3 & 0 & 0 & 0 \\ 3 & 0 & -3 & 27 & -1 \\ 0 & -3 & 0 & 2 & 28 \\ 0 & 27 & 2 & 0 & 2 \\ 0 & -1 & 28 & 2 & 0 \end{bmatrix}$$

STEP 6:

Construct a minimal spanning tree for above complete weighted graph with special character.

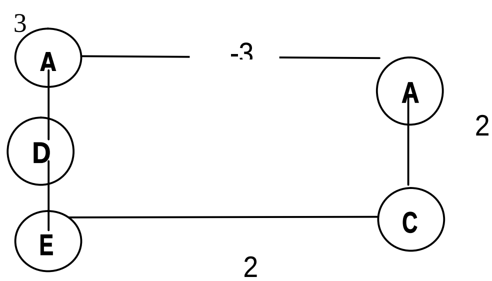

Figure 2.6: Minimal Spanning Tree

Represent the above graph in the matrix form.

$$A_2 = \begin{bmatrix} 0 & 3 & 0 & 0 & 0 \\ 3 & 0 & -3 & 0 & 0 \\ 0 & -3 & 0 & 2 & 0 \\ 0 & 0 & 2 & 0 & 2 \\ 0 & 0 & 0 & 2 & 0 \end{bmatrix}$$

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

III. ENCRYPTION PROCESS

STEP 1:
Give the number for taken original plain text.

A	D	A	C	E
0	1	2	3	4

The diagonal value of A_2 can be changed so that we get the modified matrix A_2 .

Then the modified matrix $A_2 = \begin{bmatrix} 0 & 3 & 0 & 0 & 0 \\ 3 & 1 & -3 & 0 & 0 \\ 0 & -3 & 2 & 2 & 0 \\ 0 & 0 & 2 & 3 & 2 \\ 0 & 0 & 0 & 2 & 4 \end{bmatrix}$

STEP 2:

Multiply A_1 and modified A_2 to get the new matrix A_3

$$A_1 A_2 = A_3 = \begin{bmatrix} 9 & 3 & -9 & 0 & 0 \\ 0 & 18 & 48 & 73 & 50 \\ -9 & -3 & 13 & 62 & 116 \\ 81 & 21 & -77 & 8 & 8 \\ -3 & -85 & 63 & 62 & 4 \end{bmatrix}$$

STEP 3:
Now, we use public key to encrypt C

$$\text{Let } k = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

To find the cipher text C, we multiply public key K and A_3

Then $C = kA_3$

$$C=\begin{bmatrix}1&1&1&1&1\\0&1&1&1&1\\0&0&1&1&1\\0&0&0&1&1\\0&0&0&0&1\end{bmatrix}\begin{bmatrix}9&3&-9&0&0\\0&18&48&73&50\\-9&-3&13&62&116\\81&21&-77&8&8\\-3&-85&63&62&4\end{bmatrix}$$

$$C=\begin{bmatrix}84&-44&106&209&186\\75&-47&115&209&186\\75&-65&68&132&128\\84&-62&64&70&12\\3&-83&60&62&4\end{bmatrix}$$

Now, we send the cipher text to the receiver
84 -44 106 209 186 75 -47 115 209 186 75 -65 68 132 128 84
-62 64 70 12 3 -83 60 62 4.

1) Decryption Process

On the other hand, the cipher text is multiplying with inverse of shared public key

$C = KA_3$ then $A_3 = CK^{-1}$

$$A_3=\begin{bmatrix}84&-44&106&209&186\\75&-47&115&209&186\\75&-65&68&132&128\\84&-62&64&70&12\\3&-83&60&62&4\end{bmatrix}\begin{bmatrix}1&-1&0&0&0\\0&1&-1&0&0\\0&0&1&-1&0\\0&0&0&1&-1\\0&0&0&0&1\end{bmatrix}$$

Therefore, $A_2 = A_3A_1^{-1} = \begin{bmatrix}0&3&0&0&0\\3&1&-3&0&0\\0&-3&2&2&0\\0&0&2&3&2\\0&0&0&2&4\end{bmatrix}$

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

A_2 represent the original text. The diagonal represents the original text.

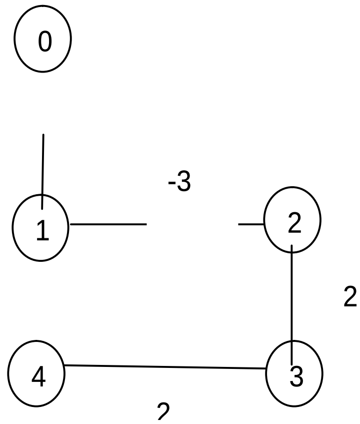

Figure 2.7: Decrypted Graph

Suppose the vertex 0 is A, then by using encoding table
Vertex 1 = code (A) + 3 = 4, which is character D
Vertex 2 = code (D) – 3 = 1, which is character A
Vertex 3 = code (A) + 2 = 3, which is character C
Vertex 4 = code(C) + 2 = 5, which is character E
Which gives us to the original text **'DACE'.**

B. Section 2.2

We will encrypt the data **MATHS,** which we will be sending to the receiver on other hand. Now, we change this text into graph by converting each letter to vertices of graph.

STEP 1:

Draw a each letter as node of graph.

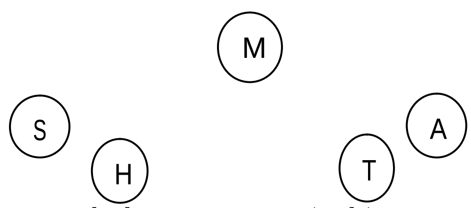

Figure 2.8: Convert the letter into vertex (node)

STEP 2:

Form a cycle graph by joining two vertices.

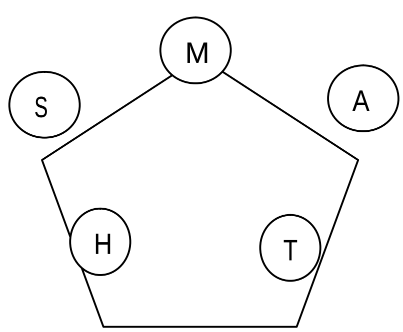

Figure 2.9: Cycle graph

STEP 3:

In this step we create the encoding table

A	B	C	-	-	-	W	X	Y	Z
1	2	3	-	-	-	23	24	25	26

This encoding table represent each character by the numerical values. By using Encoding table, we can find the distance between two vertices. Each edge represents the distance between two vertices. To find the distance between the connected two vertices.

We have Distance = code (A) – code (M) = 1 – 13 = -12. By continuing this process, we can find the distance of other edges in the graph. Then we label the graph containing all the plain text letters and we get weighted graph.

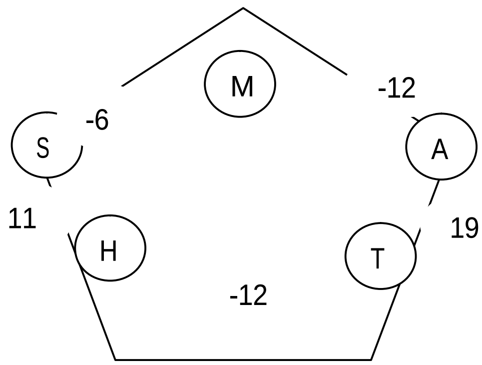

Figure 2.3: Weighted Graph

STEP 4:

Then we add the edges to form complete graph. Each new added edge has a sequential weight starting from maximum weight in the encoding table which the maximum weight is 26. The new added edge has weight 27, 28, 29, 30.

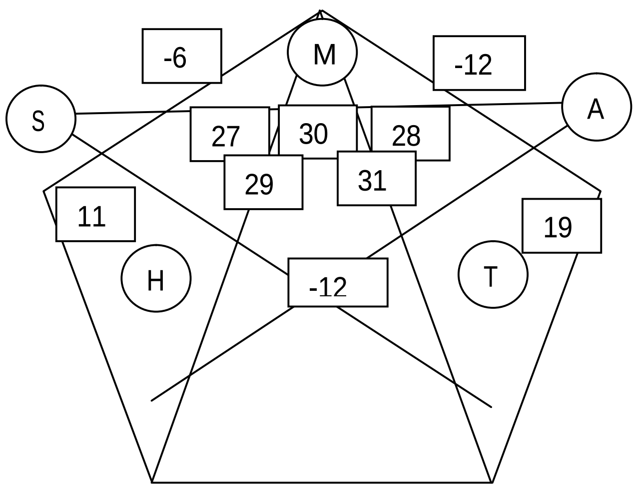

Figure 2.10: Complete weighted Graph

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

STEP 5:

Then add a special character before the first character. The special character is "A".

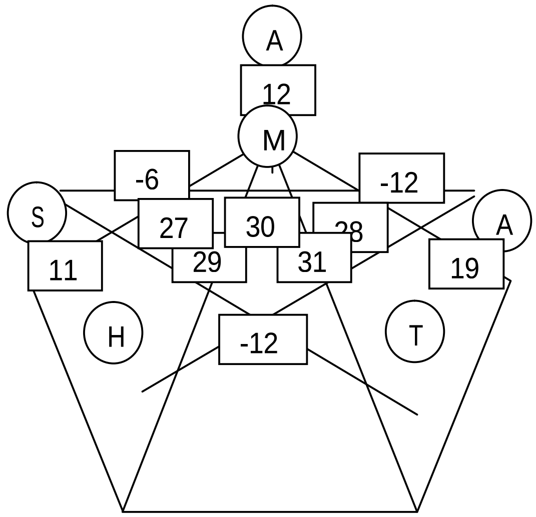

Figure 2.11: Complete plain graph with special character

Represent the graph in the matrix from.

$$A_1 = \begin{bmatrix} 0 & 12 & 0 & 0 & 0 & 0 \\ 12 & 0 & -12 & 28 & 27 & -6 \\ 0 & -12 & 0 & 19 & 31 & 30 \\ 0 & 28 & 19 & 0 & -12 & 29 \\ 0 & 27 & 31 & -12 & 0 & 11 \\ 0 & -6 & 30 & 29 & 11 & 0 \end{bmatrix}$$

STEP 6:

Construct the minimal spanning tree for the above graph.

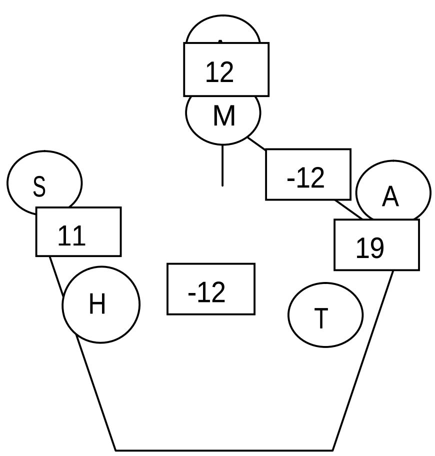

Figure 2.12: Minimal Spanning Tree

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

Represent the above graph by matrix.

$$A_2 = \begin{bmatrix} 0 & 12 & 0 & 0 & 0 & 0 \\ 12 & 0 & -12 & 0 & 0 & 0 \\ 0 & -12 & 0 & 19 & 0 & 0 \\ 0 & 0 & 19 & 0 & -12 & 0 \\ 0 & 0 & 0 & -12 & 0 & 11 \\ 0 & 0 & 0 & 0 & 11 & 0 \end{bmatrix}$$

1) Encryption Process

STEP 1:

Give the number for taken original plain text.

The diagonal value of A_2 can be changed so that we get the modified matrix A_2. Then the modified matrix

$$A_2 = \begin{bmatrix} 0 & 12 & 0 & 0 & 0 & 0 \\ 12 & 1 & -12 & 0 & 0 & 0 \\ 0 & -12 & 2 & 19 & 0 & 0 \\ 0 & 0 & 19 & 3 & -12 & 0 \\ 0 & 0 & 0 & -12 & 4 & 11 \\ 0 & 0 & 0 & 0 & 11 & 5 \end{bmatrix}$$

STEP 2:

Multiply A_1 and modified A_2 to get the new matrix A_3.

$$A_1 A_2 = A_3 = \begin{bmatrix} 144 & 12 & -144 & 0 & 0 & 0 \\ 0 & 288 & 508 & -468 & -294 & 267 \\ -144 & -12 & 505 & -315 & 226 & 491 \\ 336 & -200 & -298 & 505 & 271 & 13 \\ 324 & -345 & -490 & 553 & 265 & 55 \\ -72 & -366 & 683 & 525 & -304 & 121 \end{bmatrix}$$

STEP 3:

Now we use public key to encrypt C.

A	M	A	T	H	**S**
0	1	2	3	4	5

$$\text{Let } k = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

To find the cipher text C, we multiply public key K and A_3

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

$$C = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 144 & 12 & -144 & 0 & 0 & 0 \\ 0 & 288 & 508 & -468 & -294 & 267 \\ -144 & -12 & 505 & -315 & 226 & 491 \\ 336 & -200 & -298 & 505 & 271 & 13 \\ 324 & -345 & -490 & 553 & 265 & 55 \\ -72 & -366 & 683 & 525 & -304 & 121 \end{bmatrix}$$

$$C = \begin{bmatrix} 588 & -623 & 764 & 800 & 164 & 947 \\ 444 & -635 & 908 & 800 & 164 & 947 \\ 444 & -923 & 400 & 1268 & 458 & 680 \\ 588 & -911 & -105 & 1583 & 232 & 189 \\ 252 & -711 & 193 & 1078 & -39 & 176 \\ -72 & -366 & 683 & 525 & -304 & 121 \end{bmatrix}$$

Cipher text: 588 -623 764 800 164 947 444 -635 908 800 164 947 444 -923 400 1268 458 680 588 -911 -105 1583 232 189 252
-711 193 1078 -39 176 -72 -366 683 525 -304 121.

2) Decryption Process

On the other hand, the cipher text is multiplying with inverse of shared public key

$C = KA_3$ then $A_3 = CK^{-1}$

$$A_3 = \begin{bmatrix} 588 & -623 & 764 & 800 & 164 & 947 \\ 444 & -635 & 908 & 800 & 164 & 947 \\ 444 & -923 & 400 & 1268 & 458 & 680 \\ 588 & -911 & -105 & 1583 & 232 & 189 \\ 252 & -711 & 193 & 1078 & -39 & 176 \\ -72 & -366 & 683 & 525 & -304 & 121 \end{bmatrix} \times \begin{bmatrix} 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Therefore, $A_2 = A_3 A^{-1} = \begin{bmatrix} 0 & 12 & 0 & 0 & 0 & 0 \\ 12 & 1 & -12 & 0 & 0 & 0 \\ 0 & -12 & 2 & 19 & 0 & 0 \\ 0 & 0 & 19 & 3 & -12 & 0 \\ 0 & 0 & 0 & -12 & 4 & 11 \\ 0 & 0 & 0 & 0 & 11 & 5 \end{bmatrix}$

A_2 represent the original text. The diagonal values represent the original text.

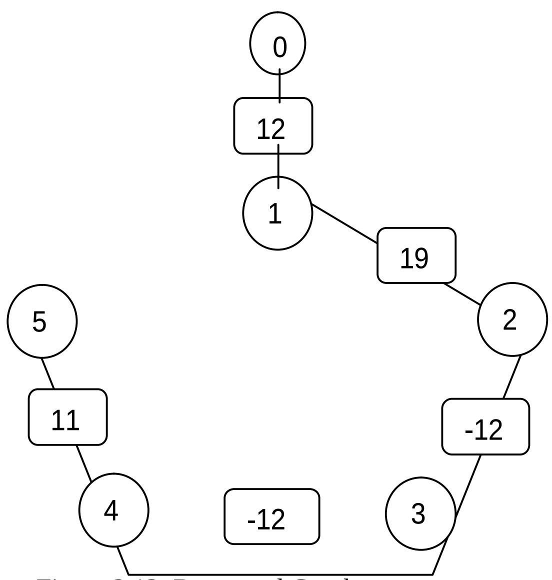

Figure 2.13: Decrypted Graph

We take the vertex 0 is A, then by encoding table,

Vertex 1 = code (A) + 12 = 1 + 12 = 13, which is character M

Vertex 2 = code (M) - 12 = 13 - 12 = 1, which is character A

Vertex 3 = code (A) + 19 = 1 + 19 = 20, which is character T

Vertex 4 = code (T) - 12 = 20 - 12 = 8, which is character H

Vertex 5 = code (H) + 11 = 8 + 11 = 19, which is character S

The original text is ‘MATHS’.

IV. CONCLUSION

In this paper, we have studied to encrypt the original plain text into numerical values by using spanning tree concept, for this first we convert the letter in plain text into vertices and join all the vertices to form cycle graph, then by using encoding table we find the value for edges so that we get weighted graph. We add extra edges for the weighted graph to form complete weighted graph. By using Kruskal's or prim's algorithm we can construct minimal spanning tree then convert into matrix form. In encryption process, we use public key as matrix form (upper triangular matrix) to get cipher text. In decryption process, we use inverse of public key as matrix form to decrypt the cipher text and we get the original plain text.

REFERENCES

[1] Corman TH, Leiserson CE, Rivest RL, Stein C. Introduction to algorithm 2nd edition, McGraw-Hill.

[2] Etaiwi W. M. A., Encryption Algorithm using Graph Theory. Journal of Scientific Research and Reports. 3(19) (2014) 2519-2527.

[3] Janaki, G., & Vidhya, S. (2016). On the integer solutions of the Pell equation t y x 4 20 2 2-=. International Journal of Multidisciplinary Research and Development, 3(5), 39-42.

[4] Janaki, G., & Vidhya, S. (2016). On the integer solutions of the Pell equation k y x 9 79 2 2=-. International Journal of Scientific Research in Science, Engineering and Technology, 2(2), 1195-1197.

[5] Janaki, G., & Vidhya, S. (2016). On the negative Pell equation 3 21 2 2-= x y. International Journal of Applied Research, 2(11), 462-466.

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

[7] 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.

[8] Litta, E., & Dharshini, S. M. (2023). Proper Colourings in r-Regular Modified Zagreb Index Graph. International Journal for Research in Applied Science & Engineering Technology (IJRASET), 11(3), 1553-1558.

[9] Litta, E., & Datchini, S. (2023). Proper Colourings in r–Regular Zagreb Index Graph. Aryabhatta Journal of Mathematics and Informatics, 15(1), 149-154.

[10] E Litta, S Narmadha. Proper Colourings in -Regular Inverse Sum Indeg Index Graphs. Research and Applications Towards Mathematics and Computer Science Vol. 9, BP International, pp.66-76, 2024. ⟨hal-05249331⟩.

[11] Uma Dixit, CRYPTOGRAPHY A GRAPH THEORY APPROACH, International Journal of Advance Research in Science and Engineering, 6(01) , 2017, BVCNSCS 2017.

[12] Wael Mahmoud Al Etaiwi, Encryption Algorithm Using Graph Theory, Journal of Scientific Research and Reports, 3(19), 2519-2527, 2014, Article no. JSRR.2014.19.004.

[13] 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, 2012.