iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** XI **Month of publication:** November 2022

DOI: https://doi.org/10.22214/ijraset.2022.47675

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue XI Nov 2022- Available at www.ijraset.com

An Approach of Graph Theory on Cryptography

Indhu. K[1], Rekha. S[2]
[1]*M.sc Mathematics, Department of Mathematics, Dr. SNS Rajalakshmi College of Arts and Science, Coimbatore, Tamil Nadu, India*
[2]*Assistant Professor, Department of Mathematics, Dr.SNS Rajalakshmi college of Arts and Science, Coimbatore, Tamil Nadu, India*

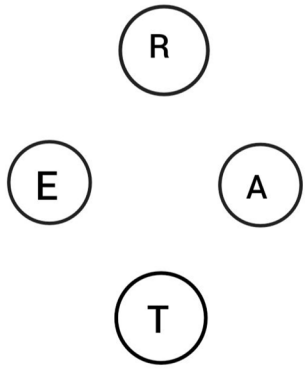
Abstract: In this paper, we discuss about the connection between graph theory and cryptography. We use the spanning tree concept of graph theory to encryption the message.
Keywords: Public key, cryptography, graphs, encryption, network security.

I. INTRODUCTION

Cryptography is the art of protect information by transforming it to unreadable format called Cipher text. The process of converting plain text to cipher text called encryption, and the process of converting cipher text on its original plain text called decryption. The remainder of this paper is a discussion of intractable problem from graph theory keeping cryptography as the base.
Firstly we represent the given text as node of the graph. Every node represent a character of the data. Now every adjacent character in the given text will be represented by adjacent vertices in the graph.

II. APPLICATION

Example :1
We will encrypt the text or data, say *RATE* , which we will be sending to the receiver on the other end.
Now we change this text into graph by converting each letter to vertices of graph.



Convert the letter to vertex(node)

To form a Cycle Graph , we link each two characters.

Further we label each edge by using the encoding table, which is followed by most researchers.

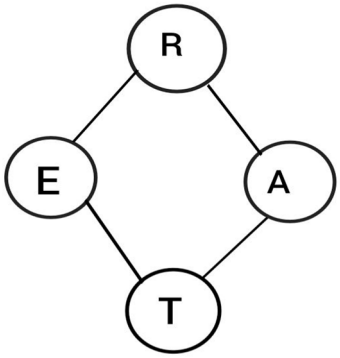
Table 1 : Encoding Table

A	B	C	D	-	-	-	-	W	X	Y	Z
1	2	3	4	-	-	-	-	23	24	25	26

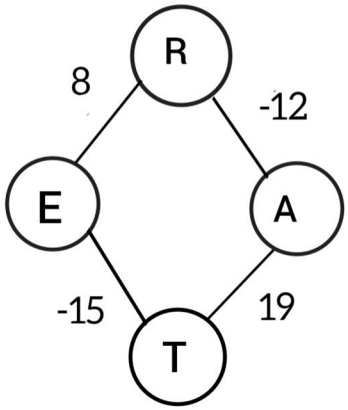
The label on each edge represents the distance between the connected two vertices from the encoding table. So the edge connecting vertex *C* with vertex *O* has a label which is distance between the two characters in the encoding table.

Distance = code (*A*)−code (*H*) = 1 − 8 = −7.

Similarly we can deduce the distances of other edges. Then we label the graph containing all the plaintext letters and we get weighted graph which is given below. After that, we keep adding edges to form a complete graph and each new added edge has a sequential weight starting from the maximum weight in the encoding table which is 26.Therefore we can add 27,28 and so on.

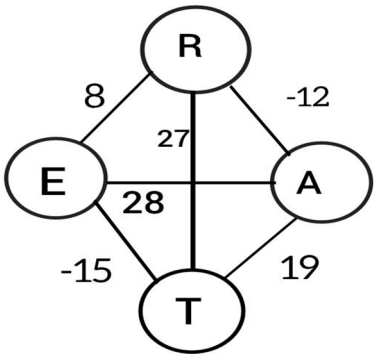


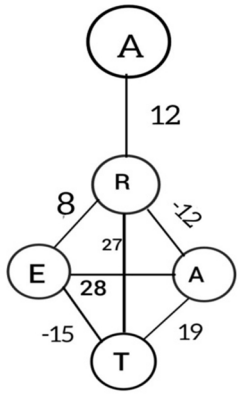
cycle Graph



Weighted Graph

Then add a special character before the first character to point to the first character, say A is special character , then we get.





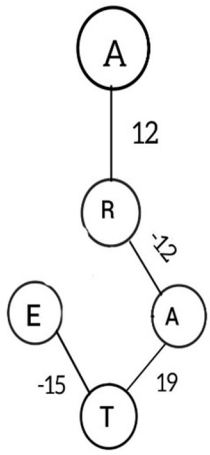
Complete plain Graph

Complete plain Graph with special character

Now represent the above graph in the form of a matrix.

$$A1 = \begin{matrix} 0 & 12 & 0 & 0 & 0 \\ 12 & 0 & -12 & 27 & 8 \\ 0 & 12 & 0 & 19 & 28 \\ 0 & 27 & 19 & 0 & -15 \\ 0 & 8 & 0 & -15 & 0 \end{matrix}$$

We now construct a minimal spanning tree of the above graph



Minimal spanning tree

$$A2 = \begin{matrix} 0 & 12 & 0 & 0 & 0 \\ 12 & 0 & -12 & 0 & 0 \\ 0 & -12 & 0 & 19 & 0 \\ 0 & 0 & 19 & 0 & -15 \\ 0 & 0 & 0 & -15 & 0 \end{matrix}$$

A. Encryption Process

Now we store the character order in the diagonalinstead of zeroes as follows:

Table 2 :

A	H	A	T	E
0	1	2	3	4

The modified A2=

0	12	0	0	0
0	1	-12	0	0
0	-12	2	19	0
0	0	1 9	3	-15
0	0	0	-15	4

we multiply matrix A_1 by A_2 to form A^1.

A3 = A1A2 =

0	12	-144	0	0
0	288	-450	-267	437
0	144	505	363	-173
0	-201	-511	586	-60
0	8	-381	-45	225

We now send the encrypted data C to the receiver -37-981 637 429 -49 -837 -637 429 -337 -387 904 8 -193 892 541 1 8 -381 -45 225.

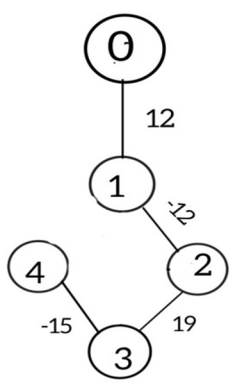
B. Decryption Process

On the receiver side, C is got from multiplying the cipher text received with the inverse of shared Key Then calculate B by multiplying C by K−1

A3=

0	1728	2412	2112	96
0	-1809	-1293	6446	6309
0	-1103	3724	3112	4293
0	9642	11868	-14236	-10398
0	5157	5349	-10398	739

Then A_2 represent the below graph, regardless of te diagonal, we use it to retrieve the original text.



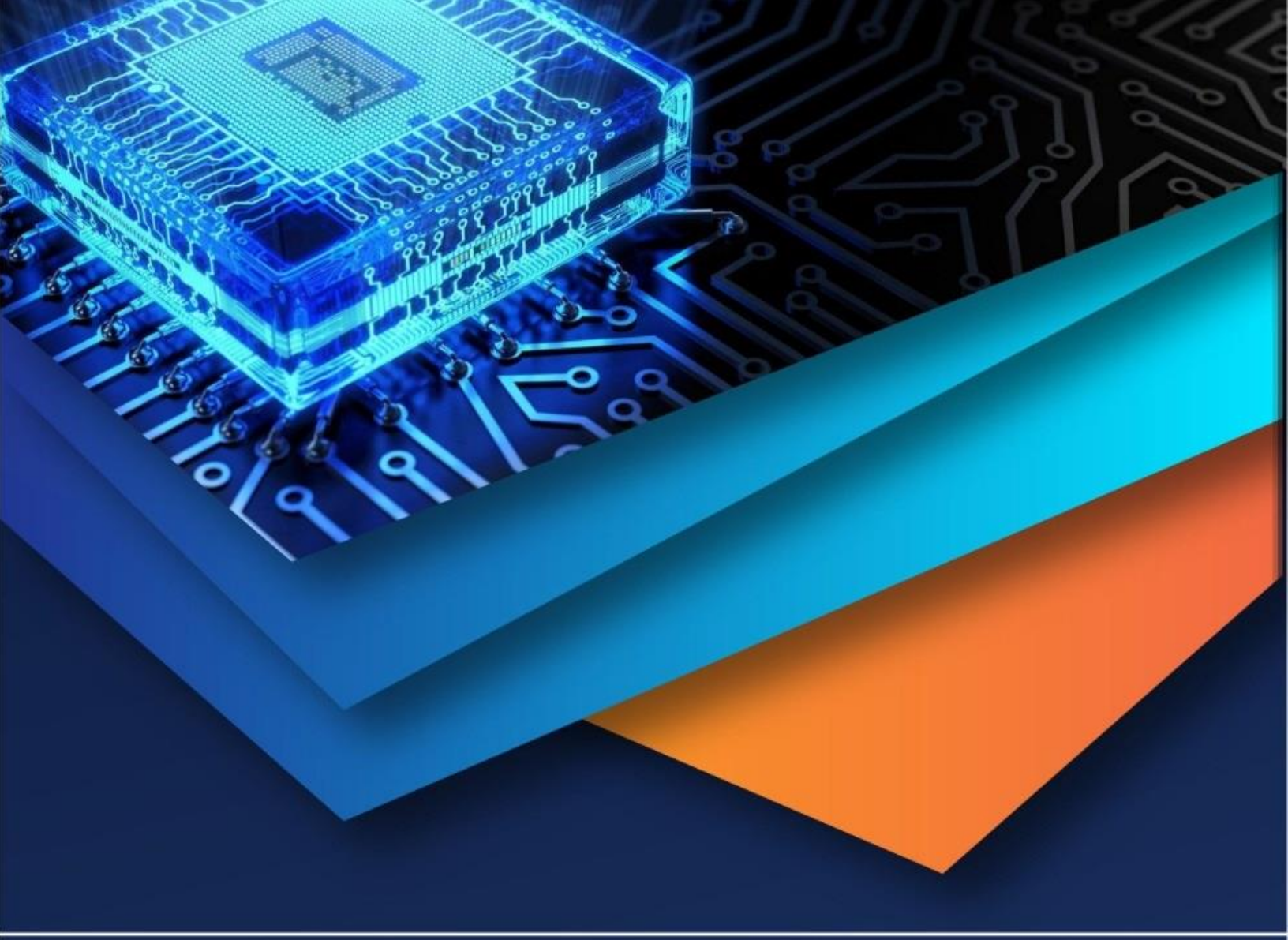
Decrypted Graph

We suppose that the vertex 0 is A, and by using encoding table
Vertex 1 = code (A) + -19 = 18, which is character R
Vertex 2 = code (H) - 7 = 1, which is character A
Vertex 3 = code (A) + 19 = 20, which is character T
Vertex 4 = code (T) + −15 = 5, which is character E
Which gives us the original text R A T E

Acknowledgement
One of the author (Dr. V. Balaji) acknowledges University Grants Commission, SERO, Hyderabad and India for financial assistance (*No.FMRP*5766/15(*SERO/UGC*)).

REFERENCES

[1] Corman TH, Leiserson CE, Rivest RL, Stein C. Introduction to algorithms 2nd edition, McGraw-Hill.
[2] 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.
[3] Ustimenko VA. On graph-based cryptography and symbolic computations, Serdica. Journal of Computing, 2007, 131-156.
[4] Uma Dixit,CRYPTOGRAPHY A GRAPH THEORY APPROACH, International Journalof Advance Research in Science and Engineering, 6(01), 2017, BVCNSCS 2017.
[5] Wael Mahmoud Al Etaiwi , Encryption Algorithm Using Graph Theory, Journal of Scientific Research and Reports, 3(19), 2519-2527, 2014, Article no.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY