J. Comp.Matha. Vol.2(1), (2018). ISSN: 2456–8686

Original Research Article

SACRED HEART RESEARCH PUBLICATIONS

Journal of Computational Mathematica

Journal homepage: www.shcpub.edu.in

COMPUTATIONAL MATHEMATICA

ISSN: 2456-8686

A Graph Theory Approach on Cryptography

[1]R.Nandhini, [2]V.Maheswari and [3]V.Balaji

Received on 15 January 2018, Accepted on 02 April 2018

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.

Key words: Public key, cryptography, graphs, encryption, network security.

1. Introduction

Definition 1.1. **Weighted graph** is a graph in which each branch is given a numerical weight. A weighted graph is therefore a special type of labeled graph in which the labels are numbers.

Definition 1.2. A cycle graph of order n is a connected graph whose edges form a **cycle** of length n.

Definition 1.3. A **spanning tree** T of a graph G is a sub graph 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. Out of all the spanning trees of G, the minimum spanning tree is one with least weight.

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

[1]Corresponding Author: E-mail: pulibala70@gmail.com

[1,3]PG and Research Department of Mathematics, Sacred Heart College, Tirupattur, Vellore District - 635 601, Tamil Nadu, S.India,

[2]Department of Mathematics, Vels University, Chennai - 600117.

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.

2. Proposed Application

Example 2.1. *We will encrypt the text or data, say* ***HATE*** *, 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.

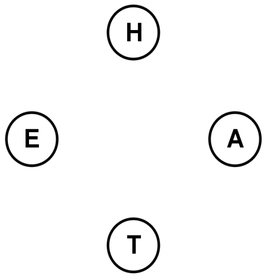

Figure 1. Convert the letter to vertex(node)

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

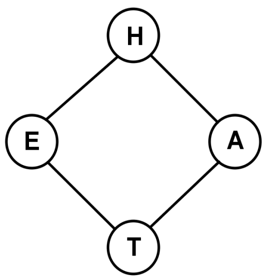

Figure 2. cycle Graph

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 plain text letters and we get weighted graph which is given below.

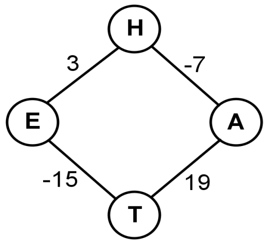

Figure 3. Weighted Graph

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.

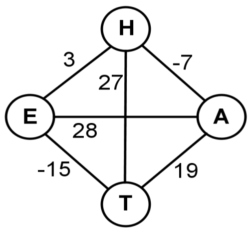

Figure 4. Complete plain Graph

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

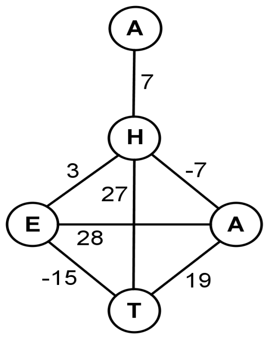

Figure 5. Complete plain Graph with special character

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

$$A_1 = \begin{bmatrix} 0 & 7 & 0 & 0 & 0 \\ 7 & 0 & -7 & 27 & 3 \\ 0 & -7 & 0 & 19 & 28 \\ 0 & 27 & 19 & 0 & -15 \\ 0 & 3 & 28 & -15 & 0 \end{bmatrix}$$

We now connstruct a minimal spanning tree of the above graph

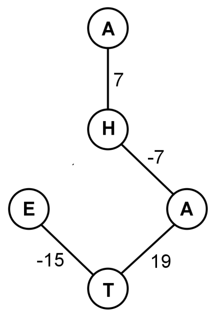

FIGURE 6. Minimal spanning tree

$$A_2 = \begin{bmatrix} 0 & 7 & 0 & 0 & 0 \\ 7 & 0 & -7 & 0 & 0 \\ 0 & -7 & 0 & 19 & 0 \\ 0 & 0 & 19 & 0 & -15 \\ 0 & 0 & 0 & -15 & 0 \end{bmatrix}$$

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

Then the modified A_2 is $$\begin{bmatrix} 0 & 7 & 0 & 0 & 0 \\ 7 & 1 & -7 & 0 & 0 \\ 0 & -7 & 2 & 19 & 0 \\ 0 & 0 & 19 & 3 & -15 \\ 0 & 0 & 0 & -15 & 4 \end{bmatrix}.$$

we multiply matrix A_1 by A_2 to form A_3.

$$A_3 = A_1A_2 = \begin{bmatrix} 49 & 7 & -49 & 0 & 0 \\ 0 & 98 & 499 & 36 & -393 \\ -49 & -7 & 410 & -363 & -173 \\ 189 & -106 & -151 & 225 & 60 \\ 21 & -193 & -250 & -45 & 225 \end{bmatrix}$$

Then use a Public Key K to encrypt C

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

so cipher text$C = KA_3$

$$C = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 49 & 7 & -49 & 0 & 0 \\ 0 & 98 & 499 & 36 & -393 \\ -49 & -7 & 410 & -363 & -173 \\ 189 & -106 & -151 & 225 & 60 \\ 21 & -193 & -250 & -45 & 225 \end{bmatrix}$$

$$C = \begin{bmatrix} 210 & -201 & 459 & -147 & -401 \\ 161 & -208 & -508 & -147 & 401 \\ 161 & -306 & 9 & -183 & -8 \\ 210 & -299 & -401 & 180 & 165 \\ 21 & -193 & -250 & -45 & 225 \end{bmatrix}$$

We now send the encrypted data C to the receiver.

210 -201 459 -147 401 161 -208 -508 -147 401 161 -306 9 -183 -8 210 -299 -401 180 165 21 -193 -250 -45 225

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}

$$A_3 = \begin{bmatrix} 210 & -201 & 459 & -147 & -401 \\ 161 & -208 & -508 & -147 & 401 \\ 161 & -306 & 9 & -183 & -8 \\ 210 & -299 & -401 & 180 & 165 \\ 21 & -193 & -250 & -45 & 225 \end{bmatrix} \begin{bmatrix} 1 & -1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\text{Therefore , } A_2 = A_3 A_1^{-1} = \begin{bmatrix} 0 & 7 & 0 & 0 & 0 \\ 7 & 0 & -7 & 0 & 0 \\ 0 & -7 & 0 & 19 & 0 \\ 0 & 0 & 19 & 0 & -15 \\ 0 & 0 & 0 & -15 & 0 \end{bmatrix}$$

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

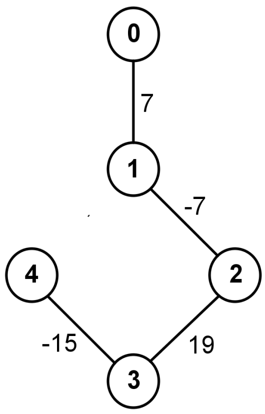

FIGURE 7. Decrypted Graph

We suppose that the vertex 0 is A, and by using encoding table

Vertex 1 = code (A) + 7 = 8, which is character H

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 H A T E

3. Acknowledgement

One of the author (Dr. V. Balaji) acknowledges University Grants Commission, SERO, Hyderabad and India for financial assistance $(No.FMRP5766/15(SERO/UGC))$.

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 Vol.No.6, Special Issue (01), September 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. JSRR.2014.19.004