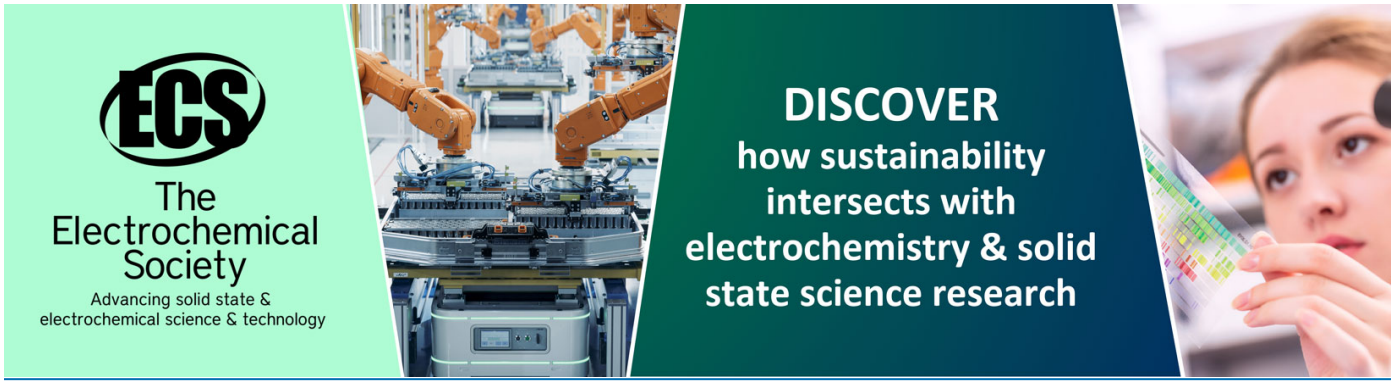
Encryption and Decryption Process Using Edge Magic Labeling



Journal of Physics: Conference Series **1362** (2019) 012024 doi:10.1088/1742-6596/1362/1/012024

ENCRYPTION AND DECRYPTION PROCESS USING EDGE MAGIC LABELING

D.A.ANGEL SHERIN[1] and V.MAHESWARI[2]

[1]Research Scholar, Department of Mathematics, Vels Institute of Science Technology & Advanced Studies (VISTAS), Pallavaram Chennai.
d.a.angelsherin@gmail.com

[2]Associate Professor Department of Mathematics, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Pallavaram Chennai.

maheswari.sbs@velsuniv.ac.in

ABSTRACT--In this paper we are using edge magic labeling graph to encrypt a message. Then using Longest cycle path technique we decrypt the message by inverse matrix multiplication.
Keywords: Labeling, Encryption, Decryption, Cycle Graph.
2010 Mathematical subject classification Number: 05C78.

1. INTRODUCTION

Wael Mahmoud Al Etaiwi [2] conferred an encryption algorithm using minimum spanning tree, they encrypt the data from spanning tree and decrypt the data using minimum spanning tree. Abdulaziz B.M.Hame and Ibrahim O.A. Albudaw [5] presented an encryption and decryption process using modulo 27. Intended from the above references, we used plain and cycle graph to encrypt and decrypt the message.

Let us take an undirected plain graph G(A)=(V,E) associated with vertices V and edges E. An unique way of moving from one vertex to another vertex without repetition of vertex is called path. An undirected movement starts from one vertex and return back to the same vertex, is called closed path. Closed path otherwise called cycle graph. Let us consider a plain graph with five vertices and seven edges graph.

Graph can be represented using adjacency list and adjacency matrix. The adjacency list is a group of hierarchical list of confined graphs. The adjacency matrix is a symmetric matrix of elements representing the combination of edges to a vertex $|v| \otimes |v|$. A graph with a particular marking is called graph labeling. A graph labeling is of two kinds, vertex labeling and edge labeling. The edge magic total is the sum of distance between the edges. This type of labeled graph is also called a weighted graph. In this work we define a problem of longest closed path which forms a cycle graph.

Cryptography is a hidden way of communicating a message from a sender to the receiver. A message is given using secret key called cipher text. We can use various steps to encrypt the message.

Encryption algorithm can be classified into two classes

(1) Symmetric key
(2) Asymmetric key

Encryption and decryption of a message using the same key is called symmetric key. Encryption and decryption of a message using the distinct key is called asymmetric key. In asymmetric key one key is

known to all but another key remains secret. The way of using longest closed path has a wide industrial application.

A. ALGORITHM

- Let us consider a message as vertices in a graph.
- Each word in a message is represented as a vertex as long as all adjacent words in the message will be noted as adjacent vertices in the graph.
- Every edge has its own edge magic total by adding distance of two words in the encoding table.
- A weighted graph is obtained
- Using longest path routine we get a cycle graph
- Adjacency matrix of a graph is multiplied to the adjacency matrix of cycle graph
- The outcome matrix multiplied to the key matrix
- The end matrix is the encrypted message sent to the receiver

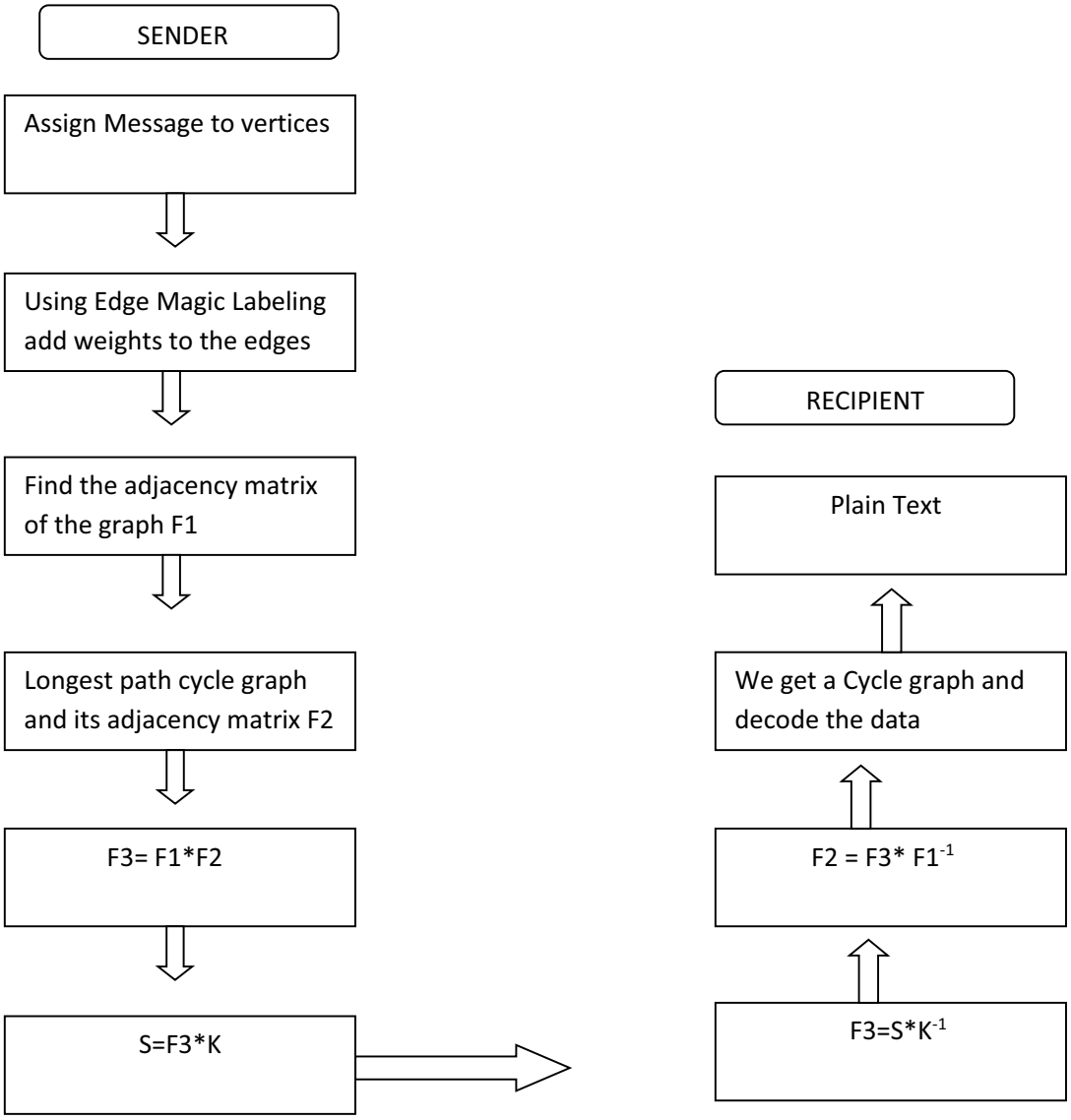
B. ENCRYPTION

- Draw the plain graph with five vertices and seven edges
- From the encoding table weight the edges, by adding the distance between the two vertices
- Using adjacency list of vertices we form adjacency matrix F1
- Find the longest cycle path in the plain graph and remove all other edges in it
- Using this cycle graph find the adjacency matrix F2
- Modify the F2 with the order given in table II
- Multiply F1 and F2 to get F3
- Multiply F3 with a pre- defined common key to form S
- Then we get encrypted text

C. DECRYPTION

- The encrypted message received by the recipient
- The receiver calculates F3 by using the inverse form of the common key S^{-1}
- Then calculate F2 by using the inverse form of F1
- We get a original message by decrypting F1 using the encoding table II

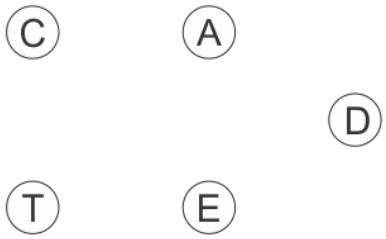
D. STRUCTURE OF ENCRYPTION AND DECRYPTION



2. ILLUSTRATION WITH EXAMPLE

A message CADET is encrypted by the sender to send it to recipient.

Label each word in message to vertex and connect the edges to form a plain graph

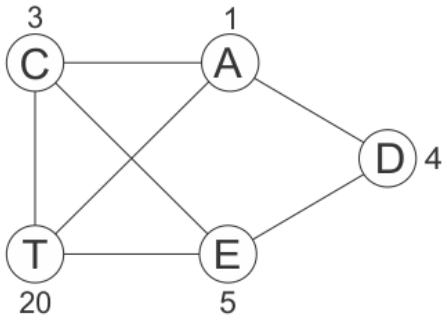


Then weight each edge by **Table 1**.

1	2	3	4	5	6	7	8	9		10	11	12	13
A	B	C	D	E	F	G	H	I		J	K	L	M

14	15	16	17	18	19	20	21	22	23	24	25	26
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Now evaluate the distance between edges using the table I



Distance = code (C) + code (A)

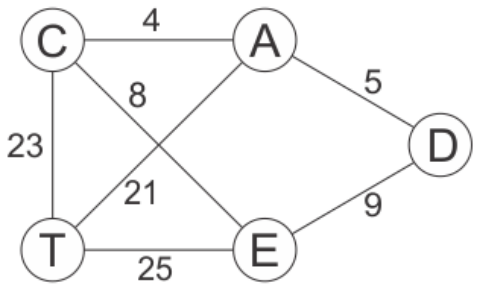
W1 =3+1=4

W2 =1+4=5

W3 =4+5=9

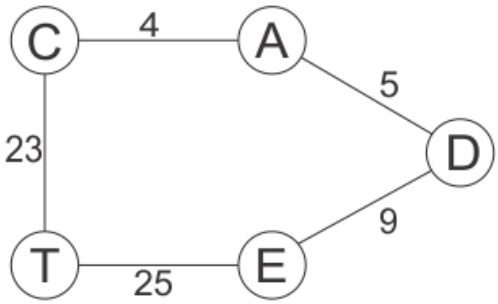
W4 =5+20=25

W5 =20+3=23



$$F1 = \begin{bmatrix} 0 & 4 & 0 & 8 & 0 \\ 0 & 0 & 5 & 0 & 21 \\ 0 & 0 & 0 & 9 & 0 \\ 8 & 0 & 0 & 0 & 25 \\ 23 & 21 & 0 & 0 & 0 \end{bmatrix}$$

Then we find a longest path in the graph



$$F2 = \begin{bmatrix} 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 5 & 0 & 0 \\ 0 & 0 & 0 & 9 & 0 \\ 0 & 0 & 0 & 0 & 25 \\ 23 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Now we replace order of corresponding words in the diagonal

Table 2: corresponding

Message	C	A	D	E	T
Order	0	1	2	3	4

We get a reformed adjacency matrix of F2 by replacing C·C = 0, A·A = 1, D·D = 2, E·E = 3, T·T = 4 in the adjacency matrix.

$$F2 = \begin{bmatrix} 0 & 4 & 0 & 0 & 0 \\ 0 & 1 & 5 & 0 & 0 \\ 0 & 0 & 2 & 9 & 0 \\ 0 & 0 & 0 & 3 & 25 \\ 23 & 0 & 0 & 0 & 4 \end{bmatrix}$$

Multiply the matrix F1 by F2 to get F3

$$F3 = F1*F2 = \begin{bmatrix} 0 & 4 & 20 & 24 & 200 \\ 483 & 0 & 10 & 45 & 84 \\ 0 & 0 & 0 & 27 & 225 \\ 575 & 32 & 0 & 0 & 100 \\ 0 & 113 & 105 & 0 & 0 \end{bmatrix}$$

Now use a common key K to encrypt F2

Let K = $\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$ we get a encrypted message by multiplying K*F3

Encrypt message is S = $\begin{bmatrix} 0 & 4 & 24 & 48 & 248 \\ 483 & 483 & 493 & 538 & 622 \\ 0 & 0 & 0 & 27 & 252 \\ 575 & 607 & 607 & 607 & 607 \\ 0 & 113 & 218 & 218 & 218 \end{bmatrix}$

In the recipient side, we get F3 by multiplying the encrypt message with inverse form of common of K^{-1}

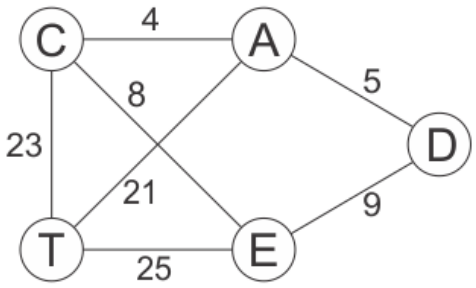
$$F3 = S\,K^{-1} = \begin{bmatrix} 0 & 4 & 24 & 48 & 248 \\ 483 & 483 & 493 & 538 & 622 \\ 0 & 0 & 0 & 27 & 252 \\ 575 & 607 & 607 & 607 & 607 \\ 0 & 113 & 218 & 218 & 218 \end{bmatrix} * \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$F3 = \begin{bmatrix} 0 & 4 & 20 & 24 & 200 \\ 483 & 0 & 10 & 45 & 84 \\ 0 & 0 & 0 & 27 & 225 \\ 575 & 32 & 0 & 0 & 100 \\ 0 & 113 & 105 & 0 & 0 \end{bmatrix}$$

Then calculate F2 by multiplying F3 by $F1^{-1}$

$$F2 = F3 * F1^{-1} = \begin{bmatrix} 0 & 4 & 0 & 0 & 0 \\ 0 & 0 & 5 & 0 & 0 \\ 0 & 0 & 0 & 9 & 0 \\ 0 & 0 & 0 & 0 & 25 \\ 23 & 0 & 0 & 0 & 0 \end{bmatrix}$$

F2 gives the final graph which is a graph originally defined at the beginning.



3. CONCLUSION

In this paper, we use a particular graph with five vertices and seven edges and a new algorithm is defined. The encryption of message is done using encoding table and graph theory properties of longest closed path. Then we use a shared key concept, which is predefined and known by sender as well as receiver. Then we use common key cryptography system to break the unrevealed message.

More progression can be done in future relevant to increase or decrease the matrices suitable to reveal the message.

4. APPLICATIONS

The longest path is the critical path in a graph. Longest path are used in project planning and scheduling. Next, enumeration of longest path also can be used to find hamiltonian paths and related problem to the Travelling Salesman problem. Many such problems have applications in vehicle routing and Complicated scheduling problems . Longest path finding is useful in calculating Non deterministic Problem. NP- Problem has a wide application in creating games like Super Mario Bros, Number link, Nonograms, Lemmings and Same Game.

NP-problem leads to some special type of problem like edge dominating set problem in line graphs, connected dominating set problem and the maximum leaf spanning tree problem.

5. REFERENCE

[1]. P.Femina, D.Antony David, A Study of Data Encryption Standard using Graph Theory.ICSTM 978-81-931039-6-8.
[2]. Weal Mahmoud Al Etaiwi, Encryption Algorithm using Graph Theory. JSRR.2014.19.004.
[3]. V.A.Ustimenko, On Graph based Crytography and symbolic computations. Serica J. Computing 1 (2007), 131-156.
[4]. B.Vellaikannan, Dr.V.Mohan, V.Gnanaraj, A note on the Applications of Quadratic forms in coding theory with a note on Security. Int. J. Comp. Tech. Appl. Vol 1 (1), 78-87.
[5]. Abdulaziz B.M.Hame and Ibrahim O.A. Albudaw, Encrypt and Decrypt messages using Invertible matrices. AJER e-ISSN- 2320-0847 p-ISSN-2320-0936, Vol-6,ISSU-6, pp- 217-217.
[6]. https://core.ac.uk/download/pdf/62657982.pdf
[7]. http://math.nsc.ru/conference/g2/g2c2/TokarevaN.pdf
[8]. http://data.conferenceworld.in/ICSTM2/P1928-1938.pdf
[9]. http://mathworld.wolfram.com/KnightGraph.html.