Encoding And Decoding Process Using Prime Graceful Labeling

[1] M. V. Nayana, [2] K. R. Sobha

[1] Research Scholar, Reg.No.21213182092001,
Sree Ayyappa College for Women, Chunkankadai, Nagercoil-629003, TamilNadu, India.
[2]Assistant Professor, Department of Mathematics, Sree Ayyappa College for Women,
Chunkankadai, Nagercoil-629003.
[Affiliated to Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli-627012,
TamilNadu,India.]
E-mail: [1] nayanamv98@gmail.com, [2] vijayakumar.sobha9@gmail.com

Abstract: In this paper, an interesting application of Prime graceful labeling in the field of coding theory is examined. Here, a new algorithm for encoding and decoding blended with prime graceful labeling is constructed and an interpretation for the proposed algorithm is also presented.

Keywords: Prime graceful labeling, Encoding, Cipher text, Decoding.
2010 Mathematics Subject Classification: 05C78, 94A60.

1. Introduction

Graph Labeling was first introduced by Rosa.A in 1967[5]. Graph labeling has various applications and one among them is Cryptography. It is the study of secured communication techniques that allows only the sender and intended recipient of a message to view its contents.

While transmitting electronic data, the most common use of cryptography is to encode and decode email and other plain text messages. The simplest method uses the symmetric or “secret key” system. Here data is encrypted using a secret key, and then both the encoded message and secret key are sent to the recipient for decryption, If the message is intercepted, a third party has everything they need to decrypt and read the message.

To address this issue, cryptologists devised the asymmetric or “public key” system. Here every user has two keys namely one public and one private. Senders request the public key of their intended recipient, encrypt the message and send it along. When the message arrives, only the recipient’s private key will decode it. Thus theft is of no use without the corresponding private 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 method of using longest closed path has a wide industrial application.

Wael Mahmoud Al Etaiwi conferred an encryption algorithm using minimum spanning tree[11]. Here data is encrypted using spanning tree and decrypted using minimum spanning tree. From the above reference studied, here we use a plain, cycle graph to encrypt and decrypt the message.

2. Preliminaries

Definition 1:[6]

A prime graceful labeling of a graph $G = (V,E)$ with n vertices and m edges is a one-to-one mapping ψ of the vertex set $V(G)$ into the set $\{ 1,2, \dots ,m+1\}$ with the following property: for any edge $e = \{u,v\} \in E(G)$, the value gcd($\psi(u)$, $\psi(v)$) = 1 and the induced function $\psi^* : E(G) \to \{ 1,2, \dots ,m\}$, defined as $\psi^* (e) = | \psi(u) - \psi(v)|$, is injective. A graph is called prime graceful if it has a prime graceful labeling.

Definition 2:[3]

The original secret text from the sender to the receiver which requires to be transformed into some version is called Plaintext.

Definition 3: [3] The required version of our Plaintext is called Ciphertext.
Definition 4: [3] The process of transforming Plaintext to Ciphertext is called Encryption.
Definition 5: [3] The transformation of Ciphertext to Plaintext is termed as Decryption.
Definition 6: [3] The essential tool that encodes the Plaintext and also decodes the Cipher text is called Key.

3. Main Results

Encryption Algorithm:

- Let us consider a message as vertices in a graph.
- Denote each character in a message as a vertex
- All adjacent characters in the message will be named as adjacent vertices in the graph.
- Here assign weights for each vertex using encoding table and join using an edge.
- Every edge of a prime graceful graph thus obtained, has its own weight by subtracting the weights of both end vertices using the encoding table.
- A weighted graph G is thus obtained.
- Compute the adjacency matrix M_1 from G.
- Determine the minimum spanning tree.
- Find adjacency matrix M_2 from minimum spanning tree.
- Determine $M_3 = M_1 \times M_2$.
- Fix Key Matrix K.
- Cipher text $C = M_3 \times K$.

Decryption Algorithm:

- The encrypted message received by the recipient.
- Calculate M_3 by using the inverse form of the common key K^{-1}.
- Then calculate M_2 by using the inverse form of M_1.
- Decrypt M_1 using the encoding table and thus we get the original message.

Illustration

Here we come up with two different shared key matrices such as upper triangular matrix and lower triangular matrix in type I and type II for a word “UKRAINE” framed in a prime graceful graph.
Let the message considered here is “UKRAINE” which is to be send to the recipient. Each character in the message is denoted as vertex and the adjacent characters are joined by an edge which forms a graph.

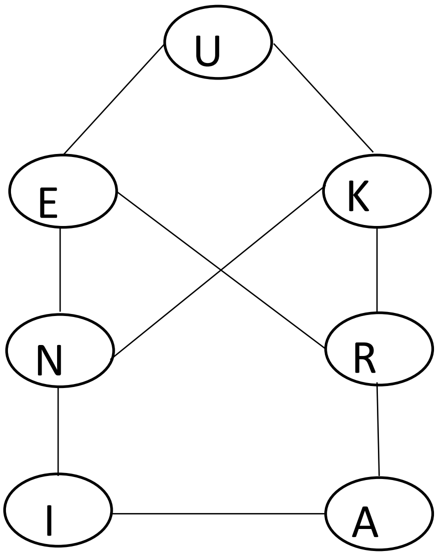

Fig 1: Plain graph with text characters

The encoding table is given below:

Table 1: Encoding Table

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

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

Each vertex is labeled using the encoding table and each edge weight is obtained from the difference of the adjacent vertices.

Thus we obtain a weighted graph *G* where all the vertex, edge labels are distinct and the gcd of any two adjacent vertices is 1. Hence this graph satisfies the condition of prime graceful labeling and is a prime graceful graph.

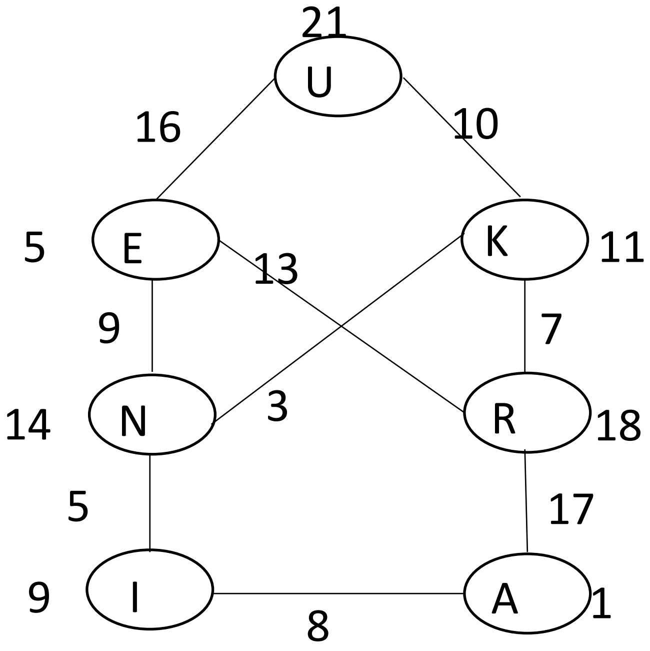

Fig 2: Weighted Graph *G*

$$\text{Matrix } M_1 = \begin{bmatrix} 0 & 10 & 0 & 0 & 0 & 0 & 16 \\ 10 & 0 & 7 & 0 & 0 & 3 & 0 \\ 0 & 7 & 0 & 17 & 0 & 0 & 13 \\ 0 & 0 & 17 & 0 & 8 & 0 & 0 \\ 0 & 0 & 0 & 8 & 0 & 5 & 0 \\ 0 & 3 & 0 & 0 & 5 & 0 & 9 \\ 16 & 0 & 13 & 0 & 0 & 9 & 0 \end{bmatrix}$$

Then we determine a longest path in *G*. Let the matrix be M_2.

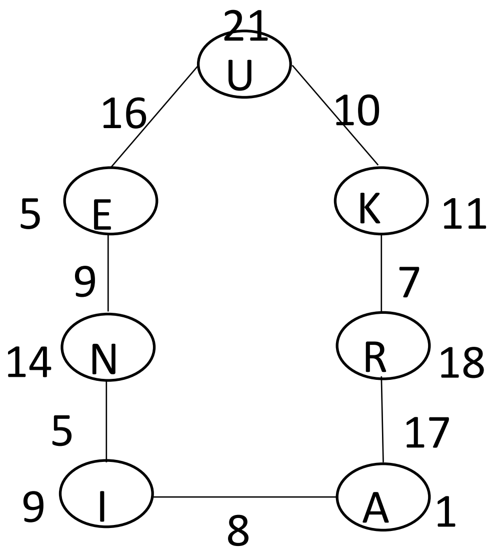

Fig 3: Longest path of G

$$M_2 = \begin{bmatrix} 0 & 10 & 0 & 0 & 0 & 0 & 16 \\ 10 & 0 & 7 & 0 & 0 & 0 & 0 \\ 0 & 7 & 0 & 17 & 0 & 0 & 0 \\ 0 & 0 & 17 & 0 & 8 & 0 & 0 \\ 0 & 0 & 0 & 8 & 0 & 5 & 0 \\ 0 & 0 & 0 & 0 & 5 & 0 & 9 \\ 16 & 0 & 0 & 0 & 0 & 9 & 0 \end{bmatrix}$$

In matrix M_2 we replace the corresponding characters in the diagonal from the table below.

Character	U	K	R	A	I	N	E
Order	1	2	3	4	5	6	7

$$\text{Thus } M_2 = \begin{bmatrix} 1 & 10 & 0 & 0 & 0 & 0 & 16 \\ 10 & 2 & 7 & 0 & 0 & 0 & 0 \\ 0 & 7 & 3 & 17 & 0 & 0 & 0 \\ 0 & 0 & 17 & 4 & 8 & 0 & 0 \\ 0 & 0 & 0 & 8 & 5 & 5 & 0 \\ 0 & 0 & 0 & 0 & 5 & 6 & 9 \\ 16 & 0 & 0 & 0 & 0 & 9 & 7 \end{bmatrix}$$

To get M_3 multiply M_1 with M_2.

$$M_3 = M_1 \times M_2 = \begin{bmatrix} 0 & 10 & 0 & 0 & 0 & 0 & 16 \\ 10 & 0 & 7 & 0 & 0 & 3 & 0 \\ 0 & 7 & 0 & 17 & 0 & 0 & 13 \\ 0 & 0 & 17 & 0 & 8 & 0 & 0 \\ 0 & 0 & 0 & 8 & 0 & 5 & 0 \\ 0 & 3 & 0 & 0 & 5 & 0 & 9 \\ 16 & 0 & 13 & 0 & 0 & 9 & 0 \end{bmatrix} \times \begin{bmatrix} 1 & 10 & 0 & 0 & 0 & 0 & 16 \\ 10 & 2 & 7 & 0 & 0 & 0 & 0 \\ 0 & 7 & 3 & 17 & 0 & 0 & 0 \\ 0 & 0 & 17 & 4 & 8 & 0 & 0 \\ 0 & 0 & 0 & 8 & 5 & 5 & 0 \\ 0 & 0 & 0 & 0 & 5 & 6 & 9 \\ 16 & 0 & 0 & 0 & 0 & 9 & 7 \end{bmatrix}$$

$$M_3 = \begin{bmatrix} 356 & 20 & 70 & 0 & 0 & 144 & 112 \\ 10 & 149 & 21 & 119 & 15 & 18 & 187 \\ 278 & 14 & 338 & 68 & 136 & 117 & 91 \\ 0 & 119 & 51 & 353 & 40 & 40 & 0 \\ 0 & 0 & 136 & 32 & 89 & 30 & 45 \\ 174 & 6 & 21 & 40 & 25 & 106 & 63 \\ 16 & 251 & 39 & 221 & 45 & 54 & 337 \end{bmatrix}$$

A shared key K is fixed to encrypt M_3.

Here we use two types of keys namely upper triangular matrix in type I and lower triangular matrix in type II.

Type I:

Encryption: Let the shared key K be upper triangular matrix to encrypt M_3.

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

Let C be the Cipher text. Then $C = M_3 \times K$.

$$C = M_3 \times K = \begin{bmatrix} 356 & 376 & 446 & 446 & 446 & 590 & 702 \\ 10 & 159 & 180 & 299 & 314 & 332 & 519 \\ 278 & 292 & 630 & 698 & 834 & 951 & 1042 \\ 0 & 119 & 170 & 523 & 563 & 603 & 603 \\ 0 & 0 & 136 & 168 & 257 & 287 & 332 \\ 174 & 180 & 201 & 241 & 266 & 372 & 435 \\ 16 & 267 & 306 & 527 & 572 & 626 & 963 \end{bmatrix}$$

The data to be sent is taken as $C + M_1$ for more secured transmission of data.

Decryption:

Now we decrypt the cipher text into plain text.

$$M_3 = C \times K^{-1} = \begin{bmatrix} 356 & 20 & 70 & 0 & 0 & 144 & 112 \\ 10 & 149 & 21 & 119 & 15 & 18 & 187 \\ 278 & 14 & 338 & 68 & 136 & 117 & 91 \\ 0 & 119 & 51 & 353 & 40 & 40 & 0 \\ 0 & 0 & 136 & 32 & 89 & 30 & 45 \\ 174 & 6 & 21 & 40 & 25 & 106 & 63 \\ 16 & 251 & 39 & 221 & 45 & 54 & 337 \end{bmatrix}$$

To find M_2, we have $M_2 = M_1^{-1} \times M_3$.

$$M_2 = \begin{bmatrix} 1 & 10 & 0 & 0 & 0 & 0 & 16 \\ 10 & 2 & 7 & 0 & 0 & 0 & 0 \\ 0 & 7 & 3 & 17 & 0 & 0 & 0 \\ 0 & 0 & 17 & 4 & 8 & 0 & 0 \\ 0 & 0 & 0 & 8 & 5 & 5 & 0 \\ 0 & 0 & 0 & 0 & 5 & 6 & 9 \\ 16 & 0 & 0 & 0 & 0 & 9 & 7 \end{bmatrix}$$

Type II:

Encryption: Here let M_1, M_2, M_3 be the same matrices taken as in type I.

Here the shared key K be lower triangular matrix to encrypt M_3.

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

Let Cipher text C be $C = M_3 \times K$.

$$C = M_3 \times K = \begin{bmatrix} 702 & 346 & 326 & 256 & 256 & 256 & 112 \\ 519 & 509 & 360 & 339 & 220 & 205 & 187 \\ 1042 & 764 & 750 & 412 & 344 & 208 & 91 \\ 603 & 603 & 484 & 433 & 80 & 40 & 0 \\ 332 & 332 & 332 & 196 & 164 & 75 & 45 \\ 435 & 261 & 255 & 234 & 194 & 169 & 63 \\ 963 & 947 & 696 & 657 & 436 & 391 & 337 \end{bmatrix}$$

The data to be sent is taken as $C + M_1$ for more secured transmission of data.

Decryption:

Now we decrypt the cipher text into plain text.

$$M_3 = C \times K^{-1} = \begin{bmatrix} 356 & 20 & 70 & 0 & 0 & 144 & 112 \\ 10 & 149 & 21 & 119 & 15 & 18 & 187 \\ 278 & 14 & 338 & 68 & 136 & 117 & 91 \\ 0 & 119 & 51 & 353 & 40 & 40 & 0 \\ 0 & 0 & 136 & 32 & 89 & 30 & 45 \\ 174 & 6 & 21 & 40 & 25 & 106 & 63 \\ 16 & 251 & 39 & 221 & 45 & 54 & 337 \end{bmatrix}$$

$$M_2 = M_1^{-1} \times M_3 = \begin{bmatrix} 1 & 10 & 0 & 0 & 0 & 0 & 16 \\ 10 & 2 & 7 & 0 & 0 & 0 & 0 \\ 0 & 7 & 3 & 17 & 0 & 0 & 0 \\ 0 & 0 & 17 & 4 & 8 & 0 & 0 \\ 0 & 0 & 0 & 8 & 5 & 5 & 0 \\ 0 & 0 & 0 & 0 & 5 & 6 & 9 \\ 16 & 0 & 0 & 0 & 0 & 9 & 7 \end{bmatrix}$$

Thus both in type I and type II, M_2 represents the following final graph that we use to retrieve the original message.

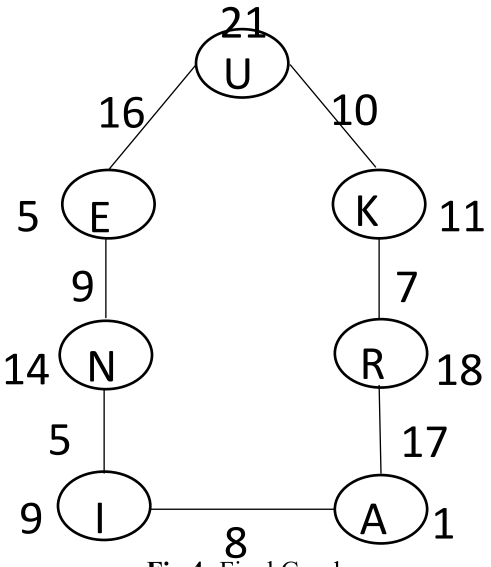

Fig 4: Final Graph

4. Conclusion

In this paper, we use a particular graph with 7 vertices and 9 edges. The encryption of a message is done using encoding table and graph theory properties of longest closed path. Here we have proposed an algorithm using two different types of keys for encryption and decryption of cipher text. Cryptography is used in everyday life for the purpose of Authentication/ Digital signatures, Time stamping, Electronic money, Encryption/ Decryption in e-mail, Encryption in whatsapp, Instagram, Sim card authentication, etc.

5. References:

[1] Bondy JA and Murthy USR, Graph Theory with Applications, Macmillan, London, 1979.

[2] Frank Harary , Graph Theory , Narosa Publishing House.

[3] Jaya Shruthy.V.N, V.Maheswari, " Double encryption and Decryption Process using Graph Labelling through Enhanced Vigenere Cipher", Journal of Physics: Conference Series, 1362(2019), Pg.No: 1-7.

[4] Joseph A. Gallian, "A Dynamic Survey of Graph Labeling", The Electronic Journal of Combinatorics (2021), #DS6.

[5] Rosa A, "On certain valuations of the vertices of a graph", Theory of Graphs(International Symposium, Rome, July(1966), Gordon and Breach: (1967), pp.349-355.

[6] Sayan Panma, Penying Rochanakul, "Prime-Graceful Graphs", Thai Journal of Mathematics, Vol.19, No.4,(2021), pp.1685-1697.

[7] Sedlack.J, "Theory of Graphs and its Applications", Smolenice Symposium (Prague,1964), 163-164.

[8] T.M. Selvarajan, R. Subramoniam, "Prime Graceful Labeling", International Journal of Engineering and Technology,7 (4.36) (2018) 750-752 .

[9] Tout R, Dabboucy AN and Howalla K, "Prime Labeling of Graphs", National Academy Science Letters-India, Vol.5, No.11,(1982), pp.307-370.

[10] Uma R and Murugesan N, Graceful Labeling of some graphs and their subgraphs, Asian Journal of Current Engineering and Maths, Vol.1, No.6,(2013), pp. 367-370.

[11] 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.