Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 5, pp. 1355–1365
DOI : 10.47974/JDMSC-1752

Encryption and decryption of a word into weighted graph using super-edge anti-magic total labeling of Bi-star graph

R. Jegan *
Department of Mathematics
GIET University
Gunupur
Odisha 765 022
India

and

Panimalar Engineering College
Chennai
Tamilnadu 600123
India

P. Vijayakumar †
Department of Mathematics
GIET University
Gunupur 765022
Odisha
India

V. D. Ambethkumar §
Department of Computer Engineering
Mizoram University
Aizwal 796004
Mizoram
India

Pa Vijay ‡
Department of Artificial Intelligence and Data Science
Panimalar Engineering College
Chennai 600123
Tamil Nadu
India

* *E-mail:* **rjch12571@gmail.com (Corresponding Author)**
† *E-mail:* **vijaykumar@giet.edu**
§ *E-mail:* **dr.vdambethkumar@gmail.com**
‡ *E-mail:* **vijayparthiban28092002@gmail.com**

Edeh Michael Onyema [@]
Department of Mathematics and Computer Science
Mathematics and Computer Science
Coal City University
Enugu
Nigeria

Abstract

Graph labeling is an important topic in Graph theory, a branch of Mathematics, having applications in the field of Networks, radio astronomy and cryptography etc. In most of encryption algorithms, words are encrypted as words. But our implementation is based on the algorithm that encrypts words into numbers, with the help of an edge weighted graph. Mapping of certain positive integers to graph elements in such a way that weights of all edges computed as, sum of the labels of all graph elements, are distinct is termed as Antimagic labeling In this paper, we present an algorithm that encrypts words into edge weighted graphs using super-edge antimagic total labeling of Bi-star graph and illustrate with an example.

Subject Classification: *68M25, 05C22.*

Keywords: *Super-edge antimagic labeling, Weighted graph, Encryption, decryption, Bi-star graph, RSA algorithm.*

1. Introduction

Cryptography, play an important role in secured message transmission. Several algorithms were developed for encryption and decryption over the period of time. In this research paper, we are using the conceptual implementation of one of the leading cryptographic algorithms, RSA algorithm that uses two different keys for encryption and decryption namely public key and private key. Various technical advancements are taking place in the field of cryptography, wherein through this research we are about to enhance its security by embedding a edge weighted graph using super-edge antimagic total labeling where the sum of the weights of all edges are distinct. We are about represent the Bi-star graph through the matrix where the matrix elements are the weights of the edges of the Bi-star graph. We are also going to discuss the implementation, merits and demerits of our research.

[@] *E-mail:* **michael.edeh@ccu.edu.ng**

2. Literature Survey

Let us discuss several techniques adopted by various authors through this survey.

P. Amudha, et. al. [1] discussed a new algorithmic technique that involves encoding and decoding the message using the graph labeling much securely. It has provide an overview of basic technique on public key and private key utilization. Aiden A. Bruen, et. al. [2], have collectively discussed some procedures in the modernday cryptography.

Adesh Kumari, et. al. have[3] proposed an advanced authentication framework for two users. It also shows analysis on the security and shows comparisons with other algorithms realted to it. Sampathkumar[4] through this paper investigates various classes of graphs especially with duplicate graphs. It also gives an interpretation on pen-labeling. P K Dewi, et. al. [5] have discussed on super edge-antimagic labeling which is a simple graph obtained by introducing a twist in the prism graph. It also proves its summary and discusses the various properties of it.

IW Sudarsana, et. al. [6] discuss on various graphs like super mean draphs and magic graphs and on the ways to increase the security levels of Affine Cipher to encrypt a text. Similar to this, Wael Mohammed Al Etaiwi [7] gave a new encryption algorithm for encryption and decryption of data securely to generate a complex cipher text using shared key. YahiaAlemami, et. al. [8], presented a research on various techniques based on cryptography for encryption and decryption and their algorithms. Baizhu Ni, et. al. [9] proposed some new encryption algorithms using corona graphs and bipartite graphs.

Willaim Stallings [10] through his paper gave his insights on the Cryptography principles and security of the networks based on his publishing.

3. Proposed System

Our proposed method involves conversion of the text that is given as an input into a edge weighted matrix which is the representation of the Bi-star graph in the matrix form. It is more beneficial as we have used the concept of Anti-magic labeling where every edge weight is unique. Then like other traditional methods the encrypted matrix is decrypted to give the word that was meant to be transmitted. We use RSA algorithm to encrypt and decrypt the matrices by utilizing the public and private keys. The mapping of the encrypted graph to a bi-star graph is shown in Figure 1.

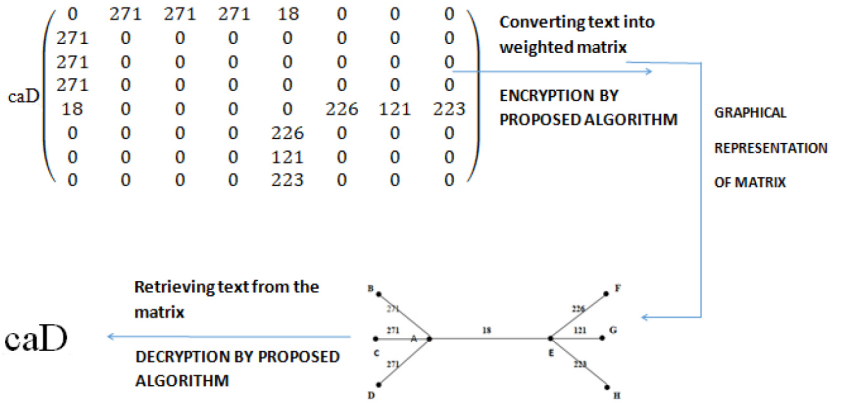

Figure 1

Encryption implementation

3.1 *An Algorithm that labels the bi-star graph with super-edge anti-magic labeling*

Bi-star graph $B_{n,n}$ has $2n+2$ vertices and $2n+1$ edges with two apex vertices v_1, v_{n+2} and pendant vertices $v_2, v_3, \ldots, v_n$ each of which is adjacent to v_1 and pendant vertices $v_{n+3}, v_{n+4}, \ldots, v_{2n+2}$ each of which is adjacent to v_{n+2}. Vertices and edges are labeled as follows:

$$f(v_i) = i, i = 1 \text{ to } 2n+2 \; f(v_1 v_i) = 2n+1+i, i = 2 \text{ ton}$$
$$+2 f(v_{n+2} v_i) = 2n+1+i, i = n+3 \text{ to } 2n+2 \quad (1)$$

For this labeling the weights are computed as

$$wt(v_1 v_i) = 2n+2+2i, i = 2 \text{ton} + 2wt(v_{n+2} v_i) = 3n+3+2i, \; i = n+3 \text{ to } 2n+2 \quad (2)$$

It is obvious to conclude that the weights of all the edges are distinct and hence the above labeling is a super-edge anti-magiclabeling of bi-star graph.

3.2 *Algorithm for Encryption*

1. Read the word ω and find its length 'n'
2. Assign alphabetical order $A_i(\omega)$ for characters / alphabets as follows

$c_i(\omega)$	a	b	…	z	A	B	….	Z
$P_i(\omega)$	2	3	…	27	29	30	….	54

For $i = 2\,\text{ton} + 1$

$$A_i(\omega) = \begin{cases} P_i(\omega), \text{if } (i-1)^{th} \text{character of the word } \omega i \text{ sin lowercase} \\ 0, \text{otherwise} \end{cases} \tag{3}$$

For $i = n+3 \text{ to } 2n+2$

$$A_i(\omega) = \begin{cases} P_{i-n-2}(\omega), \text{if}(i-n-2)^{th} \text{character of the word } \omega i \text{ sin uppercase} \\ 0, \text{ otherwise} \end{cases} \tag{4}$$

3. Form a matrix with $2n+2$ rows and $2n+2$ columns with adjacency matrix

$$a_{ij} = \begin{cases} 1, \text{for} \begin{matrix} i=1, j=2\,\text{ton}+2 \\ i=2\,\text{ton}+2, j=1 \\ i=n+2, j=n+3 \text{ to } 2n+2 \\ i=n+3 \text{ to } 2n+2, j=n+2 \end{matrix} \\ 0, \text{otherwise} \end{cases} \tag{5}$$

4. Associated weights of the edges of above bi-star graph are taken as

$$w_{ij} = 0, \text{if } a_{ij} = 0$$

If $a_{ij} = 1$,

$$w_{ij} = \begin{cases} 2n+2+2j, \text{for } i=1, j=2\,\text{ton}+2 \\ 2n+2+2i, \text{for } i=2\,\text{ton}+2, j=1 \\ 3n+3+2j, \text{for } i=n+2, j=n+3 \text{ to } 2n+2 \\ 3n+3+2i, \text{for } i=n+3 \text{ to } 2n+2, j=n+2 \end{cases} \tag{6}$$

5. Encoded edge weighted matrix is :

$$e_{ij} = \begin{cases} w_{ij} + A_j(\omega), \text{for } i=1, j=2\,\text{ton}+2 \\ w_{ij} + A_i(\omega), \text{for } j=1, i=2\,\text{ton}+2 \\ w_{ij} + A_j(\omega), \text{for } i=n+2, j=n+3 \text{ to } 2n+2 \\ w_{ij} + A_i(\omega), \text{for } j=n+2, i=n+3 \text{ to } 2n+2 \end{cases} \tag{7}$$

6. For each of these e_{ij} calculate encryption $e'_{ij} = e_{ij}^{e} \bmod (N)$ where e, N are generated using RSA algorithm. This edge weighted matrix represents edge-weighted graph.

3.3 *Algorithm for Decryption*

1. Consider the encrypted graph with edge weighted matrix e_{ij} of order $2n+2$
2. Decrypted matrix d'_{ij} is given by

$$d'_{ij} = e'^{d}_{ij} \pmod{N} \tag{8}$$

where d is the private key generated by RSA algorithm

3. Edge weighted matrix is retrieved using

$$d_{ij} = d'_{ij} - w_{ij} \tag{9}$$

4. For $i=1, j=1 \text{ ton} +1$ and $i=n+2,\ j=n+3$ to $2n+2$ set

$$P_{|j-i|}(\omega) = d_{ij} \text{ and } c_{|i-j|}(\omega) \tag{10}$$

is the character corresponding to the number

$$P_{|i-j|}(\omega) \text{ and } \omega = c_1 c_2 \ldots c_n \tag{11}$$

is the word.

3.4 *Illustration*

Encryption Illustration

Let us take $w = caD$ as the word to be encrypted.

1. It is of length $n = 3$.

Here, $c_1(\omega) = cc_2(\omega) = ac_3(\omega) = D$

$c_i(\omega)$	a	b	…	z	A	B	….	Z
$P_i(\omega)$	2	3	…	27	29	30	….	54

2. $P_1(\omega) = 4P_2(\omega) = 2P_3(\omega) = 32$
$A_2(\omega) = 4A_3(\omega) = 2A_4(\omega) = 0\, A_6(\omega) = 0\, A_7(\omega) = 0\, A_8(\omega) = 32$

3. So, form a 8 × 8 adjacency matrix of bi-star graph.

$$a_{ij} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

4. Weights of the edges of the above graph are :

$$w_{ij} = \begin{pmatrix} 0 & 12 & 14 & 16 & 18 & 0 & 0 & 0 \\ 12 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 14 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 16 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 18 & 0 & 0 & 0 & 0 & 24 & 26 & 28 \\ 0 & 0 & 0 & 0 & 24 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 26 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 28 & 0 & 0 & 0 \end{pmatrix}$$

$$e_{ij} = \begin{pmatrix} 0 & 16 & 16 & 16 & 18 & 0 & 0 & 0 \\ 16 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 16 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 16 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 18 & 0 & 0 & 0 & 0 & 24 & 26 & 60 \\ 0 & 0 & 0 & 0 & 24 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 26 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 60 & 0 & 0 & 0 \end{pmatrix}$$

4. The entries of the matrices are encrypted using RSA algorithm by selecting prime numbers 17,19 (one need to sufficiently large prime numbers but for manual calculation we selected these numbers)

$$N = 17 * 19 = 288 M = 16 * 18 = 323 e = 31$$

$$\Rightarrow \qquad As 31 * 223 \equiv 1 (\text{mod}\, 288) d = 223$$

and resultant encrypted matrix is

$$e'_{ij} = \begin{pmatrix} 0 & 271 & 271 & 271 & 18 & 0 & 0 & 0 \\ 271 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 271 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 271 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 18 & 0 & 0 & 0 & 0 & 226 & 121 & 223 \\ 0 & 0 & 0 & 0 & 226 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 121 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 223 & 0 & 0 & 0 \end{pmatrix}$$

The encrypted Bi-star graph which is represented as the above matrix e_{ij} is

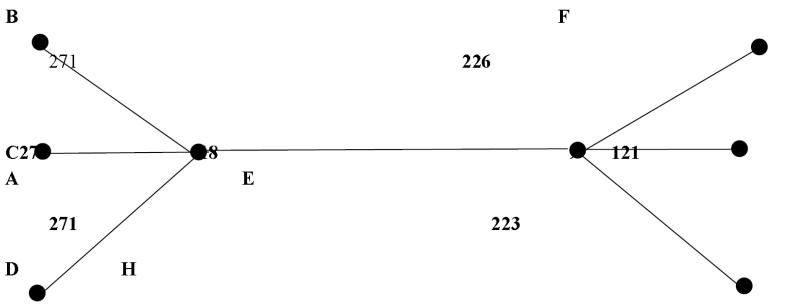

Figure 2

Bi-star graph representation of the matrix

Decryption Illustration

1. In order to decrypt, the encoded matrix is given as input

$$e'_{ij} = \begin{pmatrix} 0 & 271 & 271 & 271 & 18 & 0 & 0 & 0 \\ 271 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 271 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 271 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 18 & 0 & 0 & 0 & 0 & 226 & 121 & 223 \\ 0 & 0 & 0 & 0 & 226 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 121 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 223 & 0 & 0 & 0 \end{pmatrix}$$

2. Decrypt the entries of the above matrix with private key d = 103 which is also given as input.

   The resultant decrypted matrix is :

$$d'_{ij} = \begin{pmatrix} 0 & 16 & 16 & 16 & 18 & 0 & 0 & 0 \\ 16 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 16 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 16 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 18 & 0 & 0 & 0 & 0 & 24 & 26 & 60 \\ 0 & 0 & 0 & 0 & 24 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 26 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 60 & 0 & 0 & 0 \end{pmatrix}$$

3. The below mentioned Edge weighted matrix is retrieved by using $d_{ij} = d'_{ij} - w_{ij}$ (w_{ij} is as same as the matrix in encryption program)

$$d_{ij} = \begin{pmatrix} 0 & 4 & 2 & 0 & 0 & 0 & 0 & 0 \\ 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 32 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 32 & 0 & 0 \end{pmatrix}$$

5. For $i = 1, j = 1 \text{ton} + 1$ and $i = n + 2,\ j = n + 3$ to $2n + 2$ set $P_{|j-i|}(\omega) = d_{ij}$ and $c_{|i-j|}(\omega)$ is the character corresponding to the number $P_{|i-j|}(\omega)$ and $\omega = c_1 c_2 \ldots c_n$ is the word.

$c_i(\omega)$	a	b	…	z	A	B	….	Z
$P_i(\omega)$	2	3	…	27	29	30	….	54

$$P_1(\omega) = 4P_2(\omega) = 4P_3(\omega) = 32$$

The characters corresponding to these numbers are :

$$c_1(\omega) = cc_2(\omega) = ac_3(\omega) = D$$

4. Research Analysis

4.1 *Performance Analysis*

The main advantage of our idea is the security enhancement which is a result of combining the implementation of RSA algorithm and our idea of representing the edge weighted graphs into the encoding matrix. Even-though it is a basic level implementation, with future updations we can surely increase the performance of this existing program. The advantages of our idea are mentioned with their explanation in **Table 1**.

Table 1

Advantages with Explanation

Advantages	Short explanation
Enhanced security	Our graphical implementation combined with RSA algorithm would enhance the security levels.
Visualizing the encoded matrix	With our graphical implementation it is possible to view the matrix as a graphical output.
Faster Encryption rate	The time taken to encrypt the data is relatively shorter when compared to existing efficient algorithms.
Simpler Execution	The concept behind this implementation is quite simple to understand and much effective in performance
Differed encryption	When a character appears in two different positions they are encrypted with different numbers

Though our main idea is to encrypt a word into matrix which is a representation of an edge weighted graph, the RSA algorithm's implementation that we use here have some drawbacks which also adds to the drawback of our idea.

The drawbacks of our idea with their explanation are mentioned in **Table 2**.

Table 2

Drawbacks with explanation

Drawback	Short explanation
Rare failures	This algorithm may fail some times, when the prime numbers given as input are not sufficiently large compared to length of the word
Slower Execution	As practical executions involve larger input values, the computation time is quite longer.
Decryption rate	The time taken for decryption is quite longer.
Range of Inputs	As it is an initial implementation, our algorithm can accept only a single word of any length (no numbers, white spaces or special characters)

5. Conclusion

Our proposed technique explains the algorithm for encoding word into a numbered matrix and decoding weighted Bi-star graph to retrieve

the original message which indirectly involves graph labeling. With the help of RSA algorithm and Anti-magic labeling, our technique assures to enhance the security levels of the existing techniques which makes it even more harder for the hackers to break into the message. Moreover in the future, instead of using RSA algorithm, we are on the go to use Eliptic Curve Cryptography (ECC) as it is more advantageous when compared to RSA algorithm.

References

[1] P.Amudha, J.Jayapriya, et. al., An Algorithmic Approach for Encryption using Graph Labeling J. Phys.: Conf. Ser, 1770 012072 (2021).

[2] Aiden A. Bruen; Mario A. Forcinito; et. al., "The Fundamentals of Modern Cryptography".

[3] Adesh Kumari,M. Yahya Abbasi,Vinod Kumar Akber Ali Khan, A secure user authentication protocol using elliptic curve cryptography, *Journal of Discrete Mathematical Sciences and Cryptography*, 22:4, 521-530.

[4] Sampathkumar. E, "On duplicate graphs", *Journal of the Indian Math*. Soc. 37, 285-293 (1973).

[5] PK Dewi et al., On super (a, d)-edge-antimagic total labeling of Möbiusladder, *Journal of Physics Conference Series*,. 1040 012019

[6] I W Sudarsana, S A Suryanto, D Lusianti and N P A P S Putri An application of super mean and magic graphs labeling on cryptography system, J. Phys.: Conf. Ser. 1763 012052, IOP Publishing, P1-18 (2020).

[7] Wael Mohammed Al Etaiwi, Encryption Algorithm Using Graph Theory, *Journal of Scientific Research and Reports*, 3(19), 2519-2527 (Jan 2014).

[8] William Stallings, "Cryptography and Network security Principles and Practices", Pearson/PHI, Seventh Edition (2017).

[9] R. Aragona, R. Civino, N. Gavioli & M. Pugliese. An authenticated key scheme over elliptic curves for topological networks, *Journal of Discrete Mathematical Sciences and Cryptography*, 25:8, 2429-2448 (2022), DOI: 10.1080/09720529.2020.1866298.

[10] Wing Loon Chee. Public key cryptography based on Moufang loops, *Journal of Discrete Mathematical Sciences and Cryptography*, 25:8, 2411-2427 (2022), DOI: 10.1080/09720529.2020.1864933.