Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 4, pp. 1215–1222
DOI : 10.47974/JDMSC-1976

Super-encryption technique of graphs via matricial approach

Triveni Domada *
Gudela Ashok †
Department of Mathematics
Andhra University TDR-HUB
Visakhapatnam 531081
Andhra Pradesh
India

S. Ashok Kumar §
D. Chaya Kumari ‡
Department of Mathematics
Gayatri Vidya Parishad College for UG & PG Courses (A)
Visakhapatnam 530017
Andhra Pradesh
India

Abstract

Graph theory is quickly becoming an important area of research due to its numerous applications in areas like cryptography, coding theory, communication networks and their security. In this paper a super-encryption method of graphs is proposed via matricial approach for maintaining confidentiality in communicating the messages with two layers of encryption by taking the first level of encryption as the incidence matrix. The message is further encrypted using Fibonacci numbers (taken in matrix form) by adding to the corresponding elements of the product of the incidence matrix of the graph and message (taken as diagonal matrix). Here the graph can be taken as private key. The matrix so formed can be treated as an adjacency matrix which in turn can be represented as a graph and will be sent to the receiver as super encrypted message. The receiver writes the adjacency matrix corresponding to the graph, then subtracts the Fibonacci matrix from adjacency matrix and

* *E-mail:* trivenidomada@gmail.com (Corresponding Author)
† *E-mail:* ashokavf@gmail.com
§ *E-mail:* saiashok.84@gmail.com
‡ *E-mail:* chayakumari.divakarla@gmail.com

then multiplies it with the inverse of incidence matrix. Finally, receiver decrypts the message using the private key shared.

Subject Classification: *Primary 11B39, 94A60 Secondary 05C07.*

Keywords: *Fibonacci matrix, Matrices, Graph Fibonacci Numbers, Cryptography.*

1. Introduction

Since ancient times, trusted parties have utilized encryption to facilitate secure communications. Throughout history, a variety of cryptosystems of varying levels of sophistication have been employed for numerous objectives. The military, maneuvers, sensitive communications between political leaders and/or monarchy, and other applications have all been significant. Researchers are particularly examining the notions of graph theory that can be applied to many aspects of cryptography [1][2] [3].

2. Definitions

Fibonacci Numbers:

Fibonacci numbers can be explained with the relation

$$F_{n+1} = F_{n-1} + F_n, F_1 = 1, F_0 = 0, n = 0, \pm 1, \pm 2, \ldots.$$

The Fibonacci sequence $\{F_n\}$ can be explained using the recursive relation

$$F_n = F_{n-2} + F_{n-1}, n \geq 2 \text{ where } F_1 = 1, F_0 = 0$$

Fibonacci Matrices:

Fibonacci numbers can be computed with the aid of the *Fibonacci matrices*

We consider 4×4 Fibonacci Matrix of the form $\begin{bmatrix} F_0 & F_1 & F_2 & F_3 \\ F_4 & F_5 & F_6 & F_7 \\ F_8 & F_9 & F_{10} & F_{11} \\ F_{12} & F_{13} & F_{14} & F_{15} \end{bmatrix}$

Plain Text: The plaintext is usually ordinary text which is readable and is converted to ciphertext with the use of encryption procedure [1][2].

Cipher Text: Ciphertext is that text which has been obtained from plaintext with the use of an encryption technique [1][2].

Symmetric key Cryptography: A secret (unique) key is used for encryption process as well as decryption process, is referred as symmetric key cryptography or symmetric encryption [1][2][3][4].

Asymmetric key Cryptography: The practice of encrypting and decrypting data using separate keys is termed as asymmetric key cryptography [1][2][3][4].

Super Encryption: Combining two or more cryptographic techniques to secure data is known as super-encryption. It is, thus, the process of adding encryption to an already encrypted message [5][6][7][8][9].

Multiple encryption: Multiple encryption involves employing either the same algorithm or a different one to encrypt a message that has already been encrypted one or more times [5][7][10][11][12].

Tree: A tree is a graph with only one path connecting any two vertices and no cycles [8][9].

Binary Tree: A tree with roots is referred to as a binary tree if each vertex's out-degree is two or less.[8][9].

Incidence Matrix: Each vertex and each edge of a directed graph are represented by a row in the incidence matrix [12].

Graph: A graph is a collection of points, known as vertices and connections between those points, known as edges [12][13].

Directed Graph: A directed graph is one that has connected vertices and all of the edges are directed from one vertex to another [12][13].

Undirected Graph: An undirected graph is a graph where the connections between the vertices were not directed. The edges in an undirected graph are also bidirectional.[12][13]

Adjacency Matrix: A finite graph is described by an adjacency matrix, which is a square matrix. The elements in it express whether or not the pairs of a finite set of vertices, also known as nodes, are adjacent in the graph. Vertex matrices are another name for adjacency matrices.[12][13]

Connected Graph: A connected graph is an undirected graph that has a path connecting each pair of its vertices.[14][15]

Disconnected Graph: Disconnected graph is one which is not connected.[14][15]

Cryptography: Studying secure communication methods which keep message secret to the sender and the intended recipient is referred as cryptography.[16][17][18]

Weighted Tree: If each leaf or edge is assigned with a real number, then the tree is known as a tree with weights.[19][20]

Optimal Tree: A variety of weighted trees can exist for a given set of weights, with the optimal tree being one of them. The optimal tree in this collection is the one with the lowest weight.[19][20]

3. Algorithms

Encryption Procedure

Step 1: Consider a graph and write its incidence matrix, take a message and generate a diagonal matrix corresponding to it.

Step 2: Multiply the above 2 matrices as first level of encryption.

Step 3: Now add this matrix to a Fibonacci Matrix of same order as the second level of encryption.

Step 4: Plot a graph considering the aforesaid matrix as the adjacency matrix in the final level of encryption.

Decryption Procedure

Step 1: Using the graph shared the receiver can write the adjacency matrix corresponding to it.

Step 2: In the second level, Fibonacci Matrix of same order can be subtracted.

Step 3: Finally, the message can be obtained by multiplying this matrix with the inverse of the incidence matrix.

4. Example

Encryption

Take the graph represented in **Figure 1**

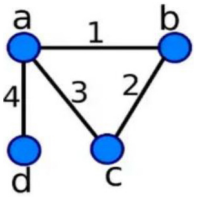

Figure 1

Whose incidence matrix is given as

$$\text{Incidence Matrix is A} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Message: B O O K

1 14 14 10 The diagonal matrix corresponding to it is

$$B = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 14 & 0 & 0 \\ 0 & 0 & 14 & 0 \\ 0 & 0 & 0 & 10 \end{bmatrix}$$

First level Encryption:

$$\text{Let } C = A \times B = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 14 & 0 & 0 \\ 0 & 0 & 14 & 0 \\ 0 & 0 & 0 & 10 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 14 & 10 \\ 1 & 14 & 0 & 0 \\ 0 & 14 & 14 & 0 \\ 0 & 0 & 0 & 10 \end{bmatrix}$$

Now consider the Fibonacci Matrix $E = \begin{bmatrix} 0 & 1 & 1 & 2 \\ 3 & 5 & 8 & 13 \\ 21 & 34 & 55 & 89 \\ 144 & 233 & 377 & 610 \end{bmatrix}$

Second level Encryption:

$$F = C + E \begin{bmatrix} 1 & 0 & 14 & 10 \\ 1 & 14 & 0 & 0 \\ 0 & 14 & 14 & 0 \\ 0 & 0 & 0 & 10 \end{bmatrix} + \begin{bmatrix} 0 & 1 & 1 & 2 \\ 3 & 5 & 8 & 13 \\ 21 & 34 & 55 & 89 \\ 144 & 233 & 377 & 610 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 15 & 12 \\ 4 & 19 & 8 & 13 \\ 21 & 48 & 69 & 89 \\ 144 & 233 & 377 & 620 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 1 & 15 & 12 \\ 4 & 19 & 8 & 13 \\ 21 & 22 & 17 & 11 \\ 14 & 25 & 13 & 22 \end{bmatrix} \text{ after being reduced to modulo 26}$$

Final Level of Encryption:

The graph of the adjacency Matrix F is as follows.

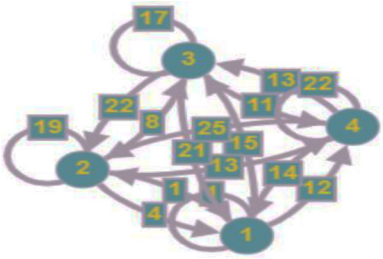

Figure 2

Adjacency Matrix

Figure 2 is the encrypted message which is being shared.

Decryption

In the First level of Decryption the adjacency matrix of the graph shared is being calculated.

$$F = \begin{bmatrix} 0 & 1 & 15 & 12 \\ 4 & 19 & 8 & 13 \\ 21 & 22 & 17 & 11 \\ 14 & 25 & 13 & 22 \end{bmatrix}$$

In the second level of decryption same order Fibonacci matrix is subtracted from this adjacency matrix F, which will result in matrix C.

$$C = F - E = \begin{bmatrix} 0 & 1 & 15 & 12 \\ 4 & 19 & 8 & 13 \\ 21 & 22 & 17 & 11 \\ 14 & 25 & 13 & 22 \end{bmatrix} - \begin{bmatrix} 0 & 1 & 1 & 2 \\ 3 & 5 & 8 & 13 \\ 21 & 34 & 55 & 89 \\ 144 & 233 & 377 & 610 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 14 & 10 \\ 1 & 14 & 0 & 0 \\ 0 & 14 & 14 & 0 \\ 0 & 0 & 0 & 10 \end{bmatrix} \text{ (modulo 26 is applied where ever it is necessary)}$$

In the final level the receiver multiplies this matrix with inverse of the matrix A to obtain the message in the form of a diagonal matrix.

$$B = A^{-I}C \begin{bmatrix} \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ 0 & 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 14 & 10 \\ 1 & 14 & 0 & 0 \\ 0 & 14 & 14 & 0 \\ 0 & 0 & 0 & 10 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 14 & 0 & 0 \\ 0 & 0 & 14 & 0 \\ 0 & 0 & 0 & 10 \end{bmatrix}$$

The decrypted message now is 1 14 14 0 which means BOOK

5. Discussion and Conclusion

The traditional cryptosystem developed above using Incidence Matrix, Adjacency Matrix, Fibonacci Matrix and Graph theory as different phases in super-encryption is more secure than the cryptosystems involving single or double layers of encryption. This work can also be extended to asymmetric key cryptosystem.

References

[1] Fred Piper and Sean Murthy" Cryptography: A very short introduction", Oxford University Press (2002).

[2] J.Buchman "Introduction to Cryptography", Springer-Verlag (2001).

[3] Neal Koblitz, "A Course in Number Theory and Cryptography", Springer-Verlag (1987).

[4] K.H.Rosen, "Elementary Number Theory and Its Applications," Third edition., Addson Wesly

[5] Gudela Ashok, S. Ashok Kumar, D. Chaya Kumari & Mathe Ramakrishna. "A type of public cryptosystem using polynomials and Pell sequences", *Journal of Discrete Mathematical Sciences and Cryptography* (JDMSC), 25:7, 1951-1963 (2022), DOI: 10.1080/09720529.2022.2133237.

[6] A. Chandrasekhar, D. Chaya Kumari, S. Ashok Kumar "Symmetric Key Cryptosystem for Multiple Encryptions", *International Journal of Mathematics Trends and Technology* (IJMTT). V29 (2):140-144 January (2016). ISSN:2231-5373.

[7] D. Chaya Kumari, S. Ashok Kumar, D. Triveni "Super-Encryption Method of Laplace Transformations using Fibonacci Numbers,", *Journal of Huazhong University of Science and Technology*, vol. 50, no. 7.

[8] Beena Kittur, D. Chaya Kumari, Sneha G. Kulkarni, Manjula K M, "Super-Encryption Method using Affine Transform Via Trees" *International Journal of Mathematics Trends and Technology,* Volume 68 Issue 6

[9] Om, Hari, and Rahul Patwa. "Affine transformation in cryptography." *Journal of Discrete Mathematical Sciences and Cryptography* 11.1 : 59-65 (2008).

[10] A. Chandra Sekhar, V. Anusha, B. Ravi Kumar & S. Ashok Kumar "Linearly independent spanning sets and linear transformations for Multi-level Encryption", *Journal of Information and Optimization Sciences*, 36:4, 385-392 (2015), DOI: 10.1080/02522667.2014.961821.

[11] A.ChandraSekhar, D. ChayaKumari, Ch.Pragathi, S. Ashok Kumar, "Multiple Encryptions of Fibonacci Lucas Transformations," *International Organization of Scientific Research,* vol. 12, no. 2, pp. 66-72 (2016). DOI: 10.9790/5728-1202026672

[12] Gross, Yoav, et al. "A Huffman Code Based Crypto-System." 2022 Data Compression Conference (DCC). IEEE (2022).

[13] Jegan, R., Vijayakumar, P., Ambeth kumar, V. D., Vijay, Pa & Onyema, Edeh Michael "Encryption and decryption of a word into weighted graph using super-edge anti-magic total labeling of Bi-star graph", *Journal of Discrete Mathematical Sciences and Cryptography* (JDMSC), 26:5,1355–1365, (2023) DOI: 10.47974/JDMSC-1752.

[14] Kessler, Gary C. "An overview of cryptography." (2003).

[15] Kumar, Ankit, Pankaj Dadheech, Vijander Singh, Ramesh C. Poonia, and Linesh Raja. "An improved quantum key distribution protocol for verification." *Journal of Discrete Mathematical Sciences and Cryptography* 22, no. 4 (2019).

[16] A. Chandrasekhar, D. ChayaKumari, Ch. Pragathi, S. Ashok Kumar, "Triple Encryption Scheme Using Two Independent Keys," *International Journal of Engineering Science and Technology,* vol. 8, No. 4 (2016).

[17] P. Amudha, A.C. Charles Sagayaraj, A.C. ShanthaSheela, "An Application of Graph Theory in Cryptography," *International Journal of Pure and Applied Mathematics,* vol. 119, no. 13, pp. 375-383 (2018).

[18] Dharmendra Kumar Gurjar and Aparajita Krishnaa, "Lexicographic Labeled Graphs in Cryptography," *Advances and Applications in Discrete Mathematics*, vol. 27, no. 2, pp. 209-232 (2021).

[19] Ranasinghe, Rajitha, Chathurangi, Madusha & Athukorala, Pabasara. A novel improvement in RSA algorithm, *Journal of Discrete Mathematical Sciences and Cryptography* (JDMSC), 27:1, 143–150 (2024), DOI: 10.47974 /JDMSC-1628.

[20] Sharba, Bashar Ahmed, Al-Khalidy, Roaa Razaq & Hussein, Raghad I. A new approach of cryptography using Taylor series of logarithm function, *Journal of Discrete Mathematical Sciences and Cryptography* (JDMSC), 26:7, 1889–1895 (2023), DOI: 10.47974/JDMSC-1680.