INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

A Hamiltonian Path-Based Enciphering Technique with the use of a Self-Invertible Key Matrix

P Mohan[1,2]*, K Rajendran[3], A Rajesh[4]

1 Research Scholar, Department of Mathematics, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, Tamil Nadu, India
2 Assistant Professor, Department of Mathematics, SRM Arts and Science College, Kanchipuram, Tamil Nadu, India
3 Assistant Professor, Department of Mathematics, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, Tamil Nadu, India
4 Associate Professor, Department of CSE, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai, Tamil Nadu, India

OPEN ACCESS

Received: 14-09-2022
Accepted: 07-10-2022
Published: 23-11-2022

Citation: Mohan P, Rajendran K, Rajesh A (2022) A Hamiltonian Path-Based Enciphering Technique with the use of a Self-Invertible Key Matrix . Indian Journal of Science and Technology 15(44): 2351-2355. https://doi.org/10.17485/IJST/v15i44.1861

* **Corresponding author**.

mohan14palani@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objective: The symmetric encryption technique is one of the most important fields for securing communications between people. In order to produce complex ciphertext, we are introducing the new enciphering technique with the help of the Hamiltonian path, a self-invertible key matrix for encryption and decryption. **Methods:** There are many kinds of symmetric enciphering methods, like the Caesar Cipher, Atbash Cipher, Hill Cipher, etc. All these methods use a common key for encryption, and while decrypting the inverse of that matrix should be found, it is also too hard to share the common key. To reduce this terminology, we proposed the novel enciphering method with the help of a self-invertible key matrix. **Findings:** We are using the generated self-invertible key matrix as a key matrix; the degree of the self-invertible matrix is even. If our graph does not form an even-degree adjacency matrix, then we have to make it into an even-degree adjacency matrix by adding dummy edges. **Novelty:** As we are using a self-invertible matrix as a key matrix, we do not need to compute the inverse of the key matrix for the process of decryption. This helps us to reduce the complexity of finding the inverse while decrypting the original message.

Keywords: Graph Theory Encryption; Hill Cipher; Hamiltonian Path; Adjacency Matrix; Self Invertible Matrix

1 Introduction

Graph theory is a primary source for cryptography[(1)]. The symmetric encryption algorithm using cycle graph, complete graph, and minimal spanning tree was explained in[(1,2)]. In both cases, the upper triangular matrix was used as a common key matrix. The concept of encryption techniques using Hamiltonian paths and complete graphs was utilized in[(3)] with the help of a lower triangular matrix as a key matrix. A connection between graph theory and cryptography was explained in[(4)], the upper triangular

matrix was used here as a key matrix. A new message encoded and decoded technique using graph labelling was explained in [5], the upper triangular matrix was used here as a key matrix, to enhance the security of cipher Tetragraphic trifunction a self-invertible matrix of order 4 was used [6]. Most of the methods that are mentioned above use the symmetric encryption algorithm. The same key, usually lower triangular and upper triangular, is used for both sender and receiver, and these keys are shared between the users over any kind of median. It is easy to break once the intermediates know the technique, and it is difficult to share the common key matrix over an unsecure channel.

In order to reduce this terminology, strengthen the key and produce more security for the given information, we have proposed a new technique that uses the adjacency matrix and self-invertible matrix [7,8] as the key for both encryption and decryption. As we are using a self-invertible matrix as a key matrix (the matrix and its inverse are both the same), so we do not need to compute the inverse while decrypting the cipher text. It helps us to reduce the complexity of finding the inverse. Also, we are not sharing the entire key matrix over an unsecured channel. This improves the security of the data and lowers the likelihood that the key matrix will be broken.

The proposed approach is made by first finding the adjacency matrix of a Hamiltonian path of an undirected graph using the given message units as graph edges, and this adjacency matrix can be multiplied with the generated self-invertible key matrix. The output is sent to the receiver over an unsecured channel, and the receiver should use the reverse process to read the original message. The rest of this paper is defined as follows: The self-invertible key matrix generation was discussed in Section 2. Section 3 explains the new proposed methodology, and in Section 4, the results and discussion will be given. Finally, the conclusion was given in Section 5.

2 Generation of self-invertible key matrix

A matrix N is said to be self-invertible matrix if $N = N^{-1}$, that is $N \cdot N^{-1} = N^{-1} \cdot N = I$, the self-invertible matrix was generated by using the following procedure, consider any arbitrary $\frac{n}{2} \times \frac{n}{2}$ matrix N_{22} (since n is the order of adjacency matrix it must be even) with the help of N_{22} we can compute the remaining $\frac{n}{2} \times \frac{n}{2}$ matrices using the following properties;

$$N_{11} + N_{22} = 0, \quad N_{12} = I - N_{11}, \; N_{21} = I + N_{11}$$

After computing $N_{11,}\ N_{12,}\ N_{21}, N_{22}$ the self-invertible matrix N was created by

$$N = \begin{bmatrix} N_{11} & N_{12} \\ N_{21} & N_{22} \end{bmatrix} = \begin{bmatrix} n_{11} & n_{12} & \cdots & \vdots & \cdots & n_{1n} \\ n_{21} & n_{22} & \cdots & \vdots & \cdots & n_{2n} \\ \cdots & \cdots & \cdots & \vdots & \cdots & \cdots \\ \cdots\cdots & \cdots & \cdots & \vdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \vdots & \cdots & \cdots \\ n_{n1} & n_{n2} & \cdots & \vdots & \cdots & n_{nn} \end{bmatrix}$$

3 Methodology

The proposed methodology using the Hamiltonian path of an undirected graph with the self-invertible key matrix was explained in this section.

3.1 Hamiltonian path-based encryption algorithm

Step 1: The given plain text message is to be converted into its numerical equivalent values. These numerical equivalent values are put into the edges of an undirected graph (i.e., as weights of the edges of the path).

Step 2: Create a path of n-vertices (depending on the number of requirements), beginning with vertex 1.

Step 3: Draw a Hamiltonian path, assign each weight, and then compute the adjacency matrix of this Hamiltonian path. Name this matrix.

Step 4: For the key matrix, we are generating a self-invertible key matrix of even order. Since the key matrix is even, the adjacency matrix must be of order even (the number of edges of a Hamiltonian path must be odd) in case the given path doesn't form an even-order adjacency matrix. We have to make that into the form of an even adjacency matrix by adding some dummy edges with false weights to the existing Hamiltonian path.

Step 5: After generating a self-invertible key matrix, multiplying it with the adjacency matrix. The final resultant matrix is the encrypted data for the original message units.

Step 6: Finally, this encrypted matrix shared with other users over an unsecure channel, either row-wise or column-wise, also represents the number of vertices, i.e., I, n, <encrypted matrix> <the matrix which helps to generate self-invertible matrix>, where I is the index value of the given Hamiltonian path, n being the size of the matrix.

3.2 Hamiltonian path-based decryption algorithm

Step 1: With the help of received data, the receiver is able to find the index value, order of the matrix, and the matrix which helps to generate the self-invertible matrix. The receiver will then separate the matrices.

Step 2: The given encrypted matrix can be multiplied with the generated self-invertible key matrix.

Step 3: Trace back the graph with the help of the above resultant matrix and write the edge length of the graph from the given index value.

Step 4: Decode these values with their numerical equivalent values. Then finally, the receiver is able to identify the original message.

4 Result & Discussion

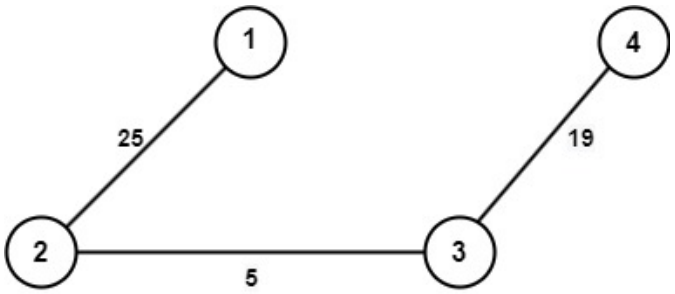
Suppose that User A(sender) wants to send the message "YES" to User B(receiver) using the above-mentioned technique. Assume that both the users know the encryption and decryption techniques of the given procedure.

4.1 Hamiltonian based encryption- User A (The sender)

Encryption is done by the following steps

Firstly, the sender converts the given message units" YES" into their numerical equivalent values that is $Y \rightarrow 25, \quad E \rightarrow 5, \quad S \rightarrow 19$.

Create a Hamiltonian path with 4 vertices, label the above mentioned numerical equivalent values as the edges of a path with 4 vertices which begins from the index value 1, the vertices are connected by sequential letters.



Compute the adjacency matrix for the above Hamiltonian path and denote it as 'M'

$$M = \begin{bmatrix} 0 & 25 & 0 & 0 \\ 25 & 0 & 5 & 0 \\ 0 & 5 & 0 & 19 \\ 0 & 0 & 19 & 0 \end{bmatrix}$$

Now we need to compute the key matrix. For that purpose, we construct the self-invertible key matrix 'N' with the help of a shared matrix and the procedure discussed above.

$$Let\ N_{22} = \begin{bmatrix} 1 & 4 \\ 9 & 6 \end{bmatrix}\ then\ N_{11} = \begin{bmatrix} 25 & 22 \\ 17 & 20 \end{bmatrix},\ N_{12} = \begin{bmatrix} 2 & 4 \\ 9 & 7 \end{bmatrix},\ and\ N_{21} = \begin{bmatrix} 0 & 22 \\ 17 & 21 \end{bmatrix}$$

$$\therefore N = \begin{bmatrix} N_{11} & N_{12} \\ N_{21} & N_{22} \end{bmatrix} = \begin{bmatrix} 25 & 22 & 2 & 4 \\ 17 & 20 & 9 & 7 \\ 0 & 22 & 1 & 4 \\ 17 & 21 & 9 & 6 \end{bmatrix}$$

Finally, we have to compute MN, this multiplication is known as the encrypted data and send it to the user B over an unsecure channel.

$$MN = \begin{bmatrix} 0 & 25 & 0 & 0 \\ 25 & 0 & 5 & 0 \\ 0 & 5 & 0 & 19 \\ 0 & 0 & 19 & 0 \end{bmatrix} \cdot \begin{bmatrix} 25 & 22 & 2 & 4 \\ 17 & 20 & 9 & 7 \\ 0 & 22 & 1 & 4 \\ 17 & 21 & 9 & 6 \end{bmatrix} = \begin{bmatrix} 425 & 500 & 225 & 175 \\ 625 & 660 & 55 & 120 \\ 408 & 499 & 216 & 149 \\ 0 & 418 & 19 & 76 \end{bmatrix}$$

This MN matrix can be converted in the form of row or column matrix and sent it to other user over an unsecure channel with index number, size of matrix, the encrypted matrix and the matrix which helps to generates self-invertible matrix.

[1, 4, 425, 500, 225, 175, 625, 660, 55, 120, 408, 499, 216 , 149, 0, 418, 19, 76, 1, 4, 9, 6]

Hamiltonian based decryption- User B (The receiver)

Decryption is done by the following steps

With the received information, the receiver separates the following matrix,

$$M_2 = \begin{bmatrix} 425 & 500 & 225 & 175 \\ 625 & 660 & 55 & 120 \\ 408 & 499 & 216 & 149 \\ 0 & 418 & 19 & 76 \end{bmatrix}$$

And the self-invertible key matrix be

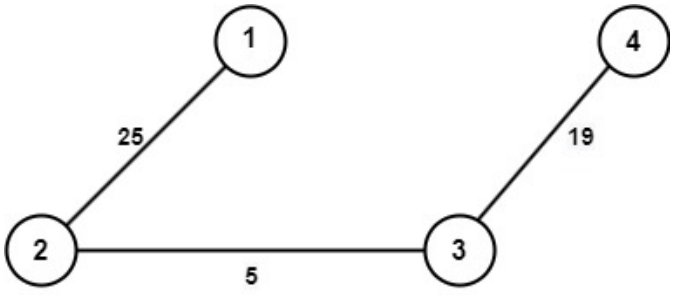
$$N_2 = \begin{bmatrix} 25 & 22 & 2 & 4 \\ 17 & 20 & 9 & 7 \\ 0 & 22 & 1 & 4 \\ 17 & 21 & 9 & 6 \end{bmatrix}$$

$$M_2N_2 = \begin{bmatrix} 425 & 500 & 225 & 175 \\ 625 & 660 & 55 & 120 \\ 408 & 499 & 216 & 149 \\ 0 & 418 & 19 & 76 \end{bmatrix} \cdot \begin{bmatrix} 25 & 22 & 2 & 4 \\ 17 & 20 & 9 & 7 \\ 0 & 22 & 1 & 4 \\ 17 & 21 & 9 & 6 \end{bmatrix} = \begin{bmatrix} 22100 & 27975 & 7150 & 7150 \\ 28885 & 30680 & 8325 & 8060 \\ 21216 & 26837 & 6864 & 6883 \\ 8398 & 10374 & 4465 & 3458 \end{bmatrix}$$

Taking addition modulo 26 (since we are using 26 alphabets), we get

$$M_2N_2 = \begin{bmatrix} 0 & 25 & 0 & 0 \\ 25 & 0 & 5 & 0 \\ 0 & 5 & 0 & 19 \\ 0 & 0 & 19 & 0 \end{bmatrix}$$

The Corresponding Path for the above adjacency matrix is



The edges(weights) of the above path are 25 5 19.

∴The original message is $25 \rightarrow Y$, $5 \rightarrow E$, $19 \rightarrow S$ i.e., YES

5 Conclusion

A new approach to cryptosystem using graphs and self-invertible matrices has been proposed in this study, which uses the concepts of Hamiltonian path, adjacency matrix, and self-invertible matrix in order to increase the security of our information. The proposed approach is more effective and resists the intermediate. In all the symmetric encryption methods provided previously using the concept of graph theory, they use a common key matrix for encryption/decryption. Sharing the key matrix, computing the inverse while decrypting are the main drawbacks in all of these methods. As we are using the self-invertible matrix as the key matrix, it eliminates the complexity involving for finding the inverse. Also, we are not sharing the entire key matrix over the unsecured medians, so this method is more effective than the existing approaches, it is also a simple encryption and decryption technique with better security. The proposed approach can also be used effectively in wireless applications.

References

1) Dixit U. Cryptography a Graph theory approach. *International Journal of Advance Research in Science and Engineering*. 2017;6(01).
2) Mahmoud W, Etaiwi AI. Encryption algorithm using Graph theory. *Journal of Scientific Research & Reports*. 2014;3(19):2519–2527. Available from: https://doi:10.9734/JSRR/2014/11804.
3) Yamuna M, Gogia M, Sikka A, Khan MJH. Encryption Using Graph Theory and Linear Algebra. *International Journal of Computer Application*. 2012;5(2):2250–1797.
4) Nandhini R, Maheswari V, Balaji V, Graph. *Theory Approach on Cryptography*. 2018. Available from: https://doi.org/10.26524/jcm32.
5) Amudha P, Jayapriya J, Gowri J. An Algorithmic Approach for Encryption using Graph Labeling. *Journal of Physics: Conference Series*. 2021;1770(1):012072–012072. Available from: https://doi:0.1088/1742-6596/1770/1/012072.
6) Lin S, Ching P, Yunos F. Effect of Self-Invertible Matrix on Cipher Hexagraphic Polyfunction. 2019. Available from: https://doi.org/10.3390/cryptography3020015.
7) Acharya B, Rath GS, Patra SK, Panigrahy S. A Novel method of generating self-invertible matrix for Hill Cipher Algorithm. *International Journal of Security* . 2007;p. 14–21. Available from: https://www.cscjournals.org/library/manuscriptinfo.php?mc=IJS-2.
8) Mohan P, Rajendran K, Rajesh A. A, An Encryption Technique using a Complete graph with a Self-invertible matrix. *Journal of Algebraic statistics*. 2022;13(3):1821–1826. Available from: https://publishoa.com/index.php/journal/article/view/816.