# Enhancing Data Security Through Graph Theory

**[1]Laxmiparbati Das, [2]Samikshya Mishra, [3]Sujit Mehar**

[1]Assistant Professor in Dept. of Computer Science, GIET Gangapatna, Bhubaneswar
[2]Assistant Professor in Dept. of Computer Science, GIET Gangapatna, Bhubaneswar
[3]Assistant Professor in Dept. of Computer Science, GIET Gangapatna, Bhubaneswar

**Abstract:** Sharing private data over unsecured channels poses a grave risk, as it can be intercepted by unauthorized entities, compromising its privacy. Consequently, the development of a cryptosystem that ensures the confidentiality, integrity, and authenticity of transmitted data has become an imperative necessity. Extensive efforts have been dedicated to this endeavor, yet the robustness and performance of many proposed cryptosystems vary considerably. Safeguarding information has been a cornerstone of human existence since ancient times, with cryptography emerging as a vital technique for securing message transmission and data protection. Additionally, graph theory plays a significant role in data security. Numerous encryption and decryption techniques are available within cryptography to render text unintelligible to adversaries. Cryptography finds wide-ranging applications, including e-commerce, electronic communications, business transactions, financial information transmission, and ATM card security, impacting various aspects of daily life. By concealing sensitive information, cryptography ensures privacy and security through mathematical techniques. A cryptographic scheme is considered secure if it remains unbreakable within a reasonable timeframe, even when adversaries are aware of the algorithm and key size. In this paper, we propose an algorithm that utilizes the adjacent matrix representation of graphs to derive encryption and decryption keys, thereby contributing to the advancement of secure data transmission methods.

## Introduction

Cryptography is a part of cryptology that is based on a number of methods and principles for converting a readable message into a completely unreadable one. This area deals with many security issues such as confidentiality of communication over insecure channels, privacy of individuals, storage of data on insecure media and so on. Cryptography refers to the study and analysis of data encryption systems to reduce the impact of hackers and to best prevent unauthorized attempts to gain access to this confidential data. Main principles of information security, especially confidentiality, integrity, authentication and non-repudiation.

Confidentiality is a key part of security. This can be ensured by an encryption process where the data becomes unintelligible to any unauthorized parties trying to access it. The idea behind the encryption process is to turn plaintext into ciphertext so that only authorized parties can retrieve the message in its original format by reversing the encryption process, known as decryption. Technically, decryption should be extremely difficult for any unauthorized and unskilled parties attempting to perform it.

The main goal of Data Security is to secure data transmission over an unreliable network. When we send a message to someone, we always suspect that someone else will catch it and read or edit it before we send it again. There is always a desire to know about a secret message sent or received between two parties with or without any personal, financial or political gains. It's no wonder to feel like sending someone a message so that no one else can interpret it. Information security has thus become a very critical aspect of a modern computer system. Information security is mostly achieved using cryptography. Art of Sciences and Graph theory computer science creates unreadable data so only a designated person is capable read text using cryptography. Encryption is the process by which we convert our data into ciphertext or not legible form. Decryption is the opposite process of encryption.

Encryption is the only conventional method for keeping data secure. Information could be which the unauthorized user accessed for nefarious purposes. Cryptography is a process to protect a network and data transmission over wireless networks. Data security is the main concept of data transmission security unreliable networks. Data security is a challenging and risky task that today's data communication touches various areas including secure communication channels, strong data encryption techniques and a trusted third party maintain a database. Rapid progress and development in the field of information technology, secure transmission confidential (secret) data thus receives a lot of attention.

The adjacency matrix that we use in the network security plays a vital role in the transmission of secure keys.

Graph theory in mathematics refers to the study of graphs, which are the main subject of discrete mathematics. In general, a graph is represented as a set of vertices connected by edges. So they are mathematical structures used to model pairwise relationships between objects. It can be found in road networks, electrical circuits, constellations, etc. Graphs provide a way of thinking that can be used to model a wide variety of problems. They are the basis of many computer programs that enable communication and advanced technological processes. The Seven Bridges of Königsberg (1736) [8] is a mathematical problem well known for laying the foundations of graph theory. Graph theory is a relatively new concept that has been successfully incorporated and allowed the development of stronger encryption algorithms that have proven difficult to crack, even for the latest software solutions. It actually consists of modeling encryption problems using a graph representation so that they end up being problems in graph theory, where the solutions are usually well known.

The design of cryptosystems based on graph theory concepts is of utmost importance. In this work, we present a new cryptosystem that uses graph theory principles that enable a high degree of security while maintaining data processing performance. The rest of the paper is structured as follows. Preliminary knowledge on cryptography and graph theory is presented. The proposed algorithm is described with example.

## Definitions

Cryptography - The process of transforming a plain message into ciphertext (unreadable) and then back again transforming this message back to its original form is called cryptography.

Plain text – The original message or plain text that must be in readable form encrypted and makes it an unreadable form.

Cipher-text – The transformed message we received after applying the key to plaintext.

Key - Some unreadable ciphertext, known only to the sender and recipient, the key is a variable that is useful using an algorithm to create ciphertext or to decrypt ciphertext.

Encipher and Decipher: The process of converting plaintext (readable text) to ciphertext (unreadable text). The process of converting ciphertext (unreadable text) back to plaintext (readable text).

Encryption and Decryption - The process of encoding a message using some key or method so that it is the meaning is not easily understood. The reverse process of the ciphertext conversion encryption method into plain text is decryption.

Brute Force Attack - A brute force attack is an intervention and testing process used to obtain information from authenticate users.

Graph: A graph G is a set of points called vertices V and a set of lines called edges E that connect some vertices together. A graph is defined as the set of vertices and edges that form the pair G = (V, E). • Simple graph: A graph in which each pair of vertices is connected by at most one edge and where no vertex has a loop.

Undirected graph: An undirected graph G is a pair (V, A) where V is a finite set of vertices and A is a set of unordered pairs of vertices. Also, loops are not allowed in undirected graphs.

Cycle: A chain whose start and end nodes are the same and which does not use the same link more than once.

## Adjacency matrix

This is a matrix representation of the graph. It is used in computer processing. In graph theory and computer science, an adjacency matrix is a square matrix used to represent a finite graph. The matrix elements indicate whether a pair of vertices in the graph are adjacent or not. In the special case of a finite simple graph, the adjacency matrix is a (0,1)-matrix with zeros on its diagonal. The advantage of using an adjacency matrix representation is that many results of matrix algebra can be arbitrarily applied to the study of structural properties of graphs. An adjacency list represents a graph (without multiple edges) by specifying the vertices that are adjacent to each vertex. This matrix is based on the arrangement chosen for the vertices. This matrix can represent both directed and undirected graphs. Let G be an undirected graph with m vertices from 1 to m. We call the adjacency matrix of graph the matrix

$A = (a_{jk})$ where $a_{jk}$ is the total number of edges joining vertex j to vertex k:

$a_{jk} = w$ if and only if j and k are adjacent. $a_{jk} = 0$ if not. (1) with w is the weight of the edge (j, k)

## Related work

Graph theory has become a very important component in many applications in the field of network security. Unfortunately, understanding the graph theory and its applications is one of the most difficult and complex missions. In this study, the authors reviewed some main applications of graph theory in IT security. Some aspects of graph theory applications were covered, especially with regard to encryption. Some related works that have applied graph theory in different types of networks and information security field are:

In 2013, Eftekhari and Abdullah [12], the researchers analyzed two graph-based authentication protocols. The weaknesses of each method were clarified. They proposed a new scheme without addressing the method of determining the number of nodes in the Journal of Discrete Mathematical Sciences and Cryptography titled Cryptanalysis and Improvements on Some Graph-Based

_____
ISSN (Print): 2278-5140, Volume-12, Issue-2,2023

12

Authentication Schemes.

In 2014, Mahmoud and Etaiwi1[7], the researchers presented a symmetric Cryptographic algorithm to encode data for the purpose of transferring by using a coding table. However, they did not mention the possibility of its application in distributed systems, in the Journal of Scientific Research& Reports titled Encryption Algorithm Using Graph Theory. In 2014, Sen and Samanta [10], the researchers focused on the possibility of using graph theory concepts in network monitoring and assessing the importance of individual routers within a network giving traffic pattern in the Journal IJIRT titled Network Security Using Graph Theory. In 2016, Dutta, et. al proposed an algorithm for encryption using the Euler graph by using encoder tracking the Hamilton circle from the encoded graph. However, the researchers had a problem applying it where each graph carries one letter of a message in the Journal International Journal of Pharmacy & Technology titled A Graph Based Message Encryption Algorithm.

**Main Result**

Proposed Algorithm: Use the proposed algorithm to encrypt and decrypt data. (Send key2 in the form of graph)

**Encryption**: This algorithm is used to convert plain text to cipher text.

- First we take a message from user which has to encrypt

- Use key1 to shift character.

- Encrypt the message by replacing each letter by decided key 1.

- Write encrypted message in the form of matrix. (where (n-1) x n where n=number of digits in key2) which is decided by sender and receiver.

- Read off the message row by row and permute the order of column.

- The output of step 5, write in matrix form again and read row by row.

- After reading row by row, we get our cipher text.

**Decryption**: This algorithm is used to convert cipher text to plain text.

- It take the cipher text and use key 2 to write cipher text in the form of matrix. (where, (n-1) x n where n=number of digits in key2) which is decided by sender and receiver.

- Arrange the cipher in matrix form column by column using key 2 .

- Read message row by row.

- Again arrange the cipher of step 3 in matrix form

column by column using key 2 .

- Now decrypt the message with key1.

- Finally we get plain text.

Example :- (Encryption)

- First take a message or plain text from user which we have to encrypt. For ex. THIS IS MY TEST

- Use key1 to shift character.

- Suppose key 1 = +4

- Encrypt the message by replacing each letter by decided key 1.

MCWLWIWQXXMX

- Write encrypted message in the form of matrix (where (n-1) x n where n=number of digits in key2) which is decided by sender and receiver.

Key2 is shared in the form of adjacent graph, sender and receiver have to calculate key2 from the given graph.
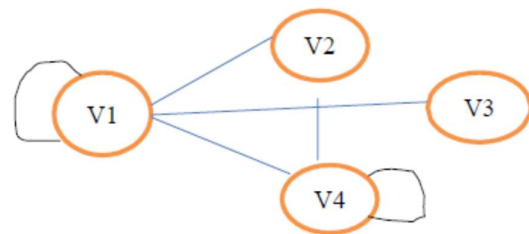


Fig.1: Graph for the calculation of key2 Convert the above graph into adjacent matrix which is used as key 2.

**Table 1: Adjacent matrix of key2**

|    | V1 | V2 | V3 | V4 |
|----|----|----|----|----|
| V1 | 1  | 1  | 1  | 1  |
| V2 | 1  | 0  | 0  | 1  |
| V3 | 1  | 0  | 0  | 0  |
| V4 | 1  | 1  | 0  | 1  |

Now the key2 is **4 2 1 3**

**Table 2(a): Message creation from key1**

| 4 | 2 | 1 | 3 |
|---|---|---|---|
| X | L | M | W |
| M | W | C | Q |
| X | I | W | X |

Read off the message row by row and permute the order of column MEELWBWRQXMI. The output of step 5, write in matrix form again and read row by row.

**Table 2(a): Message creation from key2**

| 4 | 2 | 1 | 3 |
|---|---|---|---|
| M | C | W | L |
| W | I | W | Q |
| X | X | M | X |

After reading row by row, we get our cipher text. WWMCICLQXMWX (cipher text to be sent)

**DECRYPTION**

It take the cipher text and use key2 to write cipher text in the form of matrix (where (n-1) x n, where n=number of digits in key2) which is decided by sender and receiver.

Received cipher text is: - WWMCICLQXMWX

Arrange the cipher in matrix form column by column using key2.

**Table 3(a): Cipher text in matrix form**

| 4 | 2 | 1 | 3 |
|---|---|---|---|
| M | C | W | L |
| W | I | W | Q |
| X | C | M | X |

▶ Read message row by row. MCWLWIWQXXMX

Again arrange the cipher of step 3 in matrix form column by column using key 2.

**Table 3(b): Cipher text in matrix form**

| 4 | 2 | 1 | 3 |
|---|---|---|---|
| X | L | M | W |
| M | W | C | Q |
| X | I | W | X |

Received cipher text is: - XLMWMWCQXIWX Now decrypt the message with key1. Key1= (-4) Finally we get plain text.

Result: This is my test

# Conclusion

The utilization of the "Double Transposition column" method, with the graph serving as the key, provides several advantages over simpler algorithms. Its increased complexity poses challenges for cryptanalysis, enhancing overall security. By incorporating the graph into the development of key2, the resulting plaintext becomes virtually uncrackable, effectively thwarting brute force attacks and significantly bolstering security measures. Consequently, this approach effectively surpasses the inherent limitations of the Caesar cipher. Moreover, the new application offers ease of updates and the capability to generate multiple keys tailored for various applications such as banking, e-commerce, and e-voting. However, due to the integration of graph theory in security, there may be a trade-off in terms of increased memory usage.

## Future Enhancements

This algorithm is based on the concept of taking alphabet as plaintext, which can also be extended in future with alpha numeric data.

## References

[1] Atul Kahate (2009) Cryptography and Network security, 2nd Edition, McGraw Hill

[2] "Enhancing security of caesar cipher by Double colummar transposition method" by Vinod Saroha, Suman Mor and Anurage Dagar, International journal of advanced research in computer science and software engineering, vol. 2, issue 10, Oct. 2012.

[3] Stalling. W (1999), Cryptography and Network security, 2nd Edition, Prentice Hall

[4] William stalling "Network security Essentials (Application and standards)", Pearson Education, 2004

[5] A. J. Menezes, J. Katz, P. C. Van Oorschot, and S. A. Vanstone, Handbook of applied cryptography. CRC press, 1996.

[6] P. Amudha, A. C. Sagayaraj, and A. S. Sheela, "An application of graph theory in cryptography," International Journal of Pure and Applied Mathematics, vol. 119, no. 13, pp. 375–383, 2018.

[7] Mahmoud, W. and Etaiwi, A. 2014. Encryption Algorithm Using Graph Theory. Journal of Scientific Research & Reports, 3(19): 2519-2527.

[8] Connections between graph theory and cryptography Natalia Tokareva G2C2: Graphs and Groups, Cycles and Coverings September, 2426, 2014. Novosibirsk, Russia

[9] P. Venugopal, "Encryption using double vertex graph and matrices," Solid State Technology, vol. 64, no. 2, pp. 2486–2493, 2021.

[10] D. Sensarma and S. S. Sarma, "Application of graphs in security," International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 10, pp. 2273–2279, 2019.

[11] T. A. Khaleel and A. A. Al-Shumam, "A study of graph theory applications in it security," Iraqi Journal of Science, vol. 61, no. 10, pp. 2705–2714, 2020.

[12] Abdullah, H. O. and Eftekhari, M. 2013. Cryptanalysis and Improvements on Some Graph-Based Authentication Schemes. Journal of Discrete Mathematical Sciences and Cryptography, 16(4- 5):297-306.

❖ ❖ ❖