Journal of Indian Acad. Math
Vol. 47, No. 2 (2025) pp. 381-391
ISSN: 0970-5120

Keerti Acharya[1],
Rinku Verma[2],
Pranjali kekre[3]

A NOVEL TECHNIC USING COMPLETE GRAPH LABELING AND ASCII REPRESENTATION

ABSTRACT. In this paper, we present a novel encryption technique that uses complete graph labeling and ASCII code mapping to improve data security. The method encodes plaintext characters as labeled vertices in a complete graph, with edges representing distinct relationships based on encryption rules derived from graph theory principles. By combining ASCII values with graph labeling schemes, we create a structured but complex ciphertext that is resistant to common cryptanalysis techniques. The proposed approach ensures secure communication while remaining computationally efficient. Results are verified using Matlab software.

2020 Mathematical Science Classification: 11A07, 44A10, 94A60, 11T71

Keywords and Phrases: Network security, cipher text, complete graph, extended ASCII code.

1. INTRODUCTION

With the exponential growth of digital communication and data exchange, ensuring secure transmission of sensitive information has become a paramount concern.

Secured data transfer is always a matter of discussion, several techniques are already developed and a number of them are still in pipeline. Main motto of Cryptography is information security such as data integrity, entity authentication and data origin authentication. Cryptography is a set of techniques to provide information security. While designing a cryptography scheme, cryptographer always kept in mind that the designed algorithm is not very trivial to understand, replicate and therefore easily cracked. To secure the data from hackers it needs to be encrypted with high level of security.

It helps to store sensitive information, transmit it across insecure networks like internet so that it can't be read by anyone except the intended receiver.

Analysis of cryptographic security leads to using theoretical computer science especially complexity theory.

Graph theory, a mathematical discipline concerned with the study of graphs and their properties, has found applications in numerous fields, including network security and cryptography.

Various cryptographic methods have been developed and refined over the years to meet a wide range of security needs. Rivest et.al. [1] developed the RSA algorithm, a game-changing advancement in public-key cryptography that laid the groundwork for secure digital communications. In addition to public-key encryption, symmetric encryption schemes such as the Advanced Encryption Standard (AES) have gained popularity in both commercial and academic settings, as discussed by Katz and Lindell [2]. However, as cryptographic algorithms have advanced, challenges such as computational overhead, scalability, and performance have emerged, particularly when securing large datasets and ensuring efficient encryption in real-time communications.

Data security requirements have become even more complex with the growth of distributed systems and the Internet of Things (IoT). According to Bashir and Hussain [15], lightweight cryptography is essential, particularly in settings with limited resources when energy efficiency and processing power are critical. Hybrid cryptographic algorithms have been developed to combine the advantages of several encryption techniques while reducing their respective drawbacks for applications where protection is required for both data in transit and data at rest Srinivas and Manjunath, [12]. These algorithms are perfect for situations where secure data transmission without noticeable delay is crucial since they are made to provide a balance between performance, security, and resource usage.

Another urgent concern in contemporary cyber security is database security, specifically with regard to data in transit and at rest. Database encryption methods must retain acceptable performance levels while offering high levels of protection, claims Sullivan [16]. Effective encryption techniques are crucial for reducing potential vulnerabilities and guaranteeing that data is safe from malevolent actors since databases contain and handle vast amounts of sensitive data.

In order to protect unencrypted database files while they are in transit and at rest, this study attempts to propose a versatile and reasonably priced cryptographic encryption algorithm. The suggested solution aims to combine state-of-the-art encryption techniques with realistic implementation strategies, providing a balanced approach to protecting sensitive database information in contemporary technological landscapes. It does this by drawing on the principles described in foundational cryptography texts like those by Paar and Pelzl [3] and Boneh and Shoup [14].

This study aims to suggest a flexible and affordable cryptographic encryption solution to safeguard unprotected database files both in transit and at rest. The proposed method seeks to provide a balanced approach to safeguarding sensitive database data in today's technology environments by fusing cutting-edge encryption algorithms with practical implementation strategies.

In order to improve data security, Mathur[5] presented a symmetric key encryption algorithm that makes use of ASCII character values.

Kumar et al.[13] used a modified affine cipher to encrypt data by combining encryption and decryption procedures with graph plotting techniques.

Geena and Gupta [20] presented a novel method of improving data security through the combination of symmetric key cryptography and graph theory.

The improvement of data security in electronic communication systems is the subject of "A Triple Hill Cipher Algorithm Proposed to Increase the Security of Encrypted Binary Data and its Implementation Using FPGA" by As Khalaf et al. [9].

To increase the security of text data, Rajput et al. [7] published a cryptographic technique that employs double encryption. A key aggregate searchable encryption (KASE) technique was presented by Goutham et al. [10] to facilitate safe and effective cloud data sharing. The method offered a safe way to share data in cloud-based settings by enabling users to search encrypted data in the cloud without sacrificing privacy. Sampathkumar [11] talked about attribute-based encryption (ABE) and how it may be used to secure queries. He also suggested a way to organize queries such that ABE systems perform better, particularly in large-scale settings. In order to improve the security and effectiveness of image encryption while lowering the amount of data needed for transmission or storage, Mahmood and Shehab [6] developed a method for image encryption and compression based on compressive sensing and chaos theory. Gorabal and Manjaiah [8] presented a new image encryption approach to address security concerns related to image data. The method involved both spatial and frequency domain transformations to achieve high security levels for image transmission.

A method for identifying cryptographic algorithms by examining characteristics present in ciphertexts has been presented by Li, J. et al. [21]. In order to choose the encryption technique, the suggested scheme made use of statistical characteristics and patterns found in encrypted data.

Bing et al.[4] presented intriguing findings about spanning trees in graph theory. They investigated important properties and proposed new theorems that add to our understanding of spanning tree structures. These findings had direct implications for both theoretical combinatorics research and practical applications in areas such as network reliability, circuit design, and data structure optimization.

Shaik and Natarajan K [17] proposed a flexible and cost-effective cryptographic encryption algorithm that is specifically designed to secure unencrypted database files at rest and in transit. The algorithm focuses on providing strong security while reducing computational costs and complexity, making it an excellent choice for modern database systems that require scalable, real-time encryption without sacrificing performance. Verma et al[18] proposed an encryption algorithm based on modular arithmetic and Laplace transform. Chen, Y., et al.[19] proposed a Graph based algorithm for the encryption algorithm. Based on all these we have proposed a encryption algorithm based on the concept of graph theory and modular arithmetic.

2. PRELIMINARIES

2.1 Plain text: It signifies a message that can be understood by the sender, the recipient and also by anyone else who gets access to that message.
2.2. Cipher text: When a plain text message is codified using any suitable scheme, the resulting message is called as cipher text.
2.3. Encryption and Decryption: Encryption transforms a plain text message into cipher text, whereas decryption transforms a cipher text message back into plain text.
2.4 Complete Graph : A simple graph G is said to be complete if each vertex is joined to every other vertex by means of an edge.
2.5 Minimum Spanning Tree: A subgraph of a connected graph G which is a tree and contains all the vertices G is said to be spanning tree of G. A spanning tree with minimum weight is called minimum spanning tree.

3. ALGORITHM

Pseudo Algorithm for encryption and decryption is a proposed Algorithm based on the concept of complete graph labelling technique, a minimum spanning tree used to find secret key and basic matrix theory to find cipher text and to decode it to get plain Text again.

Step 1: Input the message and take the length of message as $'L'$.

Step 2: Represent the message as vertices of complete Graph $'K_L'$ as set $\{\{u_1, u_2, ---, u_L\}$ and edges as $\{e_1, e_2, ---, e_N\}$, where $N = \left(\frac{L(L-1)}{2}\right)$.

Step 3: Label the vertices as

$$f(u_{2i+1}) = L - i; 0 \le i \le \left\lfloor \frac{(L-1)}{2} \right\rfloor,$$

$$f(u_{2i}) = i; 1 \le i \le \left\lfloor \left(\frac{L}{2}\right) \right\rfloor.$$

Step 4:Label the $e =< u, v >$ as

$$f(e) = |f(u) - f(v)| + Max\{f(u), f(v)\}.$$

Step 5: Create the weighted adjacency Matrix A for the labeled $'K_L'$.

Step 6: Obtain the extended ASCII code for the each charter of inputmessage.

Step 7: Create the weighted adjacency Matrix B of the outer cycle of $'K_L'$, and fill the diagonal entries of Matrix B with the obtained extended ASCII code of the text to be encrypted.

Step 8: Create $N = A \text{x} B$.

Step 9: Find out the minimum Spanning tree of labeled complete graph $'K_L'$ and let the length of minimum spanning tree be $'S'$.

Step 9: Consider public key matrix M with all upper triangular entries as one and other as zero.

Step 10: Create Code matrix

$C = N\text{x}\text{M}$

$C_1 = \text{mod}(C, S)$

$C_2 = Qutionet(C, S).$

Step 11: Pass (C_1, C_2, A) as Cipher text and 'S' as Secret key to the Decoder.

Step 12 Decrypt (C_1, C_2, A) with 'S' as follows

Create $D = SC_2 + C_1$.

$N = DM^{-1}$ (where M is the Public Key)

B=A^{-1}N.

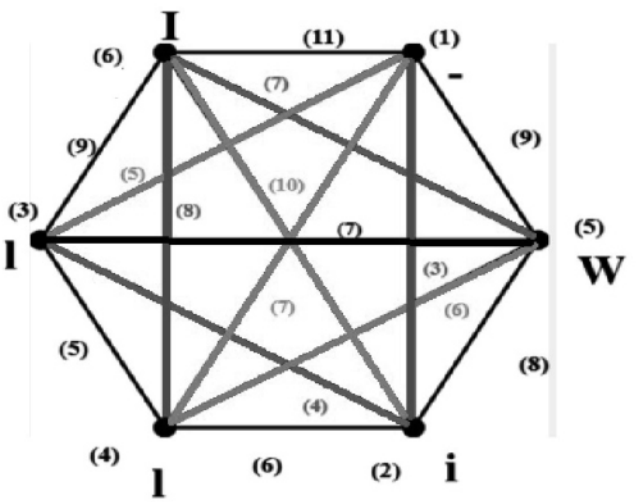
Diagonal entries of matrix B gives the extended ASCII code of input plain text and retrieved from the table.

Illustrative examples:

Plain Text "I Will"

L=6;

Graph K_6 is created and labeled as mentioned in algorithm, shown in figure 1.



Weightes adjacency matrix for the graph

$$A=\begin{bmatrix} 0 & 11 & 7 & 10 & 8 & 9 \\ 11 & 0 & 9 & 3 & 7 & 5 \\ 7 & 9 & 0 & 8 & 6 & 7 \\ 10 & 3 & 8 & 0 & 6 & 4 \\ 8 & 7 & 6 & 6 & 0 & 5 \\ 9 & 5 & 7 & 4 & 5 & 0 \end{bmatrix}$$

Weightes adjacency matrix for the outer cycle of graph

$$B=\begin{bmatrix} 0 & 11 & 0 & 0 & 0 & 9 \\ 11 & 0 & 9 & 0 & 0 & 0 \\ 0 & 9 & 0 & 8 & 0 & 0 \\ 0 & 0 & 8 & 0 & 6 & 0 \\ 0 & 0 & 0 & 6 & 0 & 5 \\ 9 & 0 & 0 & 0 & 5 & 0 \end{bmatrix}$$

Updated B with diagonal entries as extended ASCII code of message letters

$$B=\begin{bmatrix} 73 & 11 & 0 & 0 & 0 & 9 \\ 11 & 32 & 9 & 0 & 0 & 0 \\ 0 & 9 & 87 & 8 & 0 & 0 \\ 0 & 0 & 8 & 105 & 6 & 0 \\ 0 & 0 & 0 & 6 & 108 & 5 \\ 9 & 0 & 0 & 0 & 5 & 108 \end{bmatrix}$$

Resultant $N = A\text{x}B$ As

$$N = \begin{bmatrix} 202 & 415 & 788 & 1154 & 969 & 1012 \\ 848 & 202 & 807 & 429 & 799 & 674 \\ 673 & 365 & 145 & 876 & 731 & 849 \\ 799 & 278 & 723 & 100 & 668 & 552 \\ 706 & 366 & 633 & 678 & 61 & 612 \\ 712 & 322 & 686 & 506 & 564 & 106 \end{bmatrix}$$

Public key matrix

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

Length of minimum spanning tree:S=25

$C = N\text{xM}$

as

$$C=\begin{bmatrix} 202 & 617 & 1405 & 2559 & 3528 & 4540 \\ 848 & 1050 & 1857 & 2286 & 3085 & 3759 \\ 673 & 1038 & 1183 & 2059 & 2790 & 3639 \\ 799 & 1077 & 1800 & 1900 & 2568 & 3120 \\ 706 & 1072 & 1705 & 2383 & 2444 & 3056 \\ 712 & 1034 & 1720 & 2226 & 2790 & 2896 \end{bmatrix}$$

$\mathrm{C}_1 = \mathrm{mod}(C, S)$

As

$$C_1 = \begin{bmatrix} 2 & 17 & 5 & 9 & 3 & 15 \\ 23 & 0 & 7 & 11 & 10 & 9 \\ 23 & 13 & 8 & 9 & 15 & 14 \\ 24 & 2 & 0 & 0 & 18 & 20 \\ 6 & 22 & 5 & 8 & 19 & 6 \\ 12 & 9 & 20 & 1 & 15 & 21 \end{bmatrix}$$

$C_2 = Qutionet(C, S).$

$$C_2 = \begin{bmatrix} 8 & 24 & 56 & 102 & 141 & 181 \\ 33 & 42 & 74 & 91 & 123 & 150 \\ 26 & 41 & 47 & 82 & 111 & 145 \\ 31 & 43 & 72 & 76 & 102 & 124 \\ 28 & 42 & 68 & 95 & 97 & 122 \\ 28 & 41 & 68 & 89 & 111 & 115 \end{bmatrix}$$

Pass (C_1, C_2, A) as Cipher text and 'S' as Secret key to the Decoder

Now obtained

$D = SC_2 + C_1.$

as

$$D = \begin{bmatrix} 202 & 617 & 1405 & 2559 & 3528 & 4540 \\ 848 & 1050 & 1857 & 2286 & 3085 & 3759 \\ 673 & 1038 & 1183 & 2059 & 2790 & 3639 \\ 799 & 1077 & 1800 & 1900 & 2568 & 3120 \\ 706 & 1072 & 1705 & 2383 & 2444 & 3056 \\ 712 & 1034 & 1720 & 2226 & 2790 & 2896 \end{bmatrix}$$

$N = DM^{-1}$(where M is the Public Key)

as

$$N = \begin{bmatrix} 202 & 415 & 788 & 1154 & 969 & 1012 \\ 848 & 202 & 807 & 429 & 799 & 674 \\ 673 & 365 & 145 & 876 & 731 & 849 \\ 799 & 278 & 723 & 100 & 668 & 552 \\ 706 & 366 & 633 & 678 & 61 & 612 \\ 712 & 322 & 686 & 506 & 564 & 106 \end{bmatrix}$$

$B = A^{-1}N.$

as

$$B = \begin{bmatrix} 73.0000 & 11.0000 & -0.0000 & 0.0000 & 0.0000 & 9.0000 \\ 11.0000 & 32.0000 & 9.0000 & 0.0000 & 0.0000 & 0.0000 \\ 0.0000 & 9.0000 & 87.0000 & 8.0000 & 0.0000 & 0.0000 \\ 0.0000 & 0.0000 & 8.0000 & 105.0000 & 6.0000 & 0.0000 \\ 0 & 0.0000 & 0.0000 & 6.0000 & 108.0000 & 5.0000 \\ 9.0000 & 0.0000 & 0.0000 & 0 & 5.0000 & 108.0000 \end{bmatrix}$$

with digonal entries

75 32 87 105 108 108

character equivalent of these extended ASCII code is the Decoded message

'I Will'

.

CONCLUSION

In this study, we have provided a novel cryptographic technique that combines the division algorithm with graph theoretical features to produce a reliable and extremely secure means of

sending secret data. The method gives a new layer of encryption that greatly improves data security and confidentiality in communication networks by combining these two different mathematical ideas.

REFERENCES

1. Rivest, R. L., Shamir, A., and Adleman, L. (1978): A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, Vol. 21(2), pp.120–126.
2. Katz, J., and Lindell, Y. (2007): *Introduction to Modern Cryptography*, CRC Press.
3. Paar, C., and Pelzl, J. (2010): *Understanding Cryptography: A Textbook for Students and Practitioners*, Springer.
4. Bing. Y, Zhang Z .and Wang J. (2010): Some results on spanning trees. Acta *Mathematicae Applicatae Sinica*, English Series, Vol. 26 (4), pp.607-616, DOI:10.1007/s10255-010-0011-4.
5. Mathur, A. (2012): An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms, *International Journal on Computer Science and Engineering*, Vol.4(9), pp.1650-1657.
6. Mahmood, M.K., and Shehab, J.N. (2014).: Image Encryption and Compression Based on Compressive Sensing and Chaos, *International Journal of Computer Engineering & Technology*, Vol.5(1),pp. 68-84.
7. Rajput, Y., Naik, D., and Mane, C. (2014): An Improved Cryptographic Technique to Encrypt Text using Double Encryption. *International Journal of Computer Applications*, Vol. 86(6).
8. Gorabal, V., and Manjaiah , D. H. (2014):Image Encryption Approach for Security Issues, *International Journal of Information Technology and Management Information System (IJITMIS)*, Vol. 5(2), pp.59-64.
9. Khalaf, A.A.M., Karim M.S.A., and Hamed , H.F.A. (2016).:A Triple Hill Cipher Algorithm Proposed to Increase the Security of Encrypted Binary Data and its Implementation Using FPGA, *ICACT Transactions on Advanced Communications Technology (TACT)*,Vol. 5(1) ,pp.752-759.
10. Goutham, V., Kethavath, L., and Swetha, K. (2016): Key Aggregate Searchable Encryption with Secure and Efficient Data Sharing In Cloud, *International Journal of Computer Engineering and Technology*,Vol. 7(4), pp.41–47.
11. Sampathkumar, A. (2017): Entry Structure for A Few Queries in Attribute Founded Encryption, *International Journal of Mechanical Engineering and Technology*, Vol.8(8), pp.1656–1661.
12. Srinivas, K., and Manjunath, A. S. (2018): A Survey on Hybrid Cryptographic Algorithms for Data Security, *Journal of Computer Applications*, Vol. 40(1), pp. 34–42.
13. Kumari, M., and Kirubanad, V.B. (2018): Data Encryption and Decryption Using Graph Plotting. *International Journal of Civil Engineering and Technology*, Vol.9(2), pp.36-46.
14. Boneh, D., and Shoup, V. (2020): *A Graduate Course in Applied Cryptography,* Stanford University.
15. Bashir, A. M.,and Hussain, A. (2021): *A Survey on Lightweight Cryptography for IoT Applications*, IEEE Access, Vol.9, pp.12333–12349.
16. Sullivan, L. (2022) : The Importance of Encryption for Database Security,*Database Security Journal*, Vol.18(3), pp.22–28.

17. Shaik, V., and Natarajan, K. (2022): Flexible and cost-effective cryptographic encryption algorithm for securing unencrypted database files at rest and in transit, *Methods X*, **Elsevier**, *Vol.9*, https://doi.org/10.1016/j.mex.2022.101924.
18. Verma, R., Kekre, P., and Acharya, K. (2023) : Cryptanalysis Using Laplace Transform of Error Function, *Jñānābha*, Vol.53(1), pp.106–109.
19. Chen, Y., Hu, T., Lou, F., Yin, M., Zeng, T., Wu, G., and Wang, H. (2024): A knowledge graph-based consistency detection method for network security policies, *Applied Sciences,* Vol.*14*(3), pp.1295. https://doi.org/10.3390/app14031295.
20. Gena, H., and Gupta, B. (2024): Graph-Based Encryption and Decryption Algorithm in Symmetric Key Cryptography, *Frontiers in Health Informatics*, Vol.13(8),pp.947-955.
21. Li, J., Sun, H., Du, Z., Wang, Y., Yuan, K., and Jia, C. (2025): A generic cryptographic algorithm identification scheme based on ciphertext features, *Journal of Information Security and Applications*, Vol.89**, doi.** 10.1016/j.jisa.2025.103984

[1, 2, 3] *Department of Mathematics, Medi-Caps University, Pigdamber, Rau-453331,Madhya Pradesh India.*

Email: keerti.sharma@medicaps.ac.in,
Email: rinku.verma@medicaps.ac.in,
Email: pranjali.kekre@medicaps.ac.in

(Received, April 12, 2025),
(Revised, May 02, 2025)