Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 7s (2025)

Graph - Based Innovations in Cryptographic Security

Slashi Leel [1], Dr. Sweta Srivastav [2] and Dr. Sangeeta Gupta [3]
[1,2,3] Department of Mathematics, Sharda University, Greater Noida, Uttar Pradesh 201310, India
[1] 2022301198.slashi@dr.sharda.ac.in
[2] sweta.srivastav@sharda.ac.in (corresponding author)
[3] sangeeta.gupta@sharda.ac.in

Article History:

Received: *27-10-2024*

Revised:*11-11-2024*

Accepted:*19-12-2024*

Abstract:

Cryptography focuses on securely transmitting messages from one party to another, ensuring that an unauthorized third party cannot comprehend them. To achieve this, various mathematical concepts, particularly from Graph Theory, have been incorporated into cryptographic techniques for more secure data transmission. The process of converting the original plain-text message into an unreadable cipher-text is known as encryption, while converting the cipher-text back to the original plain-text is referred to as decryption. Graph Theory is essential in numerous fields, particularly in cryptography, where its properties and straightforward matrix representation in computers make it highly valuable. In this paper the encryption and decryption process has been made more safer by using adjacent matrix of complement graph. **Introduction**: In today's digital communication landscape, ensuring secure data transmission is essential, and cryptography plays a vital role in safeguarding sensitive information. Graph theory, with its intricate structures and concepts, offers innovative frameworks for creating robust encryption methods. This research explores using adjacency matrices, graph complements, and disjoint graphs to develop secure cryptographic systems. By leveraging graph complements and structural complexities, these methods obscure messages, enhancing resistance to cryptographic attacks. Applications range from securing communication channels to enhancing blockchain privacy. Building on previous studies, this work demonstrates the potential of graph-theory-based cryptography in addressing modern security challenges effectively.

Objectives: This research aims to develop cryptographic techniques using graph theory concepts like adjacency matrices and graph complements to enhance encryption security and complexity, creating systems resistant to attacks with applications in secure communication, data protection, and blockchain technology.

Methods: This study utilizes graph theory to develop cryptographic techniques by encoding messages using graph complements, adjacency matrices, and adjoint matrices. Single words are represented as graph complements, while multi-word messages are encoded using disjoint graphs for each word. Encryption and decryption leverage matrix operations, enhancing security through graph structure complexity.

Results: The study demonstrates that incorporating graph theory, specifically adjacency matrices of complement graphs, enhances the encryption and decryption processes by adding layers of structural complexity. This approach effectively obscures the original message, making it more resistant to cryptographic attacks. The results highlight the potential of graph-based methods in achieving robust and secure data transmission.

Conclusions: This study demonstrates the potential of graph theory in cryptography, using graph complements, adjacency matrices, and disjoint graphs to enhance encryption and decryption. These methods leverage graph complexity to secure messages, providing a robust and innovative approach to advanced cryptographic techniques.

Keywords: Graph, Adjacency Matrix, Adjoint of a Matrix, Cryptography, Encryption, Decryption, Plain text, Cipher text, Complement of graph, Disjoint Matrix

1. Introduction

In the modern era of digital communication, ensuring the security of data transmission is crucial. Cryptography, the art of secure communication, protects sensitive information from unauthorized access and tampering. This research explores using graph theory, specifically adjacency matrices and graph complements, to develop robust cryptographic techniques.

Graph theory, with its rich set of concepts, provides a versatile framework for creating complex encryption schemes. We use adjacency matrices and graph complements to generate intricate cipher systems resistant to common cryptographic attacks. For single-word messages, we utilize the complement of a graph, its adjacency matrix and adjoint of a matrix for both encryption and decryption, leveraging the structural complexity of graph complements to obscure the original message securely. For messages with two or more words, we employ a disjoint matrix of complement graph of each word in a sentence , treating each word as a separate complete graph and representing spaces by disjoint segments i.e. zero within the matrix. The inherent complexity of graph structures makes it challenging for adversaries to decipher encoded messages without the proper key. The use of graph complements and disjoint graphs further obfuscates the data, adding layers of security.

Graph-theory-based cryptographic techniques have numerous applications, including securing communication channels, protecting sensitive data, and ensuring the integrity of information. They can enhance digital signatures and be applied in blockchain technology to safeguard transactions and maintain user privacy.

In conclusion, integrating graph theory into cryptography offers promising avenues for developing advanced encryption methods. This research aims to explore these methodologies, demonstrating their potential and efficacy in real-world cryptographic applications. Previous studies have shown various applications and methodologies in this field, such as a graph theory approach on cryptography [1], antimagic labeled graphs for cryptographic applications [2], and the application of graph theory in secure communication [3,4]. Additional research has focused on specific graph types for encryption [5], solving cryptographic problems using graph theory [6], graph-based encryption schemes [8] and cryptography is also discussed using python [7]. These works provide a solid foundation for further exploration and development in this area .

2. Objectives

The objective of this research is to explore and develop novel cryptographic techniques leveraging graph theory concepts, such as adjacency matrices, graph complements, and disjoint graphs, to enhance the security and complexity of encryption methods. By utilizing the structural intricacies of graphs, the study aims to create encryption systems that are resistant to common attacks, with potential applications in secure communication, data protection, and blockchain technology.

Methods

This study employs graph theory for cryptography by using adjacency matrices, graph complements, and adjoint matrices for encryption and decryption. Single-word messages are encoded with complement graphs, while multi-word messages use disjoint graphs with spaces represented as zero segments. These techniques enhance message security through graph-based structural complexity.

3. Results

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9
K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19
U	V	W	X	Y	Z				
20	21	22	23	24	25				

Table 1: Numerical Representation of the alphabet

A	B	C	D	E	F	G	H	I	J
65	66	67	68	69	70	71	72	73	74
K	L	M	N	O	P	Q	R	S	T
75	76	77	78	79	80	81	82	83	84
U	V	W	X	Y	Z				
85	86	87	88	89	90				

Table 2: ASCII value representation of the alphabets

0	1	2	3	4	5	6	7	8	9
48	49	50	51	52	53	54	55	56	57

Table 3: ASCII value representation of the numbers

THEOREM 2.1: Algorithm for encryption and decryption of a message.

Proof: To encrypt and decrypt the message we will proceed with the following two cases:

CASE I- Algorithm for encryption and decryption for a single code message.

The message will be encrypted using the complement graph and the adjoint of a matrix. The message can be a combination of alphabets and numbers. The secret code required for decryption will be securely sent to the receiver, ensuring that only the intended recipient can access the original message.

Algorithm for encryption:

To initiate the encryption algorithm, follow the following steps-

1. Convert each and every alphabet and number into its ASCII value.
2. Apply the shift cipher as (Numerical Value + 4)mod26
3. Let a_1, a_2, a_3,………., a_n be the variables assigned to the values.
4. Construct a complete graph with the number of vertices equivalent to the length of the text i.e. C_n
5. Construct the complement to the above graph i.e. C'_n this is a key-value graph.
6. Convert the graph into an adjacency matrix.
7. Find the adjoint matrix of the adjacency matrix obtained in step 6.
8. Add a_1, a_2, a_3, ………. a_n to the 1^{st}, 2^{nd},.........., n^{th} column respectively of the adjoint matrix. Let this new matrix be B.
9. List all the elements of the matrix row by row in a list separately. For any number in the list that is 10 or more, convert it to the corresponding alphabet from the standard table.
10. Send the above list of matrices along with the key-value graph and key operation to the receiver. Additionally, notify the receiver of the positions of the numeric digits in the code to ensure that the key operation is not performed at those locations.

Algorithm for decryption:

To initiate the decryption algorithm, follow the following steps-

1. Examine the code for any alphabets. If any alphabets are found, convert them to their corresponding numbers from the standard table. Also form the adjacency matrix from the key-value graph.
2. Organize the code into an n x n matrix, where n represents the number of elements in the code, arranging them row by row.
3. Find the adjoint matrix of the adjacency matrix obtained in step 1.

Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 7s (2025)

4. Subtract the adjoint matrix obtained in step3 from the matrix obtained in step2.
5. Identify and extract the common element present in each column.
6. Execute the operation N.V. + 9(mod26) on each value, excluding the positions of the digits specified by the sender. Refer to the standard table to obtain the corresponding results.
7. Thus, the original text is revealed.

Example: Using the above algorithm, we will encrypt and decrypt the code **"T4A9P"**

ENCRYPTION

The initial step is to transform each letter into its corresponding numerical value using ASCII index values.

T	4	A	9	P
84	52	65	57	80

By applying the given cipher N.V. +4 (mod26) , we obtain the following numerical values for the text.

T	4	A	9	P
10	4	17	9	6

Assign the variables $\{a_1, a_2, a_3, \ldots\ldots\ldots, a_n\}$ to the values

10	4	17	9	6
a_1	a_2	a_3	a_4	a_5

Construct a complete graph with the number of vertices equivalent to the length of the text i.e. C_5

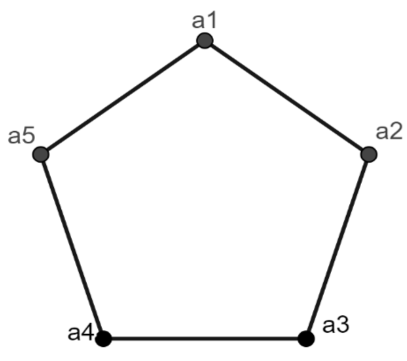

Figure 1: Complete Graph C_5

Construct the complement of C_5 i.e. C'_5 this is a key-value graph and we will keep the graph for future use.

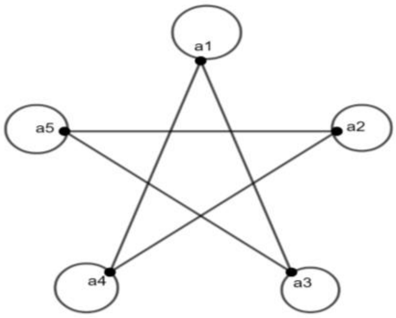

Figure 2: Complement of C_5 i.e. C'_5

Converting the above graph into an adjacency matrix. Let A be that matrix -

A =

	a_1	a_2	a_3	a_4	a_5
a_1	1	0	1	1	0
a_2	0	1	0	1	1
a_3	1	0	1	0	1
a_4	1	1	0	1	0
a_5	0	1	1	0	1

Finding the adjoint matrix of the above matrix A

$$\text{adj}(A) = \begin{bmatrix} 1 & -1 & 1 & 0 & 0 \\ -1 & 1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & -1 \\ -1 & 1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & -1 \end{bmatrix}$$

Add the value of $\{a_1, a_2, a_3, a_4, a_5\}$ to each matrix column of matrix adj(A) respectively, and we will get a new matrix B -

$$B = \begin{bmatrix} 11 & 3 & 18 & 9 & 6 \\ 9 & 5 & 16 & 10 & 7 \\ 11 & 3 & 18 & 8 & 5 \\ 9 & 5 & 16 & 10 & 7 \\ 11 & 3 & 18 & 8 & 5 \end{bmatrix}$$

Convert the elements of the above matrix row-wise into the form of a list as below -

[11 3 18 9 6 9 5 16 10 7 11 3 18 8 5 9 5 16 10 7 11 3 18 8 5]

In the above code, replace the number which is more than 10 or 10 with an alphabet from the standard table.

[L 3 S 9 6 9 5 Q K 7 L 3 S 8 5 9 5 Q K 7 L 3 S 8 5]

Send this code to the receiver and the key-value graph along with the key operation N.V.+ 9 (mod26). Also, inform the receiver that the positions to be considered are the 2nd and 4th.

DECRYPTION

Convert the alphabet into its numerical value from the standard table as shown below. Also construct the adjacency matrix from the key-value graph. Let C be that matrix -

[11 3 18 9 6 9 5 16 10 7 11 3 18 8 5 9 5 16 10 7 11 3 18 8 5]

$$C = \begin{bmatrix} & a_1 & a_2 & a_3 & a_4 & a_5 \\ a_1 & 1 & 0 & 1 & 1 & 0 \\ a_2 & 0 & 1 & 0 & 1 & 1 \\ a_3 & 1 & 0 & 1 & 0 & 1 \\ a_4 & 1 & 1 & 0 & 1 & 0 \\ a_5 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

Organize the above code into a 5x5 matrix. Let D be that matrix -

$$D = \begin{bmatrix} 11 & 3 & 18 & 9 & 6 \\ 9 & 5 & 16 & 10 & 7 \\ 11 & 3 & 18 & 8 & 5 \\ 9 & 5 & 16 & 10 & 7 \\ 11 & 3 & 18 & 8 & 5 \end{bmatrix}$$

Find the adjoint matrix of the above obtained matrix C

$$adj(C) = \begin{bmatrix} 1 & -1 & 1 & 0 & 0 \\ -1 & 1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & -1 \\ -1 & 1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & -1 \end{bmatrix}$$

Now perform the subtraction i.e. Matrix D - adj(C). Let the obtained matrix be E

$$E = \begin{bmatrix} 10 & 4 & 17 & 9 & 6 \\ 10 & 4 & 17 & 9 & 6 \\ 10 & 4 & 17 & 9 & 6 \\ 10 & 4 & 17 & 9 & 6 \\ 10 & 4 & 17 & 9 & 6 \end{bmatrix}$$

Now, extract the common numbers from each column. The numbers are:

[10 4 17 9 6]

Apply the key operation: N.V. + 9 (mod 26) and refer to the standard table to determine the value. Note that since the positions are the 2nd and 4th, this operation will not be applied to the digits in these locations. Consequently, the original message is revealed as:

“T 4 A 9 P”

CASE II- Algorithm for encryption and decryption for a sentence message.

The message will be encrypted using the complement graph, matrix of disjoint graphs and the adjoint of a matrix. The space between the words is always considered to be zero and no operation needs to be performed for the space value zero during the encryption and decryption process. The message will contain only alphabets. The secret code required for decryption will be securely sent to the receiver, ensuring that only the intended recipient can access the original message.

Algorithm for encryption:

To initiate the encryption algorithm, follow the following steps-

1. Convert each and every alphabet into its ASCII value and consider the space between the words as zero.
2. Apply the shift cipher as (Numerical Value + 4)mod26 except for the space value which is zero.
3. Let a_1, a_2, a_3,………., a_n be the variables assigned to the values.
4. For each word in the sentence, construct a complete graph with a number of vertices equal to the number of letters in the word.
5. Next, determine the complement graphs for each complete graph formed in the previous step. These are key-value graphs and will be kept for future use.
6. Determine the adjacency matrix for each complement graph formed in the previous step.
7. Now, combine all the adjacency matrices into a single square matrix, resulting in a new matrix that represents the disjoint graphs.
8. Determine the adjoint matrix of the resulting matrix from the previous step.
9. Add a_1, a_2, a_3, ………. a_n to the 1^{st}, 2^{nd},.........., n^{th} column respectively of the adjoint matrix.
10. List all the elements of the matrix row by row in a list separately. For any number in the list that is 10 or more, convert it to the corresponding alphabet from the standard table.
11. Send the above list of matrices along with the key-value graphs and key operation to the receiver.

Algorithm for decryption:

To initiate the decryption algorithm, follow the following steps-

1. Examine the code for any alphabets. If any alphabets are found, convert them to their corresponding numbers from the standard table. Also form the corresponding adjacency matrix from all the key-value graphs.
2. Organize the code into an n x n matrix, where n represents the number of elements in the code, arranging them row by row.
3. Now, combine all the adjacency matrices into a single disjoint square matrix, resulting in a new matrix that represents the disjoint graphs.
4. Determine the adjoint matrix of the resulting matrix from the previous step.
5. Subtract the adjoint matrix obtained in step4 from the matrix obtained in step2.
6. Identify and extract the common element present in each column.

7. Perform the operation N.V. + 9 (mod 26) on each value and refer to the standard table for the corresponding result and consider 0 as a space between the words.
8. Thus, the original text is revealed.

Example: Using the above algorithm, we will encrypt and decrypt the code **"THE KITE"**

ENCRYPTION

The first step is to convert each letter into its ASCII numerical value. Spaces between words are treated as zeros, and no operation is needed for these zeros.

T	H	E		K	I	T	E
84	72	69	0	75	73	84	69

Apply the shift cipher using the formula N.V + 4 (mod26) to all values, excluding the zeros that represent spaces.

T	H	E		K	I	T	E
10	24	21	0	1	25	10	21

Assign the variables $\{a_1, a_2, a_3, \ldots\ldots\ldots, a_n\}$ to the values

10	24	21	0	1	25	10	21
a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8

Next, we need to construct a complete graph for each word in the sentence. Here, C_3 will be created for the word "THE" and C_4 will be created for the word "KITE."

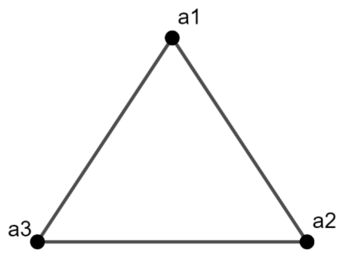

Figure 3: Complete Graph C_3

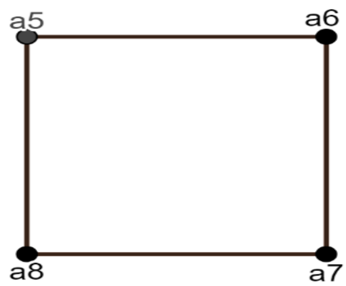

Figure 4: Complete Graph C_4

Construct the complement of C_3 i.e. C'_3 and C_4 i.e. C'_4 this is a key-value graph and we will keep the graph for future use.

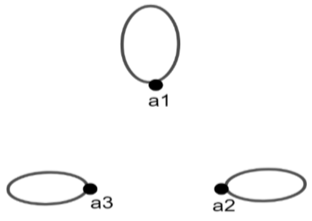

Figure 5: Complement of C_3 i.e. C'_3

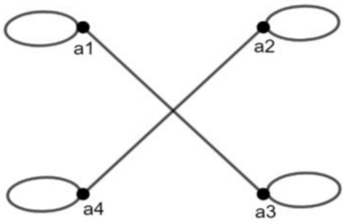

Figure 6: Complement of C_4 i.e. C'_4

Next, we need to transform the two graphs mentioned above into their corresponding adjacency matrices.

$$A = \begin{bmatrix} & a_1 & a_2 & a_3 \\ a_1 & 1 & 0 & 0 \\ a_2 & 0 & 1 & 0 \\ a_3 & 0 & 0 & 1 \end{bmatrix}$$

$$B = \begin{bmatrix} & a_5 & a_6 & a_7 & a_8 \\ a_5 & 1 & 0 & 1 & 0 \\ a_6 & 0 & 1 & 0 & 1 \\ a_7 & 1 & 0 & 1 & 0 \\ a_8 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Now, merge the adjacency matrices, namely matrix A and matrix B, into a single square matrix. This will produce a new matrix C, which represents the disjoint graphs.

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

Find the adjoint matrix of the above obtained matrix C

$$
\text{adj}(C) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \end{bmatrix}
$$

Add the value of $\{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8\}$ to each matrix column of matrix adj(C) respectively, and we will get a new matrix D -

$$
D = \begin{bmatrix} 11 & 24 & 21 & 0 & 1 & 25 & 10 & 21 \\ 10 & 25 & 21 & 0 & 1 & 25 & 10 & 21 \\ 10 & 24 & 22 & 0 & 1 & 25 & 10 & 21 \\ 10 & 24 & 21 & 0 & 1 & 25 & 10 & 21 \\ 10 & 24 & 21 & 0 & 0 & 25 & 11 & 21 \\ 10 & 24 & 21 & 0 & 1 & 24 & 10 & 22 \\ 10 & 24 & 21 & 0 & 2 & 25 & 9 & 21 \\ 10 & 24 & 21 & 0 & 1 & 26 & 10 & 20 \end{bmatrix}
$$

Convert the elements of the above matrix row-wise into the form of a list as below -

[11 24 21 0 1 25 10 21 10 25 21 0 1 25 10 21 10 24 22 0 1 25 10 21 10 24 21 0 1 25 10 21 10 24 21 0 0 25 11 21 10 24 21 0 1 24 10 22 10 24 21 0 2 25 9 21 10 24 21 0 1 26 10 20]

In the above code, replace the numbers which are more than 10 or 10 with an alphabet from the standard table.

[L Y V 0 1 Z K V K Z V 0 1 Z K V K Y W 0 1 Z K V K Y V 0 1 Z K V K Y V 0 0 Z L V K Y V 0 1 Y K W K Y V 0 2 Z 9 V K Y V 0 1 A K U]

Send this code to the receiver and the key-value graph along with the key operation N.V.+ 9 (mod26)

DECRYPTION

Convert the alphabet into its numerical value from the standard table as shown below. Also construct the adjacency matrices from the key-value graphs. Let A and B be that matrix -

[11 24 21 0 1 25 10 21 10 25 21 0 1 25 10 21 10 24 22 0 1 25 10 21 10 24 21 0 1 25 10 21 10 24 21 0 0 25 11 21 10 24 21 0 1 24 10 22 10 24 21 0 2 25 9 21 10 24 21 0 1 26 10 20]

$$A = \begin{bmatrix} & a_1 & a_2 & a_3 \\ a_1 & 1 & 0 & 0 \\ a_2 & 0 & 1 & 0 \\ a_3 & 0 & 0 & 1 \end{bmatrix}$$

$$B = \begin{bmatrix} & a_5 & a_6 & a_7 & a_8 \\ a_5 & 1 & 0 & 1 & 0 \\ a_6 & 0 & 1 & 0 & 1 \\ a_7 & 1 & 0 & 1 & 0 \\ a_8 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Organize the above code into a 8x8 matrix. Let C be that matrix -

$$C = \begin{bmatrix} 11 & 24 & 21 & 0 & 1 & 25 & 10 & 21 \\ 10 & 25 & 21 & 0 & 1 & 25 & 10 & 21 \\ 10 & 24 & 22 & 0 & 1 & 25 & 10 & 21 \\ 10 & 24 & 21 & 0 & 1 & 25 & 10 & 21 \\ 10 & 24 & 21 & 0 & 0 & 25 & 11 & 21 \\ 10 & 24 & 21 & 0 & 1 & 24 & 10 & 22 \\ 10 & 24 & 21 & 0 & 2 & 25 & 9 & 21 \\ 10 & 24 & 21 & 0 & 1 & 26 & 10 & 20 \end{bmatrix}$$

Now, merge the adjacency matrices A and B into a single disjoint square matrix, forming a new matrix D that represents the combined disjoint graphs.

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

Find the adjoint matrix of the above obtained matrix D

$$adj(D) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \end{bmatrix}$$

Subtract the adjoint matrix D from the matrix C and obtain a new matrix E

$$E = \begin{bmatrix} 10 & 24 & 21 & 0 & 1 & 25 & 10 & 21 \\ 10 & 24 & 21 & 0 & 1 & 25 & 10 & 21 \\ 10 & 24 & 21 & 0 & 1 & 25 & 10 & 21 \\ 10 & 24 & 21 & 0 & 1 & 25 & 10 & 21 \\ 10 & 24 & 21 & 0 & 1 & 25 & 10 & 21 \\ 10 & 24 & 21 & 0 & 1 & 25 & 10 & 21 \\ 10 & 24 & 21 & 0 & 1 & 25 & 10 & 21 \\ 10 & 24 & 21 & 0 & 1 & 25 & 10 & 21 \end{bmatrix}$$

Now, extract the common numbers from each column. The numbers are:

[10 24 21 0 1 25 10 21]

Apply the key operation: N.V. + 9 (mod 26) and refer to the standard table to determine the value and consider 0 as a space between the words. Consequently, the original message is revealed as:

"THE KITE"

4. Discussion

In conclusion, our research demonstrates the effectiveness of leveraging graph theory in cryptography, specifically through the use of graph complements, adjacency matrices, and adjoints of matrices for encryption and decryption. By utilizing the structural intricacies of graph complements, we successfully obscure single-word messages, enhancing security through inherent graph complexity. For multi-word messages, the application of disjoint matrices for each word, treated as separate complete graphs, further complicates the cryptographic process, with spaces represented by zero segments within the matrix. This method robustly secures encoded messages, making it significantly challenging for adversaries to decipher without the appropriate key. Our findings underscore the potential of graph theory to contribute to advanced cryptographic techniques, offering a novel approach to secure communication.

References

[1] Nandhini, R., Maheswari, V. and Balaji, V.(2018) 'A Graph Theory Approach on Cryptography', *Journal Of Computational Mathematica*, 2(1), pp. 97-104.

[2] Gurjar, D.K. and Krishnaa, A.(2022) 'Various Antimagic Labeled Graphs from Graph Theory for Cryptography Applications', *International Journal of Scientific Research in Mathematical and Statistical Sciences*, 9(3), pp. 11-18.

[3] Amudha, P., Charles Sagayaraj, A.C. and Shantha Sheela, A.C.(2018) 'An Application of Graph Theory in Cryptography', *International Journal of Pure and Applied Mathematics*, 119(13), pp. 375-383.

[4] Kaur, G. and Tripathi, N.(2021) 'Applying Graph Theory to Secure Data by Cryptography', *International Journal of Linguistics and Computational Applications (IJLCA)*, 8(1), pp. 1-3

[5] Krishnaa, A.(2021) 'Certain Specific Graphs in Cryptography', *Advances and Applications in Discrete Mathematics*, 26(2), pp. 157-177

[6] Chowdhury, S., Ghosh, P. and Jana, M.(2020) 'An Approach of Graph Theory for Solving Cryptographic Problem', *BKGC Scholars*, 1(2), pp. 64-68.

[7] Lalitha, M. and Vasu, S.(2023) 'A Study on Graph Theory in Cryptography Using Python', *Journal of Emerging Technologies and Innovative Research (JETIR)*, 10(4), pp. 97-107

[8] Ni, B., Qazi, R., Ur Rehman, S. and Farid, G.(2021) 'Some Graph-Based Encryption Schemes', *Hindawi Journal of Mathematics*, pp. 1-8