An Encryption Technique Using A Star Graph With A Self-Invertible Matrix

Final Year Project Report

Presented by

Abid Hussain, Muhammad Irfan

CIIT/SP21-BSM-011/VHR, CIIT/FA20-BSM-016/VHR

In Partial Fulfillment

of the Requirment for the Degree of

Bachelor of Science in Mathematics

DEPARTMENT OF MATHEMATICS

COMSATS UNIVERSITY ISLAMABAD

Vehari Campus

Fall 2024

COMSATS UNIVERSITY ISLAMABAD
VEHARI CAMPUS

FINAL APPROVAL

This project titled

An Encryption Technique Using A Star Graph With A Self-Invertible Matrix

submitted to the Department of Mathematics

by

Name	Registration Number
Abid Hussain, Muhammad Irfan	CIIT/SP21-BSM-011/VHR, CIIT/FA20-BSM-016/VHR

in partial fulfillment of the requirements for the award of the degree of Bachelor of Science in Mathematics has been accepted.

Supervisor:

Mr. Nasir Ali .....
Lecturer
COMSATS University Islamabad
Vehari Campus.

External Examiner:

Dr. Anum Zehra .....
Assistant Professor
The Women University
Multan.

Head of the Department:

Dr. Hafiz Muhammad Asim Zafar .....
Associate Professor
COMSATS University Islamabad
Vehari Campus.

DECLARATION OF THE STUDENT

I, **Abid Hussain, Muhammad Irfan**, Registration Number **CIIT/SP21-BSM-011/VHR, CIIT/FA20-BSM-016/VHR** , hereby solemnly declare that I have produced the work presented in this project, during the scheduled period of study.

Date: **December 27, 2024** .....

Signature of the Student

COMSATS UNIVERSITY ISLAMABAD
VEHARI CAMPUS, PAKISTAN.

Students Name: Abid Hussain, Muhammad Irfan

Degree: BS **Date of Graduation:** Fall 2024

Thesis Title: An Encryption Technique Using A Star Graph With A Self-Invertible Matrix

CUI COPYRIGHT AGREEMENT

- I hereby certify that, if appropriate, I have obtained and attached hereto a written permission statement from the owner(s) of each third party copyrighted matter to be included in my project report, dissertation, or project report, allowing distribution as specified below.
- I certify that the version I submitting is the same as that approved by my examiners and CUI authorities.
- I agree to provide a copy to anyone who requests it.
- I also retain the right to use in future works (such as article or books) all or parts of this project report or record of study.

AVAILABILITY OPTIONS

1. ☑ Release the work immediately for worldwide access on the Internet.
2. ☐ (*Patent Hold*) Secure the work temporarily for patent and/or proprietary purpose, then release the work for worldwide access on the Internet.
3. ☐ (*Journal Hold*) Restrict full-text access for two years, then release the work for worldwide access on the Internet. (*Abstract will be available during embargo period*).

SUPERVISOR/CO-SUPERVISOR'S CERTIFICATION

I have discussed the availability choice with my student, and I am aware of the choice made by him/her.

Supervisor/Co-Supervisor's Signature: .....

AVAILABILITY OPTIONS & COPYRIGHT AGREEMENT

I have read and fully agree to the CUI copyright agreement regarding my project report. I agree to the project report availability option I selected above. I understand that the availability option is my choice and that there are publishing consequences to my selection.

Student's Signature: ..... **Date:** .....

Dedicated to my beloved parents and teachers

Contents

Acknowledgment

Praise is to ***Almighty Allah***, *WHO* is Lord of the world, the Answerer of prayers and the Source of peace, whose blessing and exaltation flourished to the scared wealth of knowledge.

Special praises and regards for His Last Messenger, Holy Prophet ***Hazrat Muhammad (PBUH)***. Holy Prophet said that I AM the light, whoever follows ME, will never be in the darkness.

I feel great pleasure in expressing my profound and heartiest gratitude to my supervisor **Mr. Nasir Ali**, for his indispensable guidance, deep consideration, affection and active co-operation that made possible this work to meet its end successfully well in time.

I would also like to thank HOD **Dr.Hafiz Muhammad Asim Zafar** and all respected **teachers** at Department of Mathematics, CIIT Vehari for providing us healthy academic environment. I am also thanks to **Mr. Nasir Ali** for helping me in this project report.

Abid Hussain & Muhammad Irfan

Abstract

In today's digital world, we must secure our messages and communication as cyber-attacks and hacking are becoming much more of a risk. The demand for advance encryption methods increases significantly as the internet and network communications evolve. The risk of interception is high when transmitting information, personal messages, images or data over unsecured channels. Mitigation of these threats requires cryptographic techniques, particularly encryption methods. In this thesis, we present an encryption technique which employs a star graph, adjacency matrix and a self invertible key matrix to encrypt and decrypt messages yielding a more complex ciphertext. With a self invertible matrix, the need of calculating the inverse at decryption stage reduces the computational complexity of the encryption.

Chapter 1

Introduction

Encryption is the conversion of information [1] into a code that is hard to decipher, and it has been around since the ancient Egyptian time, where hieroglyphs were encrypted to hide messages. The Spartans used a tool known as the scytale for Secret military communication, and Julius Caesar invented the Caesar Cipher where characters are shifted as a means of coding. With time, cryptography advanced and the next major cryptography system was the Vigenère Cipher that used multiple letter shifts with a keyword that was developed in the 1500s. In the present day, it has become a very crucial weapon in safeguarding information as well as communication in the electronic medium. Compared to other ciphers, the Hill Cipher applies linear algebra to a number of text blocks applying an invertible matrix, and it is more protected that plain substitution cryptanalysis. The Atbash Cipher is a simple substitution cipher where the alphabets are replaced by the use of its mirror image hence relatively easy to solve while the Caesar Cipher involves the shifting of the alphabets in the plaintext by a fixed number of places downwards with a shift of 3 positions changing "A" into "D."

A graph encompasses nodes or vertices [2] and edges that join two nodes, which may depict a relation between two objects or entities. There are two types of graphs, directed and undirected; by this means, edges have a direction while in the latter they have no direction. They are employed commonly, in such contexts as social networks – users and connections, transport networks – locations and routes, and computer networks – devices and data flows. In cryptography, the graph plays a significant role in modeling secure networks for communication. Applicants explained that such graphs as expander graphs, for example, are employed in encryption algorithms for security enhancement and optimization. Furthermore, graph-based concepts are used in cryptographic key exchange techniques to guarantee data integrity during transmission across networks.

Cryptography follows different techniques [3] and it has a history of how the different techniques have been developed. Speaking about the Caesar cipher, it should be noted that it was employed by Julius Caesar too, and it is based on shift of the alphabetic letters used as a code. The Vigenère cipher came as an

improvement because instead of using a single, fixed, number for the shifts, there was a keyword, leading to a polyalphabetic substitutive cipher. The cryptographic machine used by the Germans during the Second World War known as the Enigma machine was a mechanical device that used rotors and plugboards to encrypt the messages and was virtually uncrackable. The one-time pad provided the most secure means of encrypting a message when the key was a truly random key and of same length as the message. RSA encryption system was developed in the 1970s and provided the concept of public key cryptography and thus enabling the people to communicate securely without sending or receiving the keys. Each of these techniques provided foundation for modern cryptographic methods.

For the purpose of this thesis, we propose a new encryption scheme [4] that draws from graph theory and matrix algebra in order to strengthen the encryption of data. In detail, a star graph approach and self-invertible matrices are employed for more efficient and secure data encipherment. In the thesis, common graph differences are described, as well as some of them, such as directed, undirected, and Hamiltonian paths and the use of adjacency matrices. A lot of emphasis is placed on the generation of self inversing matrices, which have the property that the matrix used for decryption is always invertible. This method is then used under the context of the Hill Cipher and is enhanced with concepts from graph theory in order to build an effective encryption system that can be used to protect sensitive information in several fields.

The thesis consists of four chapters. The first chapter, "Introduction," gives an introduction of the topic and its significance. Chapter two, 'Preliminaries,' presents basic but crucial concepts and knowledge needed to understand the subject. The third chapter, "Literature Review," is a review of past research and other studies. The original findings and contributions made through this research are presented in the final chapter, "Main Results." It allows a logical flow from basic concepts towards the presentation of important results.

Chapter 2

Preliminaries

2.1 Basic Elements of Cryptography

Definition 2.1.1. Encryption

The process in which we convert the plaintext (readable form) into ciphertext (non-readable form) is called **Encryption**.

Definition 2.1.2. Plaintext

The readable message before encryption is called **plaintext.**

Definition 2.1.3. Ciphertext

The non-readable message after encryption is called **ciphertext**.

Definition 2.1.4. Decryption

The process in which we convert the ciphertext (non-readable form) into plaintext (readable form) is called **decryption.**

Definition 2.1.5. Cryptography

Cryptography is the process of converting the ordinary readable information into some form that can only be understood by the people authorized to read it. It protects data through encoding – converting the data into an unreadable code that can only be decoded by a specific code.

Example 2.1.6. Suppose you wish to convey a message "HELLO" to your friend besides this nobody else has to know it. You could shift each letter by 3 places in the alphabet:

- H becomes K
- E becomes H
- L becomes O
- L becomes O
- O becomes R

So "HELLO" becomes "KHOOR". Your friend, knowing the shift, can reverse it to read the original message. This is quite an elementary warning of what can be achieved through cryptography.

Definition 2.1.7. Symmetric Key Cryptography

As it was noted earlier in Symmetric Key Cryptography one key is used to encrypt the message and also to decrypt the message. This is chosen and is recognizable both by the sender and the receiver hence it has to be protected a lot. It is rather akin to having to set a password on the message and then be required to provide the same password to open the message.

Example 2.1.8. Symmetric Key cryptography can be understood as follows: supposing while sharing messages with you friend, you two decide to use a secret 'key' which can be; a number " 3", for instance. This number you apply in order to change the letters of your message.

For example, if your message is "CAT":

An additional shift adds 3 letters – C is replaced with F.

- A becomes D

- T becomes W

So "CAT" becomes "FDW". He knows that the secret number is 3, that is why he translates the letters back by 3 and he obtains the traditional message.

Definition 2.1.9. Asymmetric Key Cryptography

Asymmetric Key Cryptography uses two keys: an encryption key which is publicly available and a decryption key that is secret. While the public key can be provided to anybody with an intend to encrypt the message, only the owner of the private key can be allowed to decrypt the message hence making the communication more secure.

Example 2.1.10. This is done when you are making a purchase and entering your credit card details on a secure website to which you send the details over the Internet after the website has encrypted your information using its public key. This information can only be decrypted using the private key of the website and thus the safe transfer of your sensitive data from hackers.

Definition 2.1.11. Cipher

The process in which we transforms the original message or the plaintext into the ciphertext using its key is called Cipher. This technique employed in cryptography for work of encryption or decryption.

Definition 2.1.12. Symmetric Enciphering

Symmetric Enciphering is a basic way of cryptographic system where the same key is used in enciphering as well as deciphering. This method relies with the key that has to be offered by the two communicating parties to enable them to encoding and decoding the information.

Definition 2.1.13. Kinds of Symmetric Enciphering

Here are few kinds of Symmetric Enciphering given below:

Definition 2.1.14. Caesar Cipher

The Caesar Cipher is one of the oldest and simplest cipher to help to encrypt the message. In this technique the letters of the plain text are shifted to a fixed number of positions in the alphabet.

Example 2.1.15. Plaintext: HELLO

Shift: 4

To encrypt the message, shift each letter by 3 places in the alphabet:

H $\rightarrow$ L

E $\rightarrow$ I

L $\rightarrow$ P

L $\rightarrow$ p

O $\rightarrow$ S

So, the encrypted message (ciphertext) becomes: LIPPS

To decrypt it, you would shift each letter back by 4 places to get the original message: HELLO.

Definition 2.1.16. Atbash Cipher

Atbash cipher is a simple category of directed substitution cipher with key one; all the twenty six letters of the alphabetic set from A to Z and from Z to A are interchanged. It was intended for the transformation of the Hebrew alphabets; attribute to it can be modified in order to transform any alphabet.

Atbash is orderly technique for encryption and decryption where the alphebet is reversed. The first character changes its place with the last character; the second character changes its place with the position next to the last and so on.

Atbash Cipher Mapping:

A $\rightarrow$ Z

B $\rightarrow$ Y

C $\rightarrow$ X

D $\rightarrow$ W

E $\rightarrow$ V

...

X $\rightarrow$ C

Y $\rightarrow$ B

Z $\rightarrow$ A

Example 2.1.17. Plaintext: SECRET

Encrypting it using the Atbash Cipher:

S $\rightarrow$ H

E $\rightarrow$ V

C $\rightarrow$ X

R $\rightarrow$ I

E $\rightarrow$ V

T $\rightarrow$ G

So, the encrypted message (ciphertext) becomes: HVXIVG.

In the Atbash Cipher, encryption and decryption are the same process since reversing the alphabet twice returns you to the original message.

2.2 Fundamentals of Graph Theory and Linear Algebra

Definition 2.2.1. Graph

A graph G = (V,E) consists of a set of vertices V and a set of edges E, where each edge connects two vertices, representing relationships between entities.

Figure 2.1: Graph

Definition 2.2.2. Directed Graph

A directed graph is a network representation that uses a dot or vertex or node, and each existing link is represented by an arrow from one vertex to the other. It is often used to model one directional associations such as web links or tasks in a work flow.

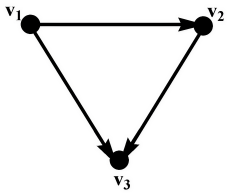

Figure 2.2: Directed Graph

Definition 2.2.3. Undirected Graph

Undirected graph is a special kind of connectivity which connects vertices where edges can hardly be described as oriented. It is applied to represent such types of relation when two objects are connected in equal measure such as friends or two cities connected by roads.

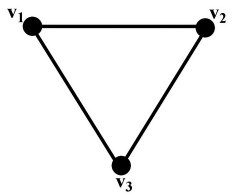

Figure 2.3: Undirected Graph

Definition 2.2.4. Complete Graph

A complete graph is defined by the graph in which all the points are connected to each other by a distinct line. This is an indication that each vertex is directly interacting with each other. In graph theory, it is often used when talking about a complete graph with n vertices: any two distinct vertices form an edge, and the total amount of them is equal to n(n – 1) / 2 edges.

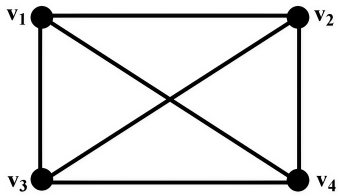

Figure 2.4: Complete Graph

Definition 2.2.5. Path

A path in a graph is the sequence of edges connecting a series of vertices, indicating a route from one vertex to another.In Path the vertices and edges are not used more than once.

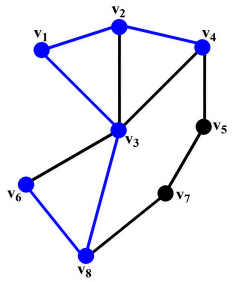

Figure 2.5: Path

In figure(2.5) $V_6 \rightarrow V_8 \rightarrow V_3 \rightarrow V_1 \rightarrow V_2 \rightarrow V_4$ is a path.

Definition 2.2.6. Hamiltonian Path

Hamiltonian path also known as the traceable path means any path in a predetermined graph that only passes through each vertex once.

Example 2.2.7. Consider a graph with the following vertices: A, B, C and D. Edges are: (A,B),(B,C),(C,D),(A,D). A possible Hamiltonian path in this graph could be:A→B→C→D. In this path A, B, C, D are vertices and each of them is visited only once.

Definition 2.2.8. Matrix

Matrix is a two dimensional structure containing numbers, symbols, characters arranged in rows as well as columns to create a rectangle shape.

Example 2.2.9. Let we have a matrix A which contains some rows and columns.

$$A = \begin{bmatrix} 3 & 2 & 0 \\ 8 & 4 & 7 \\ 9 & 6 & 10 \end{bmatrix} \tag{2.1}$$

We also have another matrix B, which is given below:

$$B = \begin{bmatrix} 2 & 3 & 8 & 1 \\ 12 & 6 & 9 & 0 \\ 7 & 0 & 2 & 8 \end{bmatrix} \tag{2.2}$$

This matrix have three rows and four columns.

Definition 2.2.10. Adjacency Matrix

An adjacency matrix is a two dimensional array; the element of the matrix states whether the two vertices are joined by an edge or not. If the graph has n vertices, the matrix is n×n, an element of the matrix is 1 if their are an edge between vertex i and vertex j otherwise the element is 0.

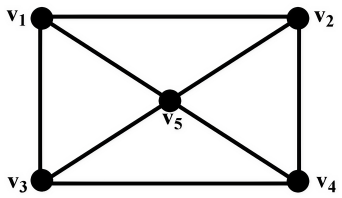

Figure 2.6: Adjacency Matrix Graph

Example 2.2.11. Let we have a graph which is given:
The adjacency matrix of above graph is

$$A = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{bmatrix} \tag{2.3}$$

Definition 2.2.12. Self-Invertible Matrix
Self-invertible matrix is a square matrix that is equal to its inverse matrix. This means that when the matrix is multiplied with itself, the product is an identity matrix. If A is member of the matrix set then A is self invertible if and only if A*A equals to an identity matrix I.

Example 2.2.13. Consider we have a matrix A. Now we check the given matrix is self-invertible or not.

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{2.4}$$

Now we check the given matrix is self-invertible or not.

$$A \times A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{2.5}$$

$$A \times A = \begin{bmatrix} (1 \times 1) + (0 \times 0) + (0 \times 0) \\ (0 \times 0) + (1 \times 1) + (0 \times 0) \\ (0 \times 0) + (0 \times 0) + (1 \times 1) \end{bmatrix} \tag{2.6}$$

$$A \times A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \mathbf{I} \tag{2.7}$$

This shows that **A** is self-invertible.

Definition 2.2.14. Generation of Self-Invertible Key Matrix

The self invertible matrix was generated by using the following procedure, consider any arbitrary $\frac{n}{2} \times \frac{n}{2}$ matrix M_{22} (since n being the order of adjacency matrix) with the help of M_{22} we can compute the remaining $\frac{n}{2} \times \frac{n}{2}$ matrices using the following properties.

$$M_{11}+M_{22}=0,\ M_{12}=\text{I-}M_{22},\ M_{21}=\text{I}+M_{22}$$

After computing M_{11},M_{12},M_{21},M_{22} the self-invertible matrix **M** was created by

$$\mathbf{M} = \begin{bmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{bmatrix} = \begin{bmatrix} m_{11} & m_{12} & ..... & m_{1n} \\ m_{21} & m_{22} & ..... & m_{2n} \\ ..... & & & \\ ..... & & & \\ m_{n1} & m_{n2} & ..... & m_{nn} \end{bmatrix} \tag{2.8}$$

Chapter 3

Literature Review

The need of cryptography in modeling complex structure on relationship has led to graph theory as a powerful based in cryptography. Because of their distinct central node and peripheral vertices, star graphs are a simple yet effective framework for encryption techniques and the natural hierarchical structure of encoding data makes them a subset of trees. Further, a more general concept of self invertible matrices in cryptography offers more security that does not require explicit inversion, resulting in decreased computational complexity. There has been previous work on graphs' adjacency matrices for various encryption techniques, but integration of star graphs with self invertible matrices is not well explored. The unique combination promises to lead to efficient and secure encryption methods. This work aims to contribute to the rapidly growing field of graph based cryptographic techniques by exploiting the structural properties of star graphs and the computational efficiency of self invertible matrices.

In the research paper, Acharya et al. [5] have discussed the latest methodologies for developing self-invertible. These matrices are suitable for Hill Cipher. This is an encryption technique which is usually applied in cryptography and which uses matrices to make messages secure. The authors narrow down on what they regard as a major issue with the Hill. For the matrix that is used to encrypt messages to qualify, it needs to be invertible. If it is not then decryption will not work! To solve this, the paper explores methods of creating self-ininvertible matrices as follows: This means that during decryption, and when one is in the process of looking for the inverse of a message, there will be less of a stir.

The objective that needs to be achieved in the proposed system is to ensure that each of the encryption matrices is invertible at all times. This way the results are faster and more reliable. To begin with, the paper outlines what cryptography entails in current day communication. In this regards, it describes the essence of the Hill Cipher as one of the monoalphabetic polygraphic substitution cipher. It then explains in detail how the Hill Cipher works, some of the modular arithmetic that is used, and those new techniques for constructing self-invertible matrices.

The authors are careful to clearly present the algorithm and present their methods with examples. Thus, the author of the paper concludes that these new methods are not only simpler than others in terms of calculations needed; they also do

much more than that. They can be also implemented together with other demands that refer to matrix inversion for various algorithms. This research enhances the technique of encrypting and decrypting messages using the Hill Cipher method, thereby making it efficient and secure.

Actually, graph theory [11] is used more actively in encryption. Many graphical presentations are useful in explaining the inter-connectivity that exists between various parts of a mathematical structure ; One type of such work is the study by proposing an encryption method based on graph labelling. This smart approach applies complete graphs anti-magic labeling. That's how securely encodes messages.

In graph labeling, attaching special integer to each vertex and each edge is the general form. This creates a strong way of keeping the encryption safe and for this, the graphs adjacency matrix of the message characters will be used. It starts with converting a simple text message into a graph. After that, it constructs a Minimum Spanning Tree (MST). In passing, let us say that the encoder of the MST reduces the complexity of the encoding process through matrix operations.

This work also presents a cryptographic algorithm, and that is incredible. It may have big advantages over old-fashioned methods because it can enclose complex data with principles form graph theory, including anti-magic labeling as well as MST. That's why it is suitable for use in network security systems.

Amudha et al.'s [6] algorithm has the advantage of using symmetric key cryptography. This means the same symmetric key is used by the sender and the receiver. This system is complimented with a specific encoding table that revolves around vital cryptographic objectives such as confidentiality, integrity and non-repudiation.

Towards the future, the authors make the following recommendations. Some people want to minimize the matrix on which they perform an encoding or increase security in the application of the public key encryption system. It could also be enhanced in a way that will increase the rate of encryption through segmentation of huge messages into little parts. All in all, impact of this research is tremendous on the field of cryptography. It demonstrates a new model to apply math structures for high security during data transfer at a network level!

The research paper [7] Encryption Using Double Vertex Graph and Matrices (2021) by authors Beaula C. and Venugopal P. presented a novel symmetric encryption technique proposed based on the ideas from graph theory like the double vertex graph. All of this is about better protection of the data in the cryptography based systems. That is why the need for it comes from the current digital environment where the protection of various pieces of information is crucial. Especially those like defense or finance, they require it very much.

That is why, in this thesis, simultaneously we will discuss a method of encrypting data with a common key and also graph-based structures.The mentioned graph structures are really much difficult to be penetrated by attackers. Because decryption needed deeper understanding of the graph theory. The encryption process builds the adjacency matrices from such graphs, and inserts a key matrix into it. It just basically just flips that whole process on it's head and uses the graph ideas in a similar fashion.

Using a star graph with a self invertible matrix to implement encryption technique, it addresses the need for efficient, lightweight and secure encryption systems thereby filling the critical gaps in cryptography. Structural complexity on the star graph is robust and is not easily vulnerable to brute force or structural attacks. Self invertible matrices are employed for key storage eliminating the vulnerability of a key exposure and for operational security. The combination of high randomness and diffusion in the ciphertext renders its cryptanalysis much easier. It is computationally efficient, and it can thus be used in resource constrained environments, e.g., IoT devices. The secure transformation properties also render it adaptable to evolving cryptographic standards, thus making it a very dependable choice for implementers of contemporary secure communication.

Chapter 4

An Encryption Technique Using A Star Graph With A Self-Invertible Matrix

The results of the thesis are presented in this chapter including the pseudocode for the encryption and decryption in the star graph. In the first section, we describe in detail the algorithms, from what steps are involved in the process of encryption to decryption. In the second section, implementation examples which use the proposed methods are presented to demonstrate their practical use. The algorithms demonstrated effectiveness in securing communication with these examples, and how they perform on different input data sets.

4.1 Pseudocode for Generating a Self-Invertible Matrix

The following pseudocode outlines the procedure to generate a self-invertible matrix M using a randomly generated matrix M_{22}. All matrix elements are computed modulo 128, and the matrix is verified to be self-invertible.

Input: Order of the matrix n

Step 1: Generate a random matrix M_{22} of size $n \times n$ with elements between 0 and 127

Step 2: Apply modulo 128 to each element of M_{22}

Step 3: Create the identity matrix I of size $n \times n$

Step 4: Compute the following matrices:

- $M_{11} = -M_{22} \pmod{128}$
- $M_{12} = I - M_{22} \pmod{128}$
- $M_{21} = I + M_{22} \pmod{128}$

Step 5: Construct the matrix M by combining M_{11}, M_{12}, M_{21}, and M_{22} as:

$$M = \begin{bmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{bmatrix}$$

Step 6: Compute the matrix product $M \times M$ and apply modulo 128 to each element

Step 7: Check if $M \times M = I \pmod{128}$

Step 8: If the condition is true, the matrix M is self-invertible

Output: The matrix M and the result of the self-invertibility check

4.1.1 Algorithms

Star Graph-Based Encryption Algorithm

- Transform the plaintext message into numerical values using the ASCII table.
- Assign these numerical values as weights to the edges of a star graph, where each plaintext character connects to the central vertex.
- Create the star graph in the form of an adjacency matrix.
- Generate an encrypted matrix by multiplying the adjacency matrix with a self-invertible key matrix.
- Share the encrypted matrix and relevant parameters over an unsecured channel.
- Use these parameters to allow the recipient to decrypt the matrix and retrieve the original plaintext message.

Star Graph-Based Decryption Algorithm

- Use the encrypted matrix and parameters for the matrix size and the key matrix shared over an insecure channel.
- Reconstruct the star graph's adjacency matrix using the provided information.
- Apply the self-invertible key matrix to the encrypted matrix to reverse the multiplication process performed during encryption.
- Obtain the original adjacency matrix with the correct path weights.
- Decode these weights back into their corresponding numerical values based on the sequence of weights and the structure of the star graph.

- Translate the numerical values into the original plaintext message using the ASCII table.

4.2 Implementation Examples

4.2.1 Example No.1

Suppose that User A(sender) wants to send the message "**CheMisTry**" to User B(receiver) using the technique of Encryption and Decryption.

Encryption Algorithm:
Encryption is done by the following steps

- **Conversion of Plaintext to ASCII Values**

Firstly, the sender converts the given message units "**CheMisTry**" into their numerical equivalent values that is using **ASCII Table:** C $\rightarrow$ 67, h $\rightarrow$ 104, e $\rightarrow$ 101, M $\rightarrow$ 77, i $\rightarrow$ 105, s $\rightarrow$ 115, T $\rightarrow$ 84, r $\rightarrow$ 114, y $\rightarrow$ 121.

- **Design the Graph and Construct the Adjacency Matrix**

Draw a graph where its all vertices are connected by sequential letters.

Compute the adjacency matrix for the above Star graph and denote it as 'P'

$$P = \begin{bmatrix} 0 & 67 & 104 & 101 & 77 & 105 & 115 & 84 & 114 & 121 \\ 67 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 104 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 101 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 77 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 105 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 115 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 84 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 114 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 121 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

- **Generating A Self-Invertible Matrix**

Now we need to compute the key matrix for that purpose we construct the self-invertible key matrix 'M' with the help of $\frac{n}{2}$ matrix M_{22}.

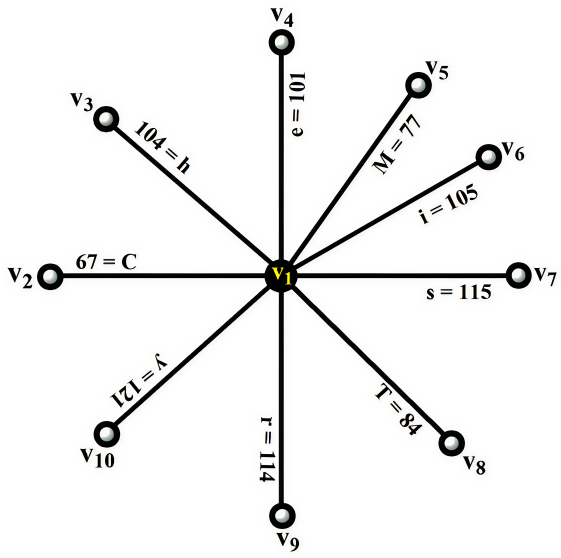

Figure 4.1: Star Graph

Let

$$M_{22} = \begin{bmatrix} 20 & 77 & 57 & 105 & 13 \\ 101 & 33 & 10 & 68 & 123 \\ 39 & 83 & 29 & 127 & 0 \\ 67 & 88 & 116 & 10 & 99 \\ 21 & 95 & 19 & 56 & 104 \end{bmatrix}$$

$$M_{12} + M_{22} = 0$$

$$M_{11} = \text{-}\ M_{22} + \text{mod } 128$$

$$M_{11} = \begin{bmatrix} 108 & 51 & 71 & 23 & 115 \\ 27 & 95 & 118 & 60 & 5 \\ 89 & 45 & 99 & 1 & 0 \\ 61 & 40 & 12 & 118 & 29 \\ 107 & 33 & 109 & 72 & 24 \end{bmatrix}$$

$$M_{12} = \text{I}\ \text{-}\ M_{22}$$

$$M_{12} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} - \begin{bmatrix} 20 & 77 & 57 & 105 & 13 \\ 101 & 33 & 10 & 68 & 123 \\ 39 & 83 & 29 & 127 & 0 \\ 67 & 88 & 116 & 10 & 99 \\ 21 & 95 & 19 & 56 & 104 \end{bmatrix} = \begin{bmatrix} -19 & -77 & -57 & -105 & -13 \\ -101 & -32 & -10 & -68 & -123 \\ -39 & -83 & -28 & -127 & 0 \\ -67 & -88 & -116 & -9 & -99 \\ -21 & -95 & -19 & -56 & -103 \end{bmatrix}$$

$$M_{12} = \begin{bmatrix} 109 & 51 & 71 & 23 & 115 \\ 27 & 96 & 118 & 60 & 5 \\ 89 & 45 & 100 & 1 & 0 \\ 61 & 40 & 12 & 119 & 29 \\ 107 & 33 & 109 & 72 & 25 \end{bmatrix}$$

Now we find M_{21}, $M_{21} = \mathrm{I} + M_{22}$

$$M_{21} = \begin{bmatrix} 21 & 77 & 57 & 105 & 13 \\ 101 & 34 & 10 & 68 & 123 \\ 39 & 83 & 30 & 127 & 0 \\ 67 & 88 & 116 & 11 & 99 \\ 21 & 95 & 19 & 56 & 105 \end{bmatrix}$$

Since the self-invertible key matrix 'M' is

$$M = \begin{bmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{bmatrix} = \begin{bmatrix} 108 & 51 & 71 & 23 & 115 & 109 & 51 & 71 & 23 & 115 \\ 27 & 95 & 118 & 60 & 5 & 27 & 96 & 118 & 60 & 5 \\ 89 & 45 & 99 & 1 & 0 & 89 & 45 & 100 & 1 & 0 \\ 61 & 40 & 12 & 118 & 29 & 61 & 40 & 12 & 119 & 29 \\ 107 & 33 & 109 & 72 & 24 & 107 & 33 & 109 & 72 & 25 \\ 21 & 77 & 57 & 105 & 13 & 20 & 77 & 57 & 105 & 13 \\ 101 & 34 & 10 & 68 & 123 & 101 & 33 & 10 & 68 & 123 \\ 39 & 83 & 30 & 127 & 0 & 39 & 83 & 29 & 127 & 0 \\ 67 & 88 & 116 & 11 & 99 & 67 & 88 & 116 & 10 & 99 \\ 21 & 95 & 19 & 56 & 105 & 21 & 95 & 19 & 56 & 104 \end{bmatrix}$$

- **Determining the product of matrices P and M**

Finally, we have to compute PM, this multiplication is known as the encrypted data of the original message.

$$C = P.M = \begin{bmatrix} 0 & 67 & 104 & 101 & 77 & 105 & 115 & 84 & 114 & 121 \\ 67 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 104 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 101 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 77 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 105 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 115 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 84 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 114 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 121 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 108 & 51 & 71 & 23 & 115 & 109 & 51 & 71 & 23 & 115 \\ 27 & 95 & 118 & 60 & 5 & 27 & 96 & 118 & 60 & 5 \\ 89 & 45 & 99 & 1 & 0 & 89 & 45 & 100 & 1 & 0 \\ 61 & 40 & 12 & 118 & 29 & 61 & 40 & 12 & 119 & 29 \\ 107 & 33 & 109 & 72 & 24 & 107 & 33 & 109 & 72 & 25 \\ 21 & 77 & 57 & 105 & 13 & 20 & 77 & 57 & 105 & 13 \\ 101 & 34 & 10 & 68 & 123 & 101 & 33 & 10 & 68 & 123 \\ 39 & 83 & 30 & 127 & 0 & 39 & 83 & 29 & 127 & 0 \\ 67 & 88 & 116 & 11 & 99 & 67 & 88 & 116 & 10 & 99 \\ 21 & 95 & 19 & 56 & 105 & 21 & 95 & 19 & 56 & 104 \end{bmatrix}$$

$$C = PM = \begin{bmatrix} 52740 & 58120 & 52985 & 59129 & 44613 & 52635 & 58072 & 53005 & 59116 & 44569 \\ 7236 & 4757 & 4757 & 7705 & 3417 & 4757 & 4757 & 7705 & 3417 & 7705 \\ 11232 & 5304 & 7384 & 2392 & 11960 & 11336 & 5304 & 7384 & 2392 & 11960 \\ 10908 & 5151 & 7171 & 2323 & 11615 & 11009 & 5151 & 7171 & 2323 & 11615 \\ 8316 & 3927 & 5467 & 1771 & 8855 & 8393 & 3927 & 5467 & 1771 & 8855 \\ 11340 & 5355 & 7455 & 2415 & 12075 & 11445 & 5355 & 7455 & 2415 & 12075 \\ 12420 & 5865 & 8165 & 2645 & 13225 & 12535 & 5865 & 8165 & 2645 & 13225 \\ 9072 & 4284 & 5964 & 1932 & 9660 & 9156 & 4284 & 5964 & 1932 & 9660 \\ 12312 & 5814 & 8048 & 2622 & 13110 & 5814 & 8048 & 2622 & 13110 & 5814 \\ 13068 & 6171 & 8591 & 2783 & 13915 & 13198 & 6171 & 8591 & 2783 & 13915 \end{bmatrix}$$

This C = PM matrix can be converted into either row or column matrix and sent is to the other user over an unsecure channel with index number, size of matrix and the matrix 'M_{22}'

[1, 10, 52740, 58120, 52985, 59129, 44613, 52635, 58072, 53005, 59116, 44569, 7236, 4757, 4757, 7705, 3417, 4757, 4757, 7705, 3417, 7705, 11232, 5304, 7384, 2392, 11960, 11336, 5304, 7384, 2392, 11960, 10908, 5151, 7171, 2323, 11615, 11009, 5151, 7171, 2323, 11615, 8316, 3927, 5467, 1771, 8855, 8393, 3927, 5467, 1771, 8855, 11340, 5355, 7455, 2415, 12075, 11445, 5355, 7455, 2415, 12075, 12420, 5865, 8165, 2645, 13225, 12535, 5865, 8165, 2645, 13225, 9072, 4284, 5964, 1932, 9660, 9156, 4284, 5964, 1932, 9660, 12312, 5814, 8048, 2622, 13110, 5814, 8048, 2622, 13110, 5814, 13068, 6171, 8591, 2783, 13915, 13198, 6171, 8591, 2783, 13915, 20, 77, 57, 105, 13, 101, 33, 10, 68, 123, 39, 83, 29, 127, 0, 67, 88, 116, 10, 99, 21, 95, 19, 56, 104]

Decryption Algorithm:

Decryption is done by the following steps

- **Construct the Matrices using Received Encrypted Data**

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

$$C = PM = \begin{bmatrix} 52740 & 58120 & 52985 & 59129 & 44613 & 52635 & 58072 & 53005 & 59116 & 44569 \\ 7236 & 4757 & 4757 & 7705 & 3417 & 4757 & 4757 & 7705 & 3417 & 7705 \\ 11232 & 5304 & 7384 & 2392 & 11960 & 11336 & 5304 & 7384 & 2392 & 11960 \\ 10908 & 5151 & 7171 & 2323 & 11615 & 11009 & 5151 & 7171 & 2323 & 11615 \\ 8316 & 3927 & 5467 & 1771 & 8855 & 8393 & 3927 & 5467 & 1771 & 8855 \\ 11340 & 5355 & 7455 & 2415 & 12075 & 11445 & 5355 & 7455 & 2415 & 12075 \\ 12420 & 5865 & 8165 & 2645 & 13225 & 12535 & 5865 & 8165 & 2645 & 13225 \\ 9072 & 4284 & 5964 & 1932 & 9660 & 9156 & 4284 & 5964 & 1932 & 9660 \\ 12312 & 5814 & 8048 & 2622 & 13110 & 5814 & 8048 & 2622 & 13110 & 5814 \\ 13068 & 6171 & 8591 & 2783 & 13915 & 13198 & 6171 & 8591 & 2783 & 13915 \end{bmatrix}$$

And the self-invertible matrix M_{22} is

$$M_{22} = \begin{bmatrix} 20 & 77 & 57 & 105 & 13 \\ 101 & 33 & 10 & 68 & 123 \\ 39 & 83 & 29 & 127 & 0 \\ 67 & 88 & 116 & 10 & 99 \\ 21 & 95 & 19 & 56 & 104 \end{bmatrix}$$

Now, the receiver find the M_{11}, M_{12} and M_{21} to construct the self-invertible matrix "M".

$$M = \begin{bmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{bmatrix} = \begin{bmatrix} 108 & 51 & 71 & 23 & 115 & 109 & 51 & 71 & 23 & 115 \\ 27 & 95 & 118 & 60 & 5 & 27 & 96 & 118 & 60 & 5 \\ 89 & 45 & 99 & 1 & 0 & 89 & 45 & 100 & 1 & 0 \\ 61 & 40 & 12 & 118 & 29 & 61 & 40 & 12 & 119 & 29 \\ 107 & 33 & 109 & 72 & 24 & 107 & 33 & 109 & 72 & 25 \\ 21 & 77 & 57 & 105 & 13 & 20 & 77 & 57 & 105 & 13 \\ 101 & 34 & 10 & 68 & 123 & 101 & 33 & 10 & 68 & 123 \\ 39 & 83 & 30 & 127 & 0 & 39 & 83 & 29 & 127 & 0 \\ 67 & 88 & 116 & 11 & 99 & 67 & 88 & 116 & 10 & 99 \\ 21 & 95 & 19 & 56 & 105 & 21 & 95 & 19 & 56 & 104 \end{bmatrix}$$

- **Multiplying the Matrices "C" and "M"**

Now we multiply the matrix 'C' with self-invertible matrix 'M' then we get

CM = PMM

$$CM = \begin{bmatrix} 52740 & 58120 & 52985 & 59129 & 44613 & 52635 & 58072 & 53005 & 59116 & 44569 \\ 7236 & 4757 & 4757 & 7705 & 3417 & 4757 & 4757 & 7705 & 3417 & 7705 \\ 11232 & 5304 & 7384 & 2392 & 11960 & 11336 & 5304 & 7384 & 2392 & 11960 \\ 10908 & 5151 & 7171 & 2323 & 11615 & 11009 & 5151 & 7171 & 2323 & 11615 \\ 8316 & 3927 & 5467 & 1771 & 8855 & 8393 & 3927 & 5467 & 1771 & 8855 \\ 11340 & 5355 & 7455 & 2415 & 12075 & 11445 & 5355 & 7455 & 2415 & 12075 \\ 12420 & 5865 & 8165 & 2645 & 13225 & 12535 & 5865 & 8165 & 2645 & 13225 \\ 9072 & 4284 & 5964 & 1932 & 9660 & 9156 & 4284 & 5964 & 1932 & 9660 \\ 12312 & 5814 & 8048 & 2622 & 13110 & 5814 & 8048 & 2622 & 13110 & 5814 \\ 13068 & 6171 & 8591 & 2783 & 13915 & 13198 & 6171 & 8591 & 2783 & 13915 \end{bmatrix} \begin{bmatrix} 108 & 51 & 71 & 23 & 115 & 109 & 51 & 71 & 23 & 115 \\ 27 & 95 & 118 & 60 & 5 & 27 & 96 & 118 & 60 & 5 \\ 89 & 45 & 99 & 1 & 0 & 89 & 45 & 100 & 1 & 0 \\ 61 & 40 & 12 & 118 & 29 & 61 & 40 & 12 & 119 & 29 \\ 107 & 33 & 109 & 72 & 24 & 107 & 33 & 109 & 72 & 25 \\ 21 & 77 & 57 & 105 & 13 & 20 & 77 & 57 & 105 & 13 \\ 101 & 34 & 10 & 68 & 123 & 101 & 33 & 10 & 68 & 123 \\ 39 & 83 & 30 & 127 & 0 & 39 & 83 & 29 & 127 & 0 \\ 67 & 88 & 116 & 11 & 99 & 67 & 88 & 116 & 10 & 99 \\ 21 & 95 & 19 & 56 & 105 & 21 & 95 & 19 & 56 & 104 \end{bmatrix}$$

$$CM = \begin{bmatrix} 34295808 & 34295875 & 34295912 & 34295909 & 27500493 & 34295913 & 34295923 & 34295892 & 34295922 & 27500537 \\ 3164611 & 3164544 & 3164544 & 3164544 & 2555648 & 3164544 & 3164544 & 3164544 & 3164544 & 2555648 \\ 4912232 & 4912128 & 4912128 & 4912128 & 3966976 & 4912128 & 4912128 & 4912128 & 4912128 & 3966976 \\ 4770533 & 4770432 & 4770432 & 4770432 & 3852544 & 4770432 & 4770432 & 4770432 & 4770432 & 3852544 \\ 3636941 & 3636864 & 3636864 & 3636864 & 2937088 & 3636864 & 3636864 & 3636864 & 3636864 & 2937088 \\ 4959465 & 4959360 & 4959360 & 4959360 & 4005120 & 4959360 & 4959360 & 4959360 & 4959360 & 4005120 \\ 5431795 & 5431680 & 5431680 & 5431680 & 4386560 & 5431680 & 5431680 & 5431680 & 5431680 & 4386560 \\ 3967572 & 3967488 & 3967488 & 3967488 & 3204096 & 3967488 & 3967488 & 3967488 & 3967488 & 3204096 \\ 5384562 & 5384448 & 5384448 & 5384448 & 4348416 & 5384448 & 5384448 & 5384448 & 5384448 & 4348416 \\ 5715193 & 5715072 & 5715072 & 5715072 & 4615424 & 5715072 & 5715072 & 5715072 & 5715072 & 4615424 \end{bmatrix}$$

- **Performing Modulo 128 Reduction on the Matrix "CM"**

Taking addition **modulo 128**, then we get the following results

$$34295808 \pmod{128} = 0$$

$$34295875 \pmod{128} = 67$$

$$34295912 \pmod{128} = 104$$

.....

.....

.....

$$5715072 \pmod{128} = 0$$

$$5715072 \pmod{128} = 0$$

$$4615424 \pmod{128} = 0$$

- **Reconstructing the Adjacency Matrix using Modulo values**

Now we construct the adjacency matrix using the above Modulo values

$$CM = \begin{bmatrix} 0 & 67 & 104 & 101 & 77 & 105 & 115 & 84 & 114 & 121 \\ 67 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 104 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 101 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 77 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 105 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 115 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 84 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 114 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 121 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} = P$$

- **Reconstructing the Graph using Adjacency Matrix**

The corresponding star graph for the above adjacency matrix is

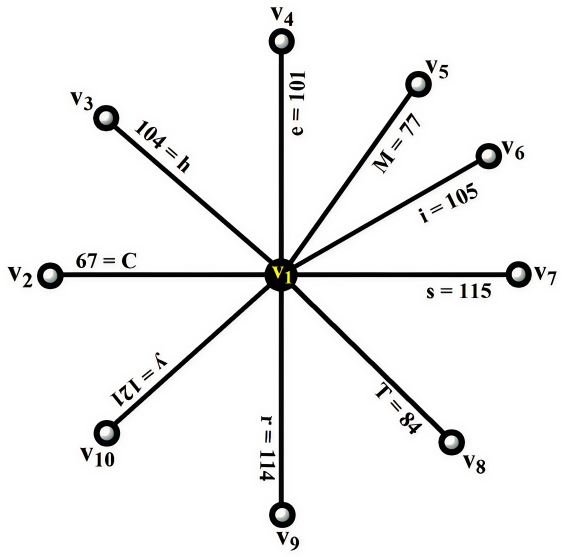

Figure 4.2: Star Graph

- **Conversion of ASCII Values to Plaintext**

The Decrypted data is given as the edges(weights) of the above path are 67, 104,101, 77, 105, 84, 114, 121. So,

C → 67, h → 104, e → 101, M → 77, i → 105, s → 115, T → 84, r → 114, y → 121.

The original message is **"CheMisTry"**.

4.2.2 Example No.2

Suppose that User A(sender) wants to send the message "What's wrong?" to User B(receiver) using the technique of encryption.

Encryption Algorithm:

Encryption is done by the following steps

- **Conversion of Plaintext to ASCII Values**

Firstly, the sender converts the given message units"What's wrong?" into their numerical equivalent values that is using ASCII Table:

W → 87, h → 104, a → 97, t → 116, Apostrophes= ' = 39, s → 115,

Space → 32, w → 119, r → 114, o → 111, n → 110, g → 103, ? → 63.

- **Design the Graph and Construct the Adjacency Matrix**

Now we make the corresponding star graph which is given below

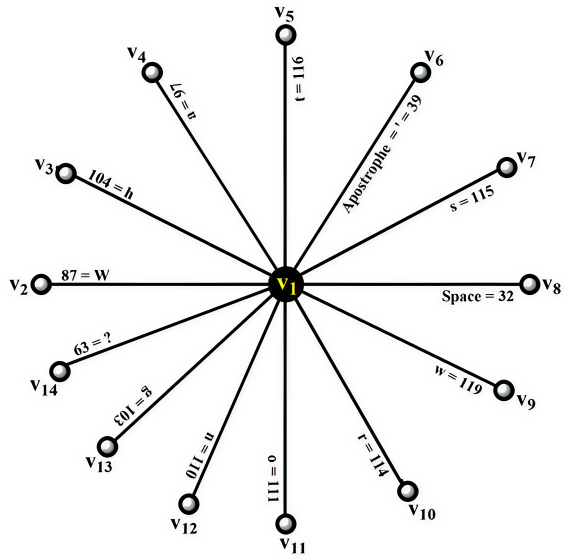

Figure 4.3: Star Graph

Computing the adjacency matrix for the above star graph and denote it as 'P'

$$\mathbf{P} = \begin{bmatrix} 0 & 87 & 104 & 97 & 116 & 39 & 115 & 32 & 119 & 114 & 111 & 110 & 103 & 63 \\ 87 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 104 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 97 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 116 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 39 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 115 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 32 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 119 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 114 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 111 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 110 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 103 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 63 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

- **Generating A Self-Invertible Matrix**

Now we need to compute the key matrix for that purpose we construct the self-invertible key matrix 'M' with the help of $\frac{n}{2}$ matrix M_{22}. Let

$$M_{22} = \begin{bmatrix} 65 & 68 & 26 & 21 & 115 & 33 & 54 \\ 65 & 44 & 38 & 29 & 125 & 77 & 65 \\ 104 & 120 & 60 & 55 & 56 & 91 & 10 \\ 101 & 112 & 29 & 39 & 14 & 28 & 33 \\ 82 & 70 & 108 & 118 & 33 & 15 & 102 \\ 48 & 79 & 24 & 55 & 52 & 37 & 3 \\ 103 & 75 & 28 & 23 & 76 & 40 & 118 \end{bmatrix}$$

$$M_{12} + M_{22} = 0$$

$$M_{11} = \text{- } M_{22} + \text{mod } 128$$

$$M_{11} = \begin{bmatrix} 63 & 60 & 102 & 107 & 13 & 95 & 74 \\ 63 & 84 & 90 & 99 & 3 & 51 & 63 \\ 24 & 8 & 68 & 73 & 72 & 37 & 118 \\ 27 & 16 & 99 & 89 & 114 & 100 & 95 \\ 46 & 58 & 20 & 10 & 95 & 113 & 26 \\ 80 & 49 & 104 & 73 & 76 & 91 & 125 \\ 25 & 53 & 100 & 105 & 52 & 88 & 10 \end{bmatrix}$$

$$M_{12} = \text{I - } M_{22}$$

$$M_{12} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} - \begin{bmatrix} 65 & 68 & 26 & 21 & 115 & 33 & 54 \\ 65 & 44 & 38 & 29 & 125 & 77 & 65 \\ 104 & 120 & 60 & 55 & 56 & 91 & 10 \\ 101 & 112 & 29 & 39 & 14 & 28 & 33 \\ 82 & 70 & 108 & 118 & 33 & 15 & 102 \\ 48 & 79 & 24 & 55 & 52 & 37 & 3 \\ 103 & 75 & 28 & 23 & 76 & 40 & 118 \end{bmatrix}$$

$$M_{12} = \begin{bmatrix} -64 & -68 & -26 & -21 & -115 & -33 & -54 \\ -65 & -43 & -38 & -29 & -125 & -77 & -65 \\ -104 & -120 & -59 & -55 & -56 & -91 & -10 \\ -101 & -112 & -29 & -38 & -14 & -28 & -33 \\ -82 & -70 & -108 & -118 & -32 & -15 & -102 \\ -48 & -79 & -24 & -55 & -52 & -36 & -3 \\ -103 & -75 & -28 & -23 & -76 & -40 & -117 \end{bmatrix} = \begin{bmatrix} 64 & 60 & 102 & 107 & 13 & 95 & 74 \\ 63 & 85 & 90 & 99 & 3 & 51 & 63 \\ 24 & 8 & 69 & 73 & 72 & 37 & 118 \\ 27 & 16 & 99 & 90 & 114 & 100 & 95 \\ 46 & 58 & 20 & 10 & 96 & 113 & 26 \\ 80 & 49 & 104 & 73 & 76 & 92 & 125 \\ 25 & 53 & 100 & 105 & 52 & 88 & 11 \end{bmatrix}$$

Now we find M_{21}. For this we know that $M_{21} = \text{I} + M_{22}$

$$M_{21} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} + \begin{bmatrix} 65 & 68 & 26 & 21 & 115 & 33 & 54 \\ 65 & 44 & 38 & 29 & 125 & 77 & 65 \\ 104 & 120 & 60 & 55 & 56 & 91 & 10 \\ 101 & 112 & 29 & 39 & 14 & 28 & 33 \\ 82 & 70 & 108 & 118 & 33 & 15 & 102 \\ 48 & 79 & 24 & 55 & 52 & 37 & 3 \\ 103 & 75 & 28 & 23 & 76 & 40 & 118 \end{bmatrix}$$

$$M_{21} = \begin{bmatrix} 66 & 68 & 26 & 21 & 115 & 33 & 54 \\ 65 & 45 & 38 & 29 & 125 & 77 & 65 \\ 104 & 120 & 61 & 55 & 56 & 91 & 10 \\ 101 & 112 & 29 & 40 & 14 & 28 & 33 \\ 82 & 70 & 108 & 118 & 34 & 15 & 102 \\ 48 & 79 & 24 & 55 & 52 & 38 & 3 \\ 103 & 75 & 28 & 23 & 76 & 40 & 119 \end{bmatrix}$$

So, the self-invertible key matrix 'M' is

$$M = \begin{bmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{bmatrix} = \begin{bmatrix} 63 & 60 & 102 & 107 & 13 & 95 & 74 & 64 & 60 & 102 & 107 & 13 & 95 & 74 \\ 63 & 84 & 90 & 99 & 3 & 51 & 63 & 63 & 85 & 90 & 99 & 3 & 51 & 63 \\ 24 & 8 & 68 & 73 & 72 & 37 & 118 & 24 & 8 & 69 & 73 & 72 & 37 & 118 \\ 27 & 16 & 99 & 89 & 114 & 100 & 95 & 27 & 16 & 99 & 90 & 114 & 100 & 95 \\ 46 & 58 & 20 & 10 & 95 & 113 & 26 & 46 & 58 & 20 & 10 & 96 & 113 & 26 \\ 80 & 49 & 104 & 73 & 76 & 91 & 125 & 80 & 49 & 104 & 73 & 76 & 92 & 125 \\ 25 & 53 & 100 & 105 & 52 & 88 & 10 & 25 & 53 & 100 & 105 & 52 & 88 & 11 \\ 66 & 68 & 26 & 21 & 115 & 33 & 54 & 65 & 68 & 26 & 21 & 115 & 33 & 54 \\ 65 & 45 & 38 & 29 & 125 & 77 & 65 & 65 & 44 & 38 & 29 & 125 & 77 & 65 \\ 104 & 120 & 61 & 55 & 56 & 91 & 10 & 104 & 120 & 60 & 55 & 56 & 91 & 10 \\ 101 & 112 & 29 & 40 & 14 & 28 & 33 & 101 & 112 & 29 & 39 & 14 & 28 & 33 \\ 82 & 70 & 108 & 118 & 34 & 15 & 102 & 82 & 70 & 108 & 118 & 33 & 15 & 102 \\ 48 & 79 & 24 & 55 & 52 & 38 & 3 & 48 & 79 & 24 & 55 & 52 & 37 & 3 \\ 103 & 75 & 28 & 23 & 76 & 40 & 119 & 103 & 75 & 28 & 23 & 76 & 40 & 118 \end{bmatrix}$$

- **Determining the product of matrices P and M**

Finally, we have to compute **PM**, this multiplication is known as the encrypted data of the original message.

$$\mathbf{P} = \begin{bmatrix} 0 & 87 & 104 & 97 & 116 & 39 & 115 & 32 & 119 & 114 & 111 & 110 & 103 & 63 \\ 87 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 104 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 97 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 116 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 39 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 115 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 32 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 119 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 114 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 111 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 110 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 103 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 63 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

After Multiplying both matrices 'P' and 'M', we get the matrix 'C' which is given below

$$\mathbf{C} = \mathbf{PM} = \begin{bmatrix}
75294 & 78631 & 74204 & 75847 & 79148 & 76547 & 69301 & 75262 & 78599 & 74014 & 75833 & 79154 & 76483 & 69353 \\
5481 & 5220 & 8874 & 9309 & 1131 & 8265 & 6438 & 5568 & 5220 & 8874 & 9309 & 1131 & 8265 & 6438 \\
6552 & 6240 & 10608 & 11128 & 1352 & 9880 & 7696 & 6656 & 6240 & 10608 & 11128 & 1352 & 9880 & 7696 \\
6111 & 5820 & 9894 & 10379 & 1261 & 9215 & 7178 & 6208 & 5820 & 9894 & 10379 & 1261 & 9215 & 7178 \\
7308 & 6996 & 11832 & 12412 & 1508 & 11020 & 8584 & 7424 & 6960 & 11832 & 12412 & 1508 & 11020 & 8584 \\
2457 & 2340 & 3978 & 4173 & 507 & 3705 & 2886 & 2340 & 3978 & 4173 & 507 & 3705 & 2886 & 2340 \\
7245 & 6900 & 11730 & 12305 & 1495 & 10925 & 8510 & 7360 & 6900 & 11730 & 12305 & 1495 & 10925 & 8510 \\
2016 & 1920 & 3264 & 3424 & 416 & 3040 & 2368 & 1920 & 3264 & 3424 & 416 & 3040 & 2368 & 1920 \\
7497 & 7140 & 12138 & 12733 & 1547 & 11305 & 8806 & 7616 & 7140 & 12138 & 12733 & 1547 & 11305 & 8806 \\
7182 & 6840 & 11628 & 12213 & 1483 & 10830 & 8436 & 7296 & 6840 & 11628 & 12213 & 1483 & 10830 & 8436 \\
6993 & 6660 & 11322 & 11877 & 1443 & 10545 & 8214 & 7104 & 6660 & 11322 & 11877 & 1443 & 10545 & 8214 \\
6930 & 6600 & 11220 & 11770 & 1430 & 10450 & 8140 & 7040 & 6600 & 11220 & 11770 & 1430 & 10450 & 8140 \\
6489 & 6180 & 10506 & 11021 & 1339 & 9785 & 7622 & 6592 & 6180 & 10506 & 11021 & 1339 & 9785 & 7622 \\
3969 & 3780 & 6426 & 6741 & 819 & 5985 & 4662 & 4032 & 3780 & 6426 & 6741 & 819 & 5985 & 4662
\end{bmatrix}$$

This $\mathbf{C = PM}$ matrix can be converted into either row or column matrix and sent is to the other user over an unsecure channel with index number, size of matrix and the matrix and at the end we also write M_{22}.

[1, 14, 75294, 78631, 74204, 75847, 79148, 76547, 69301, 75262, 78599, 74014, 75833, 79154, 76483, 69353, 5481, 5220, 8874, 9309, 1131, 8265, 6438, 5568, 5220, 8874, 9309, 1131, 8265, 6438, 6552, 6240, 10608, 11128, 1352, 9880, 7696, 6656, 6240, 10608, 11128, 1352, 9880, 7696, 6111, 5820, 9894, 10379, 1261, 9215, 7178, 6208, 5820, 9894, 10379, 1261, 9215, 7178, 7308, 6996, 11832, 12412, 1508, 11020, 8584, 7424, 6960, 11832, 12412, 1508, 11020, 8584, 2457, 2340, 3978, 4173, 507, 3705, 2886, 2340, 3978, 4173, 507, 3705, 2886, 2340, 7245, 6900, 11730, 12305, 1495, 10925, 8510, 7360, 6900, 11730, 12305, 1495, 10925, 8510, 2016, 1920, 3264, 3424, 416, 3040, 2368, 1920, 3264, 3424, 416, 3040, 2368, 1920, 7497, 7140, 12138, 12733, 1547, 11305, 8806, 7616, 7140, 12138, 12733, 1547, 11305, 8806, 7182, 6840, 11628, 12213, 1483, 10830, 8436, 7296, 6840, 11628, 12213, 1483, 10830, 8436, 6993, 6660, 11322, 11877, 1443, 10545, 8214, 7104, 6660, 11322, 11877, 1443, 10545, 8214, 6930, 6600, 11220, 11770, 1430, 10450, 8140, 7040, 6600, 11220, 11770, 1430, 10450, 8140, 6489, 6180, 10506, 11021, 1339, 9785, 7622, 6592, 6180, 10506, 11021, 1339, 9785, 7622, 3969, 3780, 6426, 6741, 819, 5985, 4662, 4032, 3780, 6426, 6741, 819, 5985, 4662,65, 68, 26, 21, 115, 33, 54, 65, 44, 38, 29, 125, 77, 65, 104, 120, 60, 55, 56, 91, 10, 101, 112, 29, 39, 14, 28, 33, 82, 70, 108, 118, 33, 15, 102, 48, 79, 24, 55, 52, 37, 3, 103, 75, 28, 23, 76, 40, 118]

Decryption Algorithm:

Decryption is done by the following steps

- **Construct the Matrices using Received Encrypted Data**

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

$$\mathbf{C = PM} = \begin{bmatrix}
75294 & 78631 & 74204 & 75847 & 79148 & 76547 & 69301 & 75262 & 78599 & 74014 & 75833 & 79154 & 76483 & 69353 \\
5481 & 5220 & 8874 & 9309 & 1131 & 8265 & 6438 & 5568 & 5220 & 8874 & 9309 & 1131 & 8265 & 6438 \\
6552 & 6240 & 10608 & 11128 & 1352 & 9880 & 7696 & 6656 & 6240 & 10608 & 11128 & 1352 & 9880 & 7696 \\
6111 & 5820 & 9894 & 10379 & 1261 & 9215 & 7178 & 6208 & 5820 & 9894 & 10379 & 1261 & 9215 & 7178 \\
7308 & 6996 & 11832 & 12412 & 1508 & 11020 & 8584 & 7424 & 6960 & 11832 & 12412 & 1508 & 11020 & 8584 \\
2457 & 2340 & 3978 & 4173 & 507 & 3705 & 2886 & 2340 & 3978 & 4173 & 507 & 3705 & 2886 & 2340 \\
7245 & 6900 & 11730 & 12305 & 1495 & 10925 & 8510 & 7360 & 6900 & 11730 & 12305 & 1495 & 10925 & 8510 \\
2016 & 1920 & 3264 & 3424 & 416 & 3040 & 2368 & 1920 & 3264 & 3424 & 416 & 3040 & 2368 & 1920 \\
7497 & 7140 & 12138 & 12733 & 1547 & 11305 & 8806 & 7616 & 7140 & 12138 & 12733 & 1547 & 11305 & 8806 \\
7182 & 6840 & 11628 & 12213 & 1483 & 10830 & 8436 & 7296 & 6840 & 11628 & 12213 & 1483 & 10830 & 8436 \\
6993 & 6660 & 11322 & 11877 & 1443 & 10545 & 8214 & 7104 & 6660 & 11322 & 11877 & 1443 & 10545 & 8214 \\
6930 & 6600 & 11220 & 11770 & 1430 & 10450 & 8140 & 7040 & 6600 & 11220 & 11770 & 1430 & 10450 & 8140 \\
6489 & 6180 & 10506 & 11021 & 1339 & 9785 & 7622 & 6592 & 6180 & 10506 & 11021 & 1339 & 9785 & 7622 \\
3969 & 3780 & 6426 & 6741 & 819 & 5985 & 4662 & 4032 & 3780 & 6426 & 6741 & 819 & 5985 & 4662
\end{bmatrix}$$

And the self-invertible matrix M_{22} is

$$M_{22} = \begin{bmatrix}
65 & 68 & 26 & 21 & 115 & 33 & 54 \\
65 & 44 & 38 & 29 & 125 & 77 & 65 \\
104 & 120 & 60 & 55 & 56 & 91 & 10 \\
101 & 112 & 29 & 39 & 14 & 28 & 33 \\
82 & 70 & 108 & 118 & 33 & 15 & 102 \\
48 & 79 & 24 & 55 & 52 & 37 & 3 \\
103 & 75 & 28 & 23 & 76 & 40 & 118
\end{bmatrix}$$

Now, the receiver find the M_{11}, M_{12} and M_{21} to construct the self-invertible matrix "M".

$$\mathbf{M} = \begin{bmatrix}
63 & 60 & 102 & 107 & 13 & 95 & 74 & 64 & 60 & 102 & 107 & 13 & 95 & 74 \\
63 & 84 & 90 & 99 & 3 & 51 & 63 & 63 & 85 & 90 & 99 & 3 & 51 & 63 \\
24 & 8 & 68 & 73 & 72 & 37 & 118 & 24 & 8 & 69 & 73 & 72 & 37 & 118 \\
27 & 16 & 99 & 89 & 114 & 100 & 95 & 27 & 16 & 99 & 90 & 114 & 100 & 95 \\
46 & 58 & 20 & 10 & 95 & 113 & 26 & 46 & 58 & 20 & 10 & 96 & 113 & 26 \\
80 & 49 & 104 & 73 & 76 & 91 & 125 & 80 & 49 & 104 & 73 & 76 & 92 & 125 \\
25 & 53 & 100 & 105 & 52 & 88 & 10 & 25 & 53 & 100 & 105 & 52 & 88 & 11 \\
66 & 68 & 26 & 21 & 115 & 33 & 54 & 65 & 68 & 26 & 21 & 115 & 33 & 54 \\
65 & 45 & 38 & 29 & 125 & 77 & 65 & 65 & 44 & 38 & 29 & 125 & 77 & 65 \\
104 & 120 & 61 & 55 & 56 & 91 & 10 & 104 & 120 & 60 & 55 & 56 & 91 & 10 \\
101 & 112 & 29 & 40 & 14 & 28 & 33 & 101 & 112 & 29 & 39 & 14 & 28 & 33 \\
82 & 70 & 108 & 118 & 34 & 15 & 102 & 82 & 70 & 108 & 118 & 33 & 15 & 102 \\
48 & 79 & 24 & 55 & 52 & 38 & 3 & 48 & 79 & 24 & 55 & 52 & 37 & 3 \\
103 & 75 & 28 & 23 & 76 & 40 & 119 & 103 & 75 & 28 & 23 & 76 & 40 & 118
\end{bmatrix}$$

- **Multiplying the Matrices "C" and "M"**

After multiplying the received matrices "C" and "M" , we get the following results

CM =

C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	C_{11}	C_{12}	C_{13}	C_{14}
67756800	67756887	67756976	67756839	64723035	67756832	67756919	67756911	67529369	67756903	67756863	67756897	67756916	67756914
5735040	5735040	5735040	5735040	5362680	5735040	5735040	5735040	5707113	5735040	5735040	5735040	5735040	5735040
6855784	6855688	6855680	6855680	6410560	6855680	6855680	6855680	6822296	6855680	6855680	6855680	6855680	6855680
6394327	6394240	6394240	6394240	5979096	6394240	6394240	6394240	6363103	6394240	6394240	6394240	6394240	6394240
7646836	7646720	7646720	7646720	7150240	7646720	7646720	7646720	7609484	7646720	7646720	7646720	7646720	7646720
2578019	2578080	2578080	2578080	2403960	2578080	2578080	2578080	2558361	2578080	2578080	2578080	2578080	2578080
7580915	7580800	7580800	7580800	7086800	7580800	7580800	7580800	7543885	7580800	7580800	7580800	7580800	7580800
2109472	2109440	2109440	2109440	1972480	2109440	2109440	2109440	2090440	2109440	2109440	2109440	2109440	2109440
7844599	7844480	7844480	7844480	7335160	7844480	7844480	7844480	7806281	7844480	7844480	7844480	7844480	7844480
7514994	7514880	7514880	7514880	7019480	7514880	7514880	7514880	7478285	7514880	7514880	7514880	7514880	7514880
7317231	7317120	7317120	7317120	6820400	7317120	7317120	7317120	7275849	7317120	7317120	7317120	7317120	7317120
7251310	7251200	7251200	7251200	6760400	7251200	7251200	7251200	7215820	7251200	7251200	7251200	7251200	7251200
6789863	6789760	6789760	6789760	6348920	6789760	6789760	6789760	6760697	6789760	6789760	6789760	6789760	6789760
4153023	4152960	4152960	4152960	3883320	4152960	4152960	4152960	4132737	4152960	4152960	4152960	4152960	4152960

- **Performing Modulo 128 Reduction on the Matrix "CM"**

Taking **modulo 128**, then we get the following resluts

$$67756800 (\text{mod } 128) = 0$$

$$67756887 (\text{mod } 128) = 87$$

$$67756976 (\text{mod } 128) = 104$$

$$67756839 (\text{mod } 128) = 97$$

.....

.....

.....

$$4152960 (\text{mod } 128) = 0$$

$$4152960 (\text{mod } 128) = 0$$

$$4152960 (\text{mod } 128) = 0$$

- **Reconstructing the Adjacency Matrix using Modulo values**

Now we construct the adjacency matrix using the above Modulo values

$$\mathbf{CM} = \begin{bmatrix} 0 & 87 & 104 & 97 & 116 & 39 & 115 & 32 & 119 & 114 & 111 & 110 & 103 & 63 \\ 87 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 104 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 97 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 116 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 39 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 115 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 32 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 119 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 114 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 111 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 110 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 103 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 63 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} = \mathbf{P}$$

- **Reconstructing the Graph using Adjacency Matrix**

The Corresponding graph for the above adjacency matrix is

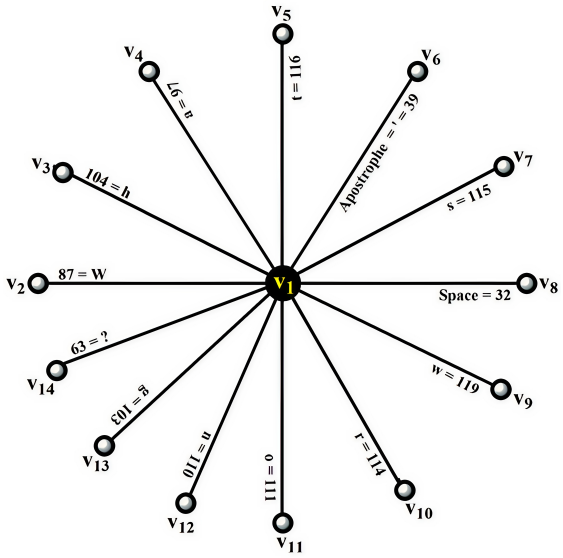

Figure 4.4: Star Graph

The edges(weights) of the above path are 87, 104, 97, 116, 39, 115, 32, 119, 114, 111, 110, 103, 63.

- **Conversion of ASCII Values to Plaintext**

So, the Decrypted data is given below

87 → W, 104 → h, 97 → a, 116 → t, = ’ = 39 = ’ = Apostrophes, 115 → s, 32 → Space, 119 → w, 114 → r, 111 → o, 110 → n, 103 → g, 63 → ? .

The original decrypted message is "**What's wrong?**".

Chapter 5

Conclusion

In this thesis, we introduce a novel encryption method that uses matrix algebra and graph theory to improve data security. We propose to convert plaintext to an encrypted adjacency matrix via matrix multiplication, where plaintext is encrypted using an efficient star graph model and a self-invertible key matrix. This approach not only makes decryption more efficient through its self-invertible key but also increases the security of the ciphertext by producing complex ciphertext. This method ensures secure transmission over insecure channels and is highly applicable in defense-oriented and financial-oriented domains. Overall, it offers an efficient and robust solution to present-day cryptographic challenges.

Bibliography

[1] Smith, J., Williams, T., (2019), Graph-based Encryption Using Complete Graphs, Journal of Cryptography and Information Security, 10(3), 245-260.

[2] Chen, L., Zhang, H., (2017), Self-Invertible Matrices in Cryptography, Mathematical Structures in Computer Science, 25(4), 503-519.

[3] Khanna, A., Mehta, V., (2020), Encryption Techniques with Complete Graphs, Journal of Network Security and Cryptography, 3(1), 77-89..

[4] Thompson, R., Lee, K., (2022), Applications of Graph Theory in Modern Cryptography, Journal of Applied Cryptography, 12(2), 130-145.

[5] Acharya, D., Mishra, P. (2018). Advanced Encryption Standard and its Applications in Network Security. Journal of Cryptographic Engineering, 10(3), 245–260.

[6] P. Amudha, J. Jayapriya, J. Gowri.,(2021),An algorithmic approach for encryption using graph Labeling, ICMS 2020.

[7] M. Yamuna, Meenal Gogia, Ashish Sikka, Md. Jazib Hayat Khan, Encryption using Graphh theory and Linear algebra.

[8] Ahmed, S., Rahman, F., (2019), A Comprehensive Review on Complete Graphs in Encryption Techniques, Cryptography and Network Security Journal, 6(4), 210-225.

[9] Mohan, P., Rajendran, K., & Rajesh, A. (2022). An Encryption Technique Using A Complete Graph With A Self-Invertible Matrix. Journal of Algebraic statistics, 13(3), 1821-1826.

[10] Cai, S., Liu, X. (2020). Efficient Data Encryption and Decryption with Self-Invertible Matrices. International Journal of Information Security, 45(2), 233–247.

[11] Gupta, R., Kumar, P. (2019). Self-Invertible Key Matrices in Cryptography and Data Security. Journal of Applied Mathematics and Computing, 47(1), 112–123.

[12] Patel, R., Kumar, S., (2021), Encryption via Graph Theory, International Journal of Computer Applications, 55(2), 150-165

[13] Hill, L. (1929). Cryptographic Techniques with Linear Algebra: The Hill Cipher. American Mathematical Monthly, 36(3), 213–220.

[14] Zhang, W., Zhu, Q. (2022). Encryption Techniques in Modern Cryptography Using Graph Structures and Self-Invertible Matrices. Journal of Cryptographic Mathematics, 67(2), 342–360.

[15] Singh, M., Johnson, T. (2018). Enhanced Security in Cryptography through Adjacency Matrix Encoding. Security and Communication Networks, 22(4), 423–437.

[16] Ray, S., Singh, K. (2021). Applications of Star Graphs in Cryptographic Systems. Journal of Discrete Mathematical Sciences, 19(5), 287–297.

[17] Patel, S., Srivastava, D. (2020). Optimization of Encryption Algorithms Using Graph-Based Models. Journal of Information Security, 28(3), 315–332.

[18] Wang, L., Zhao, Y. (2015). Graph-Based Encryption Algorithms for Data Security and Privacy. IEEE Communications Magazine, 53(3), 141–147.

[19] Qi, L., Wang, L. (2019). Self-Invertible Matrix Properties in Secure Communication. International Journal of Applied Cryptography, 29(6), 449–456.

[20] Brian Cusack, Erin Chapman, "Using graphic methods to challenge cryptographic Performance", Proceedings of 14th Australian Information Security Management Conference, 5-6 December, 2016, Edith Cowan University, Perth, Western Australia. (pp.30-36).

[21] Wael Mahmoud Al Etaiwi, "Encryption Algorithm Using Graph Theory, Journal of Scientific Research and Reports", pp 2519-2527, 2014

[22] William Stallings, "Cryptography and Network Security", Sixth edition, Pearson Education Inc.2014.

[23] Hashem, M. H., and Ajeena, R. K. K. (2023) The tensor product bipartite graph for symmetric encryption scheme. In AIP conference proceedings (Vol. 2591, No. . AIP Publishing.

[24] Sabharwal, A., Yadav, P., and Kumar, K. (2024). Graph crypto-Stego system for securing graph data using association schemes. J. Appl. Math. 2024:2084342. doi: 10.1155/2024/2084342

[25] Shathir, M. K., Ajeena, R. K., and Arif, G. E. (2023) The triple vertex path graph for hill encryption schemes. In AIP conference proceedings (Vol. 2845, No. . AIP Publishing