A STUDY ON APPLYING GRAPH THEORY IN CRYPTOGRAPHY

A Project work submitted to Thiagarajar College (Autonomous)

Affiliated to Madurai Kamaraj University

In partial fulfillment of the requirement for the award of the degree of

MASTER OF SCIENCE

IN

MATHEMATICS

Submitted by

Ms. S. SUBHASHRI

(Register No: 21SPMA36)

Under the Guidance of

Ms. B. AMBIKA, M.Sc., M.Phil., SET., (Ph.D.)

POST GRADUATE AND RESEARCH DEPARTMENT OF MATHEMATICS

THIAGARAJAR COLLEGE (AUTONOMOUS)

(Re-Accredited with “A++” Grade by NAAC)

Madurai – 625 009

April – 2023

Dr. M. SENTHILKUMARAN, M.Sc., M.Phil., Ph.D.,

Assistant Professor and Head,

Post Graduate and Research Department of Mathematics,

Thiagarajar College,

Madurai - 625 009.

Ms. B. AMBIKA, M.Sc., M.Phil., SET., (Ph.D.)

Assistant Professor,

Post Graduate and Research Department of Mathematics,

Thiagarajar College,

Madurai - 625 009.

BONAFIDE CERTIFICATE

This is to certify that this project work entitled **"A STUDY ON APPLYING GRAPH THEORY IN CRYPTOGRAPHY"** submitted by **S. SUBHASHRI,** student of M.Sc., degree course in Mathematics, **Thiagarajar College (Autonomous), Madurai**, affiliated to **Madurai Kamaraj University, Madurai** is a bonafide record of work carried out by her under my guidance and supervision as a partial fulfillment of the course.

It is further certified that to the best of my knowledge, this project report or any other part of this project has not been submitted in this university or elsewhere for any other degree or diploma.

Submitted for Viva-Voce held on ____________________

Head of the Department **Internal Guide**

External Examiner

S. SUBHASHRI,

Register No. 21SPMA36,

II M.Sc., Mathematics,

Thiagarajar College,

Madurai – 625 009.

DECLARATION

This project work entitled **“A STUDY ON APPLYING GRAPH THEORY IN CRYPTOGRAPHY”** has been carried out by me in the Post Graduate and Research Department of Mathematics, **Thiagarajar College (Autonomous)**, affiliated to **Madurai Kamaraj University, Madurai** in partial fulfillment of the requirements for the degree of Master of Science in Mathematics.

I further declare that this project work or any part of this work has not been submitted in this university or elsewhere for any other degree or diploma.

Date: **Signature of the candidate**

Place: Madurai. **(S. SUBHASHRI)**

(Reg .No. 21SPMA36)

ACKNOWLEDGEMENT

I thank God almighty whose profound blessings were showered throughout the entire period.

I take immense pleasure in thanking **Dr. D. PANDIARAJA, M.Sc., M.Phil., PGDCA., B.Ed., Ph.D.,** Principal, Thiagarajar College, Madurai for having offered me an opportunity to undertake this project and for providing with all the facilities to complete this project successfully.

I am very much thankful to our Head of the Department **Dr. M. SENTHILKUMARAN, M.Sc., M.Phil., Ph.D.,** Assistant Professor, Post Graduate and Research Department of Mathematics, Thiagarajar College, Madurai for his support and kind encouragement to complete my research work successfully.

It would have been definitely impossible for me to complete my work without the patience and encouragement rendered by my guide **Ms. B. AMBIKA, M.Sc., M.Phil., SET., (Ph.D.),** Assistant Professor, Post Graduate and Research Department of Mathematics, Thiagarajar College, Madurai. I would like to extend my hearty thanks to her for the kind support rendered to me.

I would like to thank all the faculty members, Post Graduate and Research Department of Mathematics, Thiagarajar College, Madurai. Without their support, my project work would have been incomplete.

My parents made me realize the value of hard work. I would take this opportunity to record my heartfelt gratitude to them.

(S.SUBHASHRI)

Contents

CHAPTER 1

Introduction

Chapter 1

Introduction

Introduction

Cryptography is a scientific technique of securing a communication from unauthenticated approach. Modern cryptography was established by Shannon in 1949. It is highly connected with discrete mathematics. The word Cryptography comes from the Greek word kryptos - means hidden and graphein - means writing; altogether the word cryptography means hidden and writing. In recent times, cryptography has become a significant area for research due to the vast transfer of information including the need for maintaining secrecy.

Many of the activities in the current world utilize the internet. It may involve electronic cash, bank account credentials or password, digital signatures, time stamping, email services, communication applications, and many more. Through this, we understand the importance of the encryption standards for current world applications.

Graph theory is one of the significant areas in Mathematics. It is a delightful playground for the exploration of techniques in discrete mathematics, and its results have applications in many areas like computing, social science, physics, chemistry, civil engineering, anthropology, linguistics and natural sciences. Various researchers are exploring the concepts of graph theory that can be used in different area of cryptography.

Graphs can be used for designing different encryption algorithms. The interaction between graph theory and cryptography is quite interesting, the initial data (Plaintext) can be stored in the form of Graphs or ciphers can be converted into graphs for secret communication. Since, the graphs can be easily represented in the form of matrix, it is used as the key for encryption and decryption. Rather, other forms of graphs are used as major tool for encryption techniques. Most commonly used graphs for the encryptions are complete graph, bipartite graph, Euler graph, Hamiltonian graph, cycles,….., ect. But various types of graphs are still in use for the enhanced data transmission.

The implementation of Graph theory and Number theory in the encryption techniques, becomes more difficult for the cryptanalysts to crack the information. Data encryption can be done by modular arithmetic and inverse multiplication of the integer which is used as the label for vertices in graphs has the standard encryption to enhance the security.

In recent times, it has been seen a growing interest in exploring graphs as a tool to propose new methodologies in different areas of cryptography. In 2012 [8] Yamuna M, Meenal Gogia, Ashish Sikka, Md. Jazib Hayat Khan presented an encryption mechanism using Hamilton path properties (path that covers all vertices in the graph), they encrypt data twice, once using the Hamilton path, and the second using the complete graph to impose more secure method. In 2014 [7] Wael Mahmoud Al Etaiwi introduced the new symmetric encryption algorithm using the concepts of cycle graph, complete graph and minimum spanning tree to generate a complex cipher text using a shared key. In 2018 [1] Amudha P et al proposed an encryption technique using the Euler graph obtained by incidency matrix of the graph, and an Hamiltonian circuit will be traced out from the encrypted graph. This will be used as a key for decryption.

In this project, chapter 2 gives basic definitions which are needed in the subsequent chapters. In chapter 3, we discuss about encryption algorithms for secure transmission of message using corona graphs. In chapter 4, we discuss about the algorithm using adjacent matrix of graph. In chapter 5, we study about an encryption technique for encrypting the message with the use of complete graph and Hamiltonian cycle.

CHAPTER 2

Preliminaries

Chapter 2

Preliminaries

Basic Definitions

In this chapter, we discuss some basic definitions which are needed in the subsequent chapters.

Definition 2.1:

Cryptography is the science of secret writing with the goal of hiding the meaning of a message.

Definition 2.2:

Cryptanalysis is the science of analyzing and breaking the secure communication. Cryptanalysts are also called as attackers.

Cryptology embraces both cryptography and cryptanalysis.

Definition 2.3:

Data that can be read and understood without any special measures is called **plain text** or clear text.

Definition 2.4:

A **key** is a value that works with a cryptographic algorithm to produce a specific ciphertext.

Definition 2.5:

The transformed message which we received after applying the key on plain text is known as **ciphertext**.

Definition 2.6:

Encryption is a process of encoding information (plain text) to make it unreadable without special knowledge. While encoding, the meaning of the message is not obvious.

Definition 2.7:

Decryption is the reverse process. The process of decoding or transforming an encrypted message (ciphertext) back to its readable and original form (plain text) is called decryption. The system for encryption and decryption is called a cryptosystem.

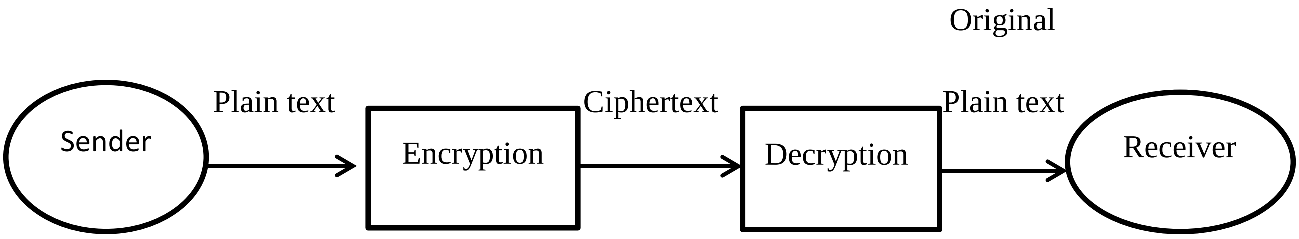

Figure 2.8

Definition 2.9:

Symmetric key cipher uses a single secret key for both encryption and decryption. We can divide traditional symmetric key cipher into two broad categories: substitution ciphers and transposition ciphers.

Definition 2.10:

A **substitution ciphers** replaces one symbol with another. If the symbols in the plaintext are alphabetic characters, we replace one character with another. For example, we can replace letter A with letter D, and letter T with letter Z. If the symbols are digits (0 to 9), we can replace 3 with 7, and 2 with 6.

Definition 2.11:

Special case of substitution ciphers is known as Caesar cipher or **shift cipher**. It shift every plaintext letter by a fixed number of positions in the alphabet. For instance, if we shift by 3 positions, a would be substituted by d, b by e, etc.,

Shift Cipher: Let $x, y, k \in Z_{26}$.

$$\text{Encryption: } e_k(x) \equiv x + k \ mod\ 26.$$

$$\text{Decryption: } d_k(y) \equiv y - k \ mod\ 26.$$

Substitution ciphers can be categorized as either monoalphabetic ciphers or polyalphabetic ciphers.

Definition 2.12:

In **monoalphabetic substitution**, a character (or a symbol) in the plaintext is always changed to the same character (or symbol) in the ciphertext regardless of its position in the text. For example, if the algorithm says that letter A in the plaintext is changed to letter D, every letter A is changed to letter D.

Definition 2.13:

In **polyalphabetic substitution**, each occurrence of a character may have a different substitute. The relationship between a character in the plaintext to a character in the ciphertext is one-to-many. For example, “A” could be enciphered as “D” in the beginning of the text, but as “N” at the middle.

Definition 2.14:

A **transposition ciphers** does not substitute one symbol for another, instead it changes the location of the symbols. A symbol in the first position of the plaintext may appear in the tenth position of the ciphertext. In other words, a transposition cipher reorders (transposes) the symbols.

Definition 2.15:

Double transposition cipher would be the one that repeats twice the algorithm used for encryption and decryption.

Definition 2.16:

In **asymmetric key cipher** there are two keys instead of one: one public key and another one private key. To send a secured message, sender first encrypts the message using receiver’s public key. To decrypt the message, receiver uses his own private key.

Definition 2.17:

Hash functions are an important cryptographic primitive and are widely used in protocols. They compute a digest of a message which is a short, fixed-length bit string. For a particular message, the message digest, or hash value, can be seen as the fingerprint of a message, i.e., a unique representation of a message

Definition 2.18:

Two positive integers a and b are **relatively prime or coprime**, if $\gcd(a, b) = 1$

Result 2.19:

If n and a are coprime, then $a^{-1}\, mod\, n = a^{\varphi(n)-1}\, mod\, n$.

Definition 2.20:

If a is an integer and n is a positive integer, we define $a\, mod\, n$ to be the remainder when is divided by n .The integer n is called the **modulus**. Thus, for any integer a , we can rewrite equation as:

$$a = qn + r \quad 0 \leq \mathrm{r} < \mathrm{n}; \quad \mathrm{q} = [a/n]$$

$$a = [a/n] \times n + (a\, mod\, n)$$

Example 2.21:

$$11\, mod\, 7 = 4; -11\, mod\, 7 = 3$$

Definition 2.22:

A **graph** G consists of a pair of $(V(G), X(G))$ where $V(G)$ is a non- empty finite set whose elements are called points or vertices and $X(G)$ is a set of unordered pairs of distinct elements of $V(G)$.

Example 2.23: Let $V = \{v_1, v_2, v_3, v_4\}$ and $X = \{\{v_1, v_2\}, \{v_1, v_3\}\{v_1, v_4\}\}$ $G = (V, X)$ is a (4,3) graph.

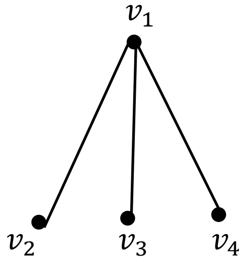

Figure 2.24

Definition 2.25:

A graph is called a **directed graph** if the edges considered represent ordered pairs of vertices. If e = (u, v) is an edge in a directed graph or digraph in short, then u is referred to as the initial vertex and v is referred to as the terminal vertex of the edge e.

Example 2.26: D= $(\{ v_1, v_2, v_3, v_4\}, \{(v_2, v_1), (v_1, v_3), (v_1, v_4)\})$ is a digraph.

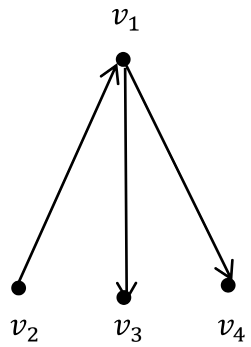

Figure 2.27

Definition 2.28:

An **undirected graph** is the one which does not have directions associated with its edge.

Definition 2.29:

If more than one line joining two vertices are allowed, the resulting graph is **multigraph.**

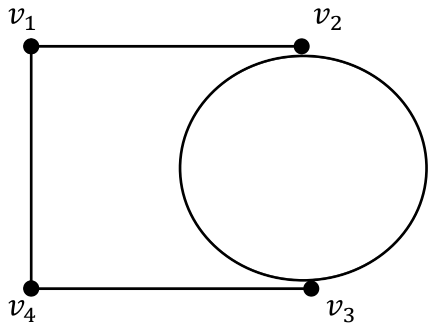

Figure 2.30

Definition 2.31:

A graph G is **simple** if it has no loops and no multiple edges.

Definition 2.32:

If $= \{u, v\} \in X(G)$, the line x is said to join u and v. we write $x = uv$ and we say that the points u ad v are **adjacent**. We also say that the point u and the line x are **incident** with each other.

Definition 2.33:

A graph in which any two distinct points are adjacent is called a **complete graph**. The complete graph with p points is denoted by k_p .

Example 2.34: Complete graph k_5

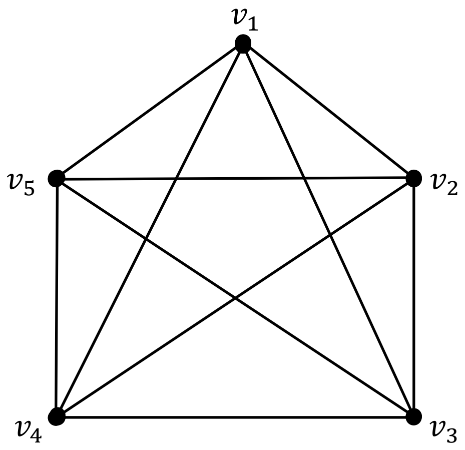

Figure 2.35

Definition 2.36:

A **cycle** is a closed trail in which the vertices are all distinct. The graph consisting of a cycle of length n is denoted by C_n.

Example 2.37: Cycle C_5

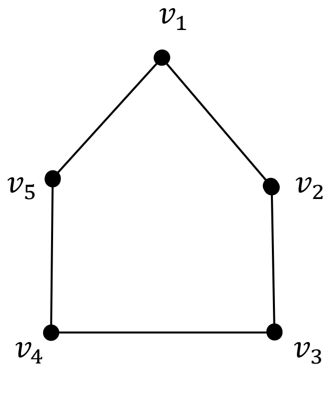

Figure 2.38

Definition 2.39:

A graph H is called a subgraph of G if $\mathrm{V(H)} \subseteq \mathrm{V(G)}\,;\mathrm{E(H)} \subseteq \mathrm{E(G)}$. A subgraph H of G is a **spanning subgraph** of G if $\mathrm{V(H)} = V(G)$

Definition 2.40:

A spanning cycle in a graph is called a Hamiltonian cycle. A graph having a Hamiltonian cycle is called **Hamiltonian graph.**

Definition 2.41:

A complete bipartite graph of the form $K_{1,\,q}$ is called a **star.**

Example 2.42: Star graph $K_{1,\,4}$

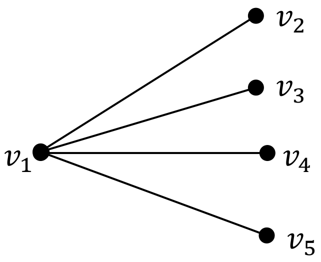

Figure 2.43

CHAPTER 3

Graph Based Encryptions

Chapter 3

Graph Based Encryptions

In this chapter, we discuss about the encryption and decryption using corona graphs.

3.1 Corona of cycle and complete graph

Definition 3.1.1:

The **corona of two graphs** G and H is the graph G⨀H formed by one copy of G and |V(G)| copies of H, where the i^{th} vertex of G is joined to each vertex in the i^{th} copy of H. The corona graph of the cycle C_n with K_1, i.e., $C_n \odot K_1$, is a graph on $2n$ vertices obtained by attaching n pendant edges in a cycle graph C_n.

Example 3.1.2: $C_3 \odot K_1$

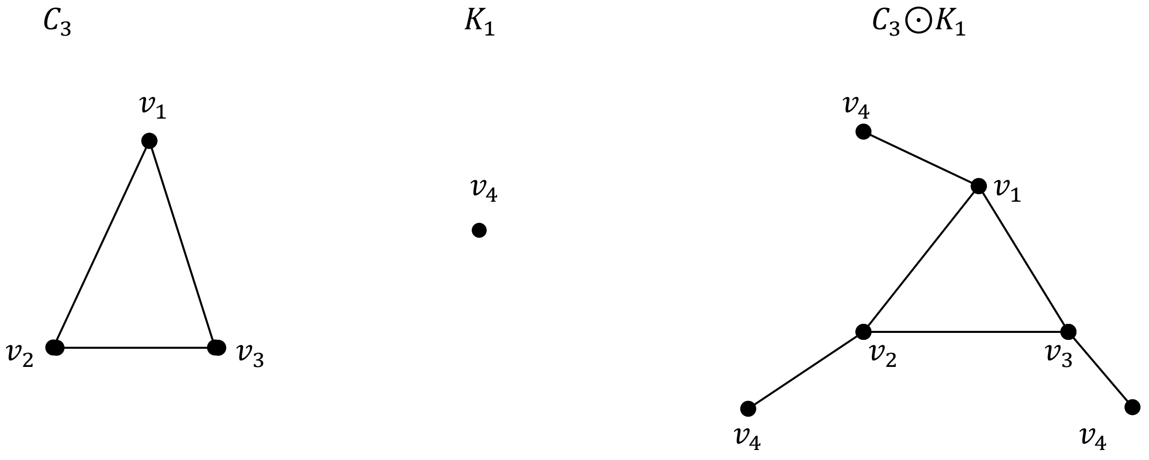

Figure 3.1.3

3.1.4 Algorithm for Encryption:

In this algorithm, the orginal message is converted into the labeled corona graph and sended to the receive, on other hand receiver decrypt the provided graph into the meaningful orginal message.

- First take a plain text of the given length n.
- Give the numerical values to the plain text word.
- Apply shift cipher $e_n(x) = x + n (mod\ 26)$ to each numerical value and get new numerical values, say a_1, a_2, a_3,……,a_n.

- Find a sequence $b_1, b_2, b_3, \ldots, b_n$ of positive integers in increasing order such that

$$gcd(b_i, a_i) = 1 \text{ and } b_i > 26.$$

- Consider a corona graph $C_n \odot K_1$ with 2n vertices and allot weights $b_1, b_2, b_3, \ldots, b_n$ to the vertices, adjacent to pendent vertices.
- Find the inverse of a_i $(mod\ b_i)$ for all i and denote them by c_i, $c_i = (a_i)^{-1}(mod\ b_i)\forall i$.
- Give numeric values $c_1, c_2, c_3, \ldots, c_n$ to pendent vertices. Send this corona graph $C_n \odot K_1$ to the receiver.

3.1.5 Algorithm for decryption:

- First, arrange all the vertices which are adjacent to the pendent vertices in the increasing order as

$$b_1 < b_2 < b_3 < \cdot \cdot \cdot \cdot < b_n.$$

- Find the inverse of c_i modulus their adjacent vertices b_i and denote it by a_i $a_i = c_i^{-1}\ (mod\ b_i)$
- Compute $w_i = a_i - \left(\frac{order\ of\ graph}{2}\right) mod\ 26, \forall i$
- Convert the numerical values of w_i for each i, to the related alphabets.

Illustration 3.1.6:

Encryption:

Let the plain text be “EDGE, convert alphabetic letter to numbers using the encoding table (figure 3.1.7)

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**

O	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
15	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**

Figure 3.1.7 Encoding table

The characters are assigned the numerical values

E = 5 D = 4 G = 7 E = 5

Here length of the word is n = 4

Apply shift cipher, $e_n = x + n(mod\ 26)$

$a_1 = 5 + 4 = 9$, $a_2 = 4 + 4 = 8$, $a_3 = 7 + 4 = 11$, $a_4 = 5 + 4 = 9$

Now the given word is encrypted in the form of

$$I\ \ H\ \ K\ \ L$$

Select the randomly increasing integers b_i such that

$$\gcd(b_i, a_i) = 1\ b_i > 26$$

$$\gcd(b_1, a_1) = \gcd(28,9) = 1,$$

$$\gcd(b_2, a_2) = \gcd(31,8) = 1,$$

$$\gcd(b_3, a_3) = \gcd(35,11) = 1,$$

$$\gcd(b_4, a_4) = \gcd(47,9) = 1.$$

Construct the corona graph $C_4 \odot K_1$ and put the value of b_i to main vertices.

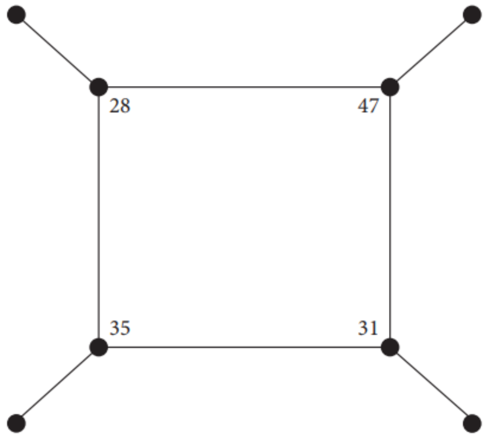

Figure 3.1.8

Now find, $c_i = (a_i)^{-1}\ (mod\ b_i)$

$c_1 = (a_1)^{-1}\ (mod\ b_1) = (9^{-1})\ (mod\ 28)$

$= (9)^{\varphi(28)-1}\,(mod\ 28) = 25$

$c_2 = (a_2)^{-1}\,(mod\ b_2) = (8^{-1})\,(mod\ 31)$

$= 8^{\varphi(31)-1}(\text{mod } 31) = 4$

$c_3 = (a_3)^{-1}(mod\ b_3) = (11^{-1})\,(mod\ 35)$

$= 11^{\varphi(35)-1}\,(\text{mod } 35) = 16$

$c_4 = (a_4)^{-1}\,(mod\ b_4) = (9^{-1})\,(mod\ 47)$

$= 9^{\varphi(47)-1}\,(mod\ 47) = 21$

These c_i values are given to adjacent pendant vertices.

Send this labeled graph to the receiver.

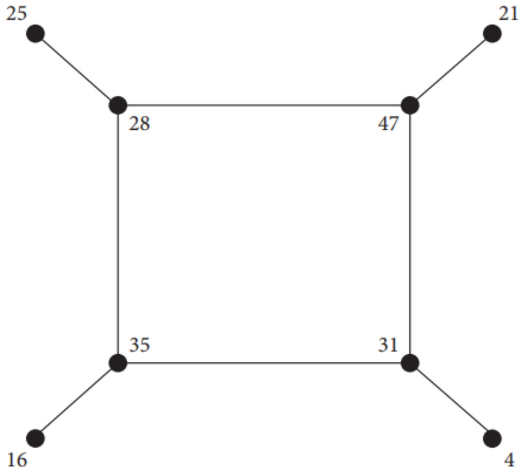

Figure 3.1.9

Decryption:

The recipient, after receiving that labeled graph, arranges the main vertices in ascending order such that $28 < 31 < 35 < 47$

Consider these numbers as values of b_i such that $b_1 < b_2 < b_3 < b_4$.

Take inverse of corresponding pendent vertices with respect to the value of each b_i

$25^{-1}(mod\ 28) = 9 = a_1, \quad 4^{-1}\,(mod\ 31) = 8 = a_2,$

$16^{-1}\,(mod\ 35) = 11 = a_3, \quad 21^{-1}\,(mod\ 47) = 9 = a_4.$

Now for w_i,

$$w_i = \ a_i - \left(\frac{2n}{2}\right) \ mod \ 26$$

Find the values of a_1, a_2, $a_3 \ and \ a_4$:

$w_1 = 9- 2(4)/\ 2\ (mod\ 26) = 5 =$ E,

$w_2 = 8- 2(4)\ /2\ (mod\ 26) = 4 =$ D,

$w_3 = 11- 2(4)/2\ (mod\ 26) = 7 =$ G,

$w_4 = 9 - 2(4)/\ 2\ (mod\ 26) = 5 =$ E.

Finally, we get the original text “EDGE”

3.2 Corona of Star graph

Definition 3.2.1:

The **star graph** S_{n+1} on $n + 1$ vertices can be obtained by corona product of the graph $K_1 \odot \overline{K_n}$.

Example 3.2.2: $K_1 \odot \overline{K_3}$.

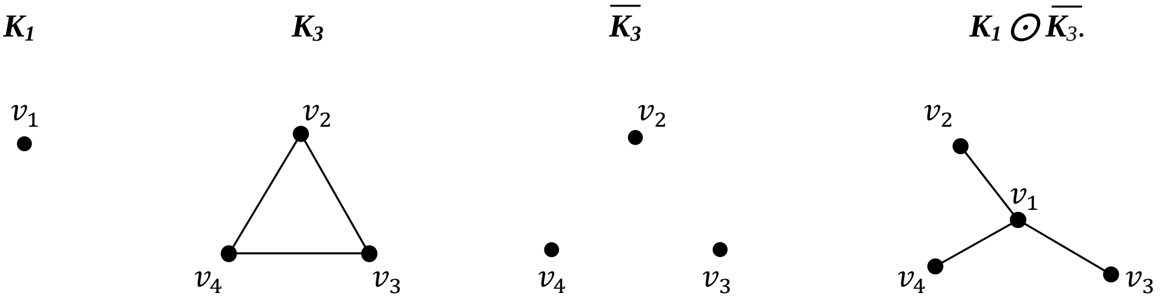

Figure 3.2.3

3.2.4 Algorithm for encryption

- Let us consider the plain text or orginal message M.
- Length of the plain text be L.
- Convert the plaintext into numerical values using the encoding table (fig 3.1.7)
- Apply the shift cipher,

$e_k\,(x) \;=\; x \;+\; k(mod\;26).$ Where $k = L$

- Take a star graph $S_{n+1} = \; K_1 \odot \overline{K}_n$, corresponding to the length of message,
- Now fix the centre vertex, such that

  Number of vertices of star graph =1 + number of alphabetic characters in the text
- Represent the adjacent vertices by adjacent letters in the message.
- Now, label each vertex with respect to their numeric representation in shift cipher.
- Subtract the increasing power of 10 from each vertex label, adjacently with respect to edges, such that

$$v_1 \;-\; 10, v_2 \;-\; 10^2\;, v_3 \;-\; 10^3, \ldots \ldots \ldots \ldots ., v_n -\; 10^n$$

  where $v_i \in$ vertex , $i \in \{1, 2, 3, \ldots, n\}$.
- These resulting values become weight of corresponding edges e_i .
- Give weights in such a way

$$w_1(e_1) < w_2(e_2\,) < w_3\;(e_3) \ldots \ldots \ldots < w_n(e_n)$$

Now, the final graph is the star graph with edge's weight (hiding the vertex label).

Send this graph to the receiver.

3.2.5 Algorithm for Decryption

- Arrange the weight of edges in ascending order.
- Now add up the increasing power of 10, respectively.
- Apply the decryption formulation for shift cipher in the resulting number.
- Decode the characters from encoding table.
- Finally, we get the required text

Illustration 3.2.6:

Encryption:

Let us consider the plain text "**CODE"**.

Length of the message is k = 4

Now, convert the plaintext into numerical values using the encoding table (fig 3.1.7)

C =3 O =15 D = 4 E = 5

consider a star graph $S_5 = K_1 \odot \overline{K_4}$, such that the number of its corner vertices is equal to the length of message. (Figure 3.2.7) shows the respective star graph in such a way that edges are labeled as e_1, e_2, e_3, and e_4.

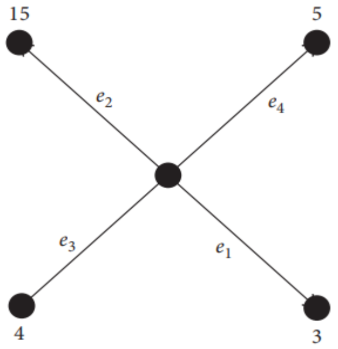

Figure 3.2.7

Apply the shift cipher

$$e_4(x) = x + 4(mod\ 26).$$

$$3 + 4(mod\ 26) = 7$$

$$15 + 4(mod\ 26) = 19$$

$$4 + 4(mod\ 26) = 8$$

$$5 + 4(mod 26) = 9$$

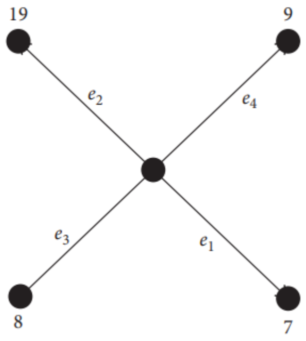

Figure 3.2.8

Now find the weights of edges in such a way

$$w_1(7) < w_2(19) < w_3\ (8) < w_4(9)$$

weight of edge $e_1 = w_1 = 7 - 10 = -3$

weight of edge $e_2 = w_2 = 19 - 10^2 = -81$

weight of edge $e_3 = w_3 = 8 - 10^3 = -992$

weight of edge $e_4 = w_4 = 9 - 10^4 = -9991$

Resulting star graph is

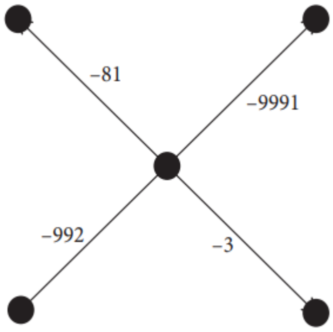

Figure 3.2.9

Decryption:

The recipient receives the labeled graph (figure 3.2.9) which is obtained through the encryption process.

The initial step is arranging the weights of edges in ascending order of mod values, i.e.,

$$|-3| < |-81| < |-992| < |-9991|$$

Add the increasing power of 10 to each adjacent value such that

$$|-3 + 10| = 7$$

$$|-81 + 100| = 19$$

$$|-992 + 1000| = 8$$

$$|-9991 + 10000| = 9$$

Through this mod operation, we get the values: 7, 19, 8, 9

Apply inverse shifting by guessing the number of edges of the star graph, (here we have 4 edges).

So, the values become as follows:

$$7 - 4 = 3,\ 19 - 4 = 15,\ 8 - 4 = 4,\ 9 - 4 = 5.$$

Finally, we get the values 3, 15, 4, 5.

Through the encoding table (fig 3.1.7), we get their respective letters as “CODE”

CHAPTER 4

Graphs for Secure Transmission of Data

Chapter 4

Graphs for Secure Transmission of Data

In this chapter, we discuss about the secure transmission of data using adjacency matrix of the graph.

Definition 4.1:

Let $G = (V, X)$ be a (p, q) graph. Let $V = \{v_1, v_2, v_3, \dots\dots, v_p\}$.The $p \times p$ matrix $A = (a_{ij})$ where

$$a_{ij} = \begin{cases} 1 & if\ \ v_i, v_j\ are\ adjacent \\ 0 & \qquad\qquad otherwise \end{cases}$$

is called the **adjacency matrix** of the graph G.

Definition 4.2:

Let $G = (V, X)$ be a (p, q) graph. Let V = $\{ v_1, v_2, v_3, \dots, v_p\}$ and X =$\{x_1, x_2, x_3, \dots, x_q\}$.

The $p \times q$ matrix $B = (b_{ij})$ where

$$b_{ij} = \begin{cases} 1 & if\ v_i\ is\ incident\ with\ x_i \\ 0 & \qquad\qquad otherwise \end{cases}$$

is called the **incidence matrix** of the graph.

4.3 Encryption Algorithm

This algorithm is used to convert plain text to ciphertext.

- First we take a message or plain text from user which have to be encrypted.
- Use key$_1$ to shift character.
- Encrypt the message by replacing each letter by decided key$_1$.
- Write encrypted message in the form of matrix $(n-1) \times n$ (where n=number of digits in key$_2$) which is decided by sender and receiver.
- Read off the message row by row and permute the order of column.
- Write the output of previous step in matrix form again and read row by row.
- After reading row by row, we get our ciphertext.

4.4 Decryption Algorithm

- Take the ciphertext and use key$_2$ to write ciphertext in the form of matrix (as considered before).
- Arrange the ciphertext in matrix form column by column.
- Read message row by row.
- Again arrange the ciphertext obtained in previous step in matrix form column by column using key$_2$.
- Now decrypt the message with key$_1$.
- Finally we get the plain text.

4.5 Illustration:

Encryption:

- Consider the plain text "THIS IS AN EXAM "
- Let key$_1$= $+3$.
- Encrypt the message by replacing each letter by decided key$_1$.

XLMWMWERIBEQ

- Write encrypted message in the form of matrix $(n-1) \times n$ (where n=number of digits in key$_2$)
- Consider key$_2$ in the form of graph.

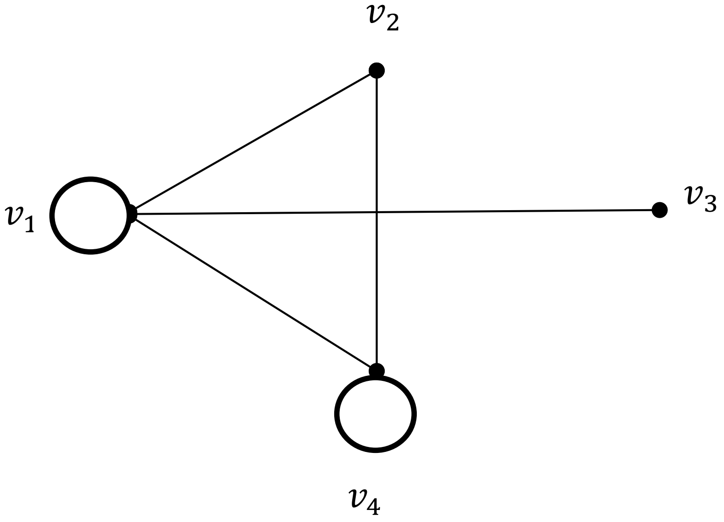

Figure 4.6 Graph for the calculation of key$_2$

- Convert the above graph into adjacent matrix which is used as Key$_2$.

	v_1	**v_2**	**v_3**	**v_4**
v_1	1	1	1	1
v_2	1	0	0	1
v_3	1	0	0	0
v_4	1	1	0	1

Figure 4.7 adjacent matrix of key $_2$

- Now the key$_2$ is 4 2 1 3.
- Read off the message row by row.

4	2	1	3
X	L	M	W
M	W	E	R
I	B	E	Q

Figure 4.8 Message creation from Key$_2$

- Now permute the order of column.

MEELWBWRQXMI

- Write the output of previous step in matrix form read row by row.

4	2	1	3
M	E	E	L
W	B	W	R
Q	X	M	I

Figure 4.9

- After reading row by row, permute the order of column, we get our ciphertext.

EWMEBXLRIMWQ (ciphertext to be sent)

Decryption:

- Arrange the received ciphertext in matrix form column by column using key$_2$.

4	2	1	3
M	E	E	L
W	B	W	R
Q	X	M	I

Figure 4.10

- Read off the message row by row

MEELWBWRQXMI.

- Again arrange the output of previous step in the matrix form column by column using key$_2$.

4	2	1	3
X	L	M	W
M	W	E	R
I	B	E	Q

Figure 4.11

- Obtain the ciphertext by reading row by row XLMWMWERIBEQ
- Now decrypt the message with key$_1$

  Key$_1$$= (-3)$

- Finally we get plain text

  Result: “THIS IS AN EXAM “

CHAPTER 5

Encryption and Decryption using Complete Graph and Hamiltonian Cycle

Chapter 5

Encryption and Decryption using Complete Graph and Hamiltonian Cycle

In this chapter, we discuss about the Encryption and Decryption using complete graph and Hamiltonian cycle.

5.1 Encryption

Definition 5.1.1:

Let G be a complete graph with n vertices labeled as $1, 2, 3, \ldots, n.$ The **complete graph matrix** is the $n \times n$ matrix in which the entry in i th row and j th column is the edge weight on the edge joining two vertices i and j.

Defined as:

$$[a_{ij}]=\begin{cases} weight\ on\ edge\ label\ joining\ the\ vertex\ i\ to\ vertex\ j; & i \neq j \\ 0; & i = j \end{cases}$$

Definition 5.1.2:

A cycle of a graph G containing every vertex of G is called a **Hamiltonian cycle**. A graph containing a Hamiltonian cycle is called Hamiltonian Graph.

5.1.3 Encryption Algorithm:

Step 1(Encryption table construction):

- We assign the numbers $0,1,2, \ldots, m$ to the columns and the numbers $m+1, m+2, m+3, \ldots, n$ to the rows in the table.
- Assign the characters in S randomly in the table. Where S is the set of characters from which the characters are used in the original message.
- Here we use set S containing elements {26 alphabets, blank space, dot (.)}.
- The first letter of the consonants represents the column number, remaining the row number.

- For space, dot and vowel first represents the row number, remaining the column number.

For example, A = 70, F = 57, R = 39, X = 210, O = 90, U = 96, SPACE = 105, DOT = 106.

	0	1	2	3	4	5	6
7	A	B	C	D	E	F	G
8	H	I	J	K	L	M	N
9	O	P	Q	R	S	T	U
10	V	W	X	Y	Z	SPACE	DOT

Figure 5.1.4 Encoding table

Step 2:

- Let M be the plain text (original message) having length n.
- The plain text is represented as vertices in the graph.
- We take a complete graph K_n where ‘n’ is the total number of characters in the original message.
- Convert the message into numerical values using (figure 5.1.4).
- Assign these values to the vertices of complete graph K_n.
- Label the edges by taking the modulus of differences of labeling of respective connecting vertices.

Step 3:

- Construct the complete graph matrix A, with the help the of labeled complete graph K_n.
- Remove the inside edges of the complete graph and construct a cycle.

- Now obtain the cycle matrix B.

Step 4:

- Store the diagonal entries in matrix B with the respective numeric value in the (figure 3.1.7) of the character in the orginal message M.
- Now modified matrixes B is obtained and denote it by B^*.

Step 5:

- Multiply matrix A with matrix B^* to obtain a new matrix N.

Step 6:

- The key matrix $\boldsymbol{K}$ is an upper triangular matrix of order $n \times n$. Where 'n' is the number of characters in the original message.

$$\boldsymbol{k} = \begin{bmatrix} \mathbf{1} & \mathbf{2} & .. & .. & \boldsymbol{n-1} & \boldsymbol{n} \\ \mathbf{0} & \mathbf{1} & \mathbf{2} & .. & .. & \boldsymbol{n-1} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{2} & .. & .. \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{2} & .. \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{2} \end{bmatrix}$$

Figure 5.1.5 key matrix

- Multiply the matrix N with a key '$\boldsymbol{K}$' to get first cipher matrix C_1.

Step 7:

Choose a Hamiltonian cycle from the complete graph. Since any complete graph contains total $(n-1)!$ Hamiltonian cycles, for choosing the required Hamiltonian cycle, we will use Nearest-Neighbor Algorithm.

Nearest-Neighbor Algorithm

- Choose a vertex having initial character of the original message as starting point.
- Go to the next vertex, which is having an edge with smallest labeling on it.
- If labeling on two or more edges are same, choose random vertex, otherwise go to next.
- Repeat, till the Hamiltonian cycle is obtained.

Step 8:

- Add the edge labeling obtained while moving on Hamiltonian cycle.
- Let sum be “S”.
- It is used as second key.

Step 9:

- Apply $mod\ S$ on every element of first cipher matrix C_1 to obtain a new final cipher matrix C_2.
- The ciphertext contains matrix C_2 in a linear format.

5.1.6 Illustration:

Encryption:

- Let us consider the original message “GRAPH”.
- It has 5 characters, so we will form a complete graph K_5.
- Assign these characters to the vertices of complete graph.
- Now find out the numerical values for each of the character with the help of encoding table (figure 5.1.4).

G = 67, R = 39, A = 70, P = 19, H = 08.

V_1 = 67, V_2 = 39, V_3 = 70, V_4 = 19, V_5 = 08.

- Label the edges by taking the modulus of differences of labeling of respective connecting vertices.

$$e_1 = |v_1 - v_2| = |67 - 39| = 28,$$

$$e_2 = |v_2 - v_3| = |39 - 70| = 31,$$

$$e_3 = |v_3 - v_4| = |70 - 19| = 51,$$

$$e_4 = |v_4 - v_5| = |19 - 08| = 11,$$

$$e_5 = |v_5 - v_1| = |08 - 67| = 59,$$

$$e_6 = |v_1 - v_3| = |67 - 70| = 03,$$

$$e_7 = |\, v_1 \text{-}\, v_4| = |67 - 19| = 48,$$

$$e_8 = |\, v_2 \text{-}\, v_4| = |39 - 19| = 20,$$

$$e_9 = |\, v_2 \text{-}\, v_5| = |39 - 08| = 31,$$

$$e_{10} = |\, v_3 \text{-}\, v_5| = |70 - 08| = 62.$$

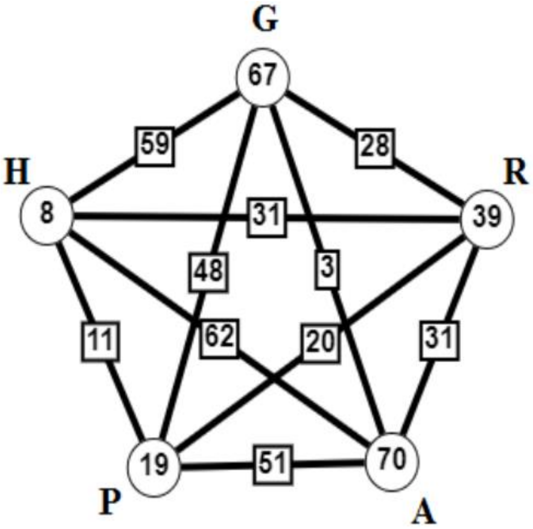

Figure 5.1.7 Complete Graph K₅

- Construct the complete graph matrix A, with the help the of labeled complete graph K_5

$$A = \begin{array}{c|ccccc} & \mathbf{G} & \mathbf{R} & \mathbf{A} & \mathbf{P} & \mathbf{H} \\ \hline \mathbf{G} & 0 & 28 & 3 & 48 & 59 \\ \mathbf{R} & 28 & 0 & 31 & 20 & 31 \\ \mathbf{A} & 3 & 31 & 0 & 51 & 62 \\ \mathbf{P} & 48 & 20 & 51 & 0 & 11 \\ \mathbf{H} & 59 & 31 & 62 & 11 & 0 \end{array}$$

Figure 5.1.8 Complete graph matrix

- Remove the inside edges of the complete graph K_5 and construct a cycle of length 5.
- Obtain a matrix ‘B’ from the cycle.

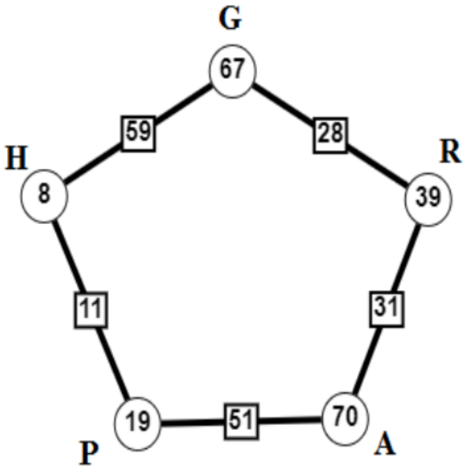

Figure 5.1.9 Cycle C_5

- The cycle matrix is prepared in a similar manner to the complete graph matrix with the cycle.

$$\boldsymbol{B} = \begin{bmatrix} \mathbf{0} & \mathbf{28} & \mathbf{0} & \mathbf{0} & \mathbf{59} \\ \mathbf{28} & \mathbf{0} & \mathbf{31} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{31} & \mathbf{0} & \mathbf{51} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{51} & \mathbf{0} & \mathbf{11} \\ \mathbf{59} & \mathbf{0} & \mathbf{0} & \mathbf{11} & \mathbf{0} \end{bmatrix}$$

Figure 5.1.10 Cycle matrix

- Replace the diagonal entries in matrix B with number value of original message from the alphabet encoding table(figure 3.1.7)

Now we obtain a new matrix ‘B*’

$$\boldsymbol{B^*} = \begin{bmatrix} \mathbf{7} & \mathbf{28} & \mathbf{0} & \mathbf{0} & \mathbf{59} \\ \mathbf{28} & \mathbf{18} & \mathbf{31} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{31} & \mathbf{1} & \mathbf{51} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{51} & \mathbf{16} & \mathbf{11} \\ \mathbf{59} & \mathbf{0} & \mathbf{0} & \mathbf{11} & \mathbf{8} \end{bmatrix}$$

Obtain new matrix ‘N’ by $A \times B^*$as follows,

$$\mathbf{N}= \boldsymbol{A} \times \boldsymbol{B^*} = \begin{bmatrix} \mathbf{0} & \mathbf{28} & \mathbf{3} & \mathbf{48} & \mathbf{59} \\ \mathbf{28} & \mathbf{0} & \mathbf{31} & \mathbf{20} & \mathbf{31} \\ \mathbf{3} & \mathbf{31} & \mathbf{0} & \mathbf{51} & \mathbf{62} \\ \mathbf{48} & \mathbf{20} & \mathbf{51} & \mathbf{0} & \mathbf{11} \\ \mathbf{59} & \mathbf{31} & \mathbf{62} & \mathbf{11} & \mathbf{0} \end{bmatrix} \times \begin{bmatrix} \mathbf{7} & \mathbf{28} & \mathbf{0} & \mathbf{0} & \mathbf{59} \\ \mathbf{28} & \mathbf{18} & \mathbf{31} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{31} & \mathbf{1} & \mathbf{51} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{51} & \mathbf{16} & \mathbf{11} \\ \mathbf{59} & \mathbf{0} & \mathbf{0} & \mathbf{11} & \mathbf{8} \end{bmatrix}$$

$$\mathbf{N} = \begin{bmatrix} \mathbf{4265} & \mathbf{597} & \mathbf{3319} & \mathbf{1570} & \mathbf{1000} \\ \mathbf{2025} & \mathbf{1745} & \mathbf{1051} & \mathbf{2242} & \mathbf{2120} \\ \mathbf{4547} & \mathbf{642} & \mathbf{3562} & \mathbf{1498} & \mathbf{1234} \\ \mathbf{1545} & \mathbf{3285} & \mathbf{671} & \mathbf{2722} & \mathbf{2920} \\ \mathbf{1281} & \mathbf{4132} & \mathbf{1584} & \mathbf{3338} & \mathbf{3602} \end{bmatrix}$$

- Construct the key matrix ‘K’. As the original message has 5 characters in it, the size of the key matrix will be 5 × 5.

$$\boldsymbol{K} = \begin{bmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} & \mathbf{5} \\ \mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{3} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{2} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} \end{bmatrix}$$

- Obtain the first cipher matrix C_1 by multiplying key matrix K with matrix N

$C_1 = N \times K$

$$= \begin{bmatrix} \mathbf{4265} & \mathbf{597} & \mathbf{3319} & \mathbf{1570} & \mathbf{1000} \\ \mathbf{2025} & \mathbf{1745} & \mathbf{1051} & \mathbf{2242} & \mathbf{2120} \\ \mathbf{4547} & \mathbf{642} & \mathbf{3562} & \mathbf{1498} & \mathbf{1234} \\ \mathbf{1545} & \mathbf{3285} & \mathbf{671} & \mathbf{2722} & \mathbf{2920} \\ \mathbf{1281} & \mathbf{4132} & \mathbf{1584} & \mathbf{3338} & \mathbf{3602} \end{bmatrix} \times \begin{bmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} & \mathbf{5} \\ \mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{3} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{2} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} \end{bmatrix}$$

$$\mathbf{C_1} = \begin{bmatrix} \mathbf{4265} & \mathbf{9127} & \mathbf{17308} & \mathbf{27059} & \mathbf{37810} \\ \mathbf{2025} & \mathbf{5795} & \mathbf{10616} & \mathbf{17679} & \mathbf{26862} \\ \mathbf{4547} & \mathbf{9736} & \mathbf{18487} & \mathbf{28736} & \mathbf{40219} \\ \mathbf{1545} & \mathbf{6375} & \mathbf{11876} & \mathbf{20099} & \mathbf{31242} \\ \mathbf{1281} & \mathbf{6694} & \mathbf{13691} & \mathbf{24026} & \mathbf{37963} \end{bmatrix}$$

Nearest-Neighbor Algorithm

- Start from the vertex of initial character of original message that is ‘G’.

- Next, we will choose vertex having minimum weight on it than others.

- Continue this process and we get required Hamiltonian cycle as

G→A→R→P→H→G.

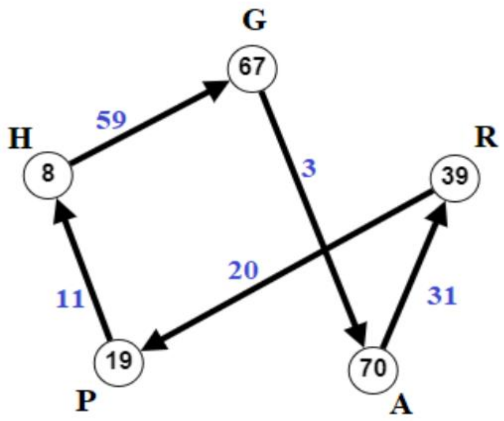

Figure 5.1.11 Hamiltonian cycle

Find second key ‘S’ $S = 3 + 31 + 20 + 11 + 59 = 124.$

- Apply mod 124 on every element of the first cipher matrix C_1 to get new final cipher matrix. Hence the final cipher matrix C_2 is C_2= C_1 $multiplication\ mod$ 124

$$\boldsymbol{C_2}= \begin{bmatrix} \mathbf{4265} & \mathbf{9127} & \mathbf{17308} & \mathbf{27059} & \mathbf{37810} \\ \mathbf{2025} & \mathbf{5795} & \mathbf{10616} & \mathbf{17679} & \mathbf{26862} \\ \mathbf{4547} & \mathbf{9736} & \mathbf{18487} & \mathbf{28736} & \mathbf{40219} \\ \mathbf{1545} & \mathbf{6375} & \mathbf{11876} & \mathbf{20099} & \mathbf{31242} \\ \mathbf{1281} & \mathbf{6694} & \mathbf{13691} & \mathbf{24026} & \mathbf{37963} \end{bmatrix} \times \boldsymbol{mod}\ \mathbf{124}$$

- C_2 matrix stores the remainders after each entry of C_1 is divided by 124

$$\boldsymbol{C_2} = \begin{bmatrix} \mathbf{49} & \mathbf{75} & \mathbf{72} & \mathbf{27} & \mathbf{114} \\ \mathbf{41} & \mathbf{91} & \mathbf{76} & \mathbf{71} & \mathbf{78} \\ \mathbf{83} & \mathbf{64} & \mathbf{11} & \mathbf{92} & \mathbf{43} \\ \mathbf{57} & \mathbf{51} & \mathbf{96} & \mathbf{11} & \mathbf{118} \\ \mathbf{41} & \mathbf{122} & \mathbf{51} & \mathbf{94} & \mathbf{19} \end{bmatrix}$$

- The quotient matrix Q stores the results of the division (quotients) after each entry of C_1 is divided by 124

$$\boldsymbol{Q} = \begin{bmatrix} \mathbf{34} & \mathbf{73} & \mathbf{139} & \mathbf{218} & \mathbf{304} \\ \mathbf{16} & \mathbf{46} & \mathbf{85} & \mathbf{142} & \mathbf{216} \\ \mathbf{36} & \mathbf{78} & \mathbf{149} & \mathbf{231} & \mathbf{324} \\ \mathbf{12} & \mathbf{51} & \mathbf{95} & \mathbf{162} & \mathbf{251} \\ \mathbf{10} & \mathbf{53} & \mathbf{110} & \mathbf{193} & \mathbf{306} \end{bmatrix}$$

- Hence, for the plain text “GRAPH”, the ciphertext will be (the entries of C_2 from left to right)

49 75 72 27 114 41 91 76 71 78 83 64 11 92 43 57 51 96 11 118 41 122 51 94 19

5.2 Decryption

5.2.1 Decryption Algorithm:

- Write the linear message in matrix form C_2.
- Obtain matrix C_1 from matrix C_2 with the use of key S.
- Compute matrix 'N' with the help of cipher matrix 'C_1' and inverse of key matrix 'K' (i.e. N = C_1×K^{-1}).
- Compute B^* with the help of $A^{-1}$and N (i.e. B^* = A^{-1} × N).
- Write the diagonal entries from the matrix B^* to compute the original message by decoding these values with the help of alphabet encoding table (fig 3.1.7).
- Finally we get the plain text.

5.2.2 Illustration:

Decryption:

- The input for decryption C_2 (final ciphertext), Q (quotient matrix), S(second key) = 124 using Hamiltonian cycle , K (key matrix), A (complete graph matrix)
- Write the ciphertext 49 75 72 27 114 41 91 76 71 78 83 64 11 92 43 57 51 96 11 118 41 122 51 94 19 in the final cipher matrix C_2 form as

$$\boldsymbol{C_2} = \begin{bmatrix} \mathbf{49} & \mathbf{75} & \mathbf{72} & \mathbf{27} & \mathbf{114} \\ \mathbf{41} & \mathbf{91} & \mathbf{76} & \mathbf{71} & \mathbf{78} \\ \mathbf{83} & \mathbf{64} & \mathbf{11} & \mathbf{92} & \mathbf{43} \\ \mathbf{57} & \mathbf{51} & \mathbf{96} & \mathbf{11} & \mathbf{118} \\ \mathbf{41} & \mathbf{122} & \mathbf{51} & \mathbf{94} & \mathbf{19} \end{bmatrix}$$

- Obtain the first cipher matrix C_1 with the use of second key $S = 124$ and final cipher matrix C_2.

  $[Q]_{ij} \times 124 + [C_2]_{ij} = [C_1]_{ij}$ where $[Q]_{ij}$, $[C_2]_{ij}$ *and* $[C_1]_{ij}$ are entries of matrices Q, C_2 and C_1 respectively at the i^{th} row and j^{th} column.

For instance, $4265 = 34 \times 124 + 49$

$$\boldsymbol{C_1} = \begin{bmatrix} \mathbf{4265} & \mathbf{9127} & \mathbf{17308} & \mathbf{27059} & \mathbf{37810} \\ \mathbf{2025} & \mathbf{5795} & \mathbf{10616} & \mathbf{17679} & \mathbf{26862} \\ \mathbf{4547} & \mathbf{9736} & \mathbf{18487} & \mathbf{28736} & \mathbf{40219} \\ \mathbf{1545} & \mathbf{6375} & \mathbf{11876} & \mathbf{20099} & \mathbf{31242} \\ \mathbf{1281} & \mathbf{6694} & \mathbf{13691} & \mathbf{24026} & \mathbf{37963} \end{bmatrix}$$

Compute inverse of matrix K

$$\boldsymbol{k^{-1}} = \begin{bmatrix} \mathbf{1} & \mathbf{-2} & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{-2} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{-2} & \mathbf{1} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{-2} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} \end{bmatrix}$$

Compute matrix N with the help of cipher matrix ‘C_1’ and inverse of key matrix ‘K’

$N = \boldsymbol{C_1} \times \boldsymbol{k^{-1}}$

$$= \begin{bmatrix} \mathbf{4265} & \mathbf{9127} & \mathbf{17308} & \mathbf{27059} & \mathbf{37810} \\ \mathbf{2025} & \mathbf{5795} & \mathbf{10616} & \mathbf{17679} & \mathbf{26862} \\ \mathbf{4547} & \mathbf{9736} & \mathbf{18487} & \mathbf{28736} & \mathbf{40219} \\ \mathbf{1545} & \mathbf{6375} & \mathbf{11876} & \mathbf{20099} & \mathbf{31242} \\ \mathbf{1281} & \mathbf{6694} & \mathbf{13691} & \mathbf{24026} & \mathbf{37963} \end{bmatrix} \times \begin{bmatrix} \mathbf{1} & \mathbf{-2} & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{-2} & \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{-2} & \mathbf{1} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{-2} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} \end{bmatrix}$$

$$N = \begin{bmatrix} 4265 & 597 & 3319 & 1570 & 1000 \\ 2025 & 1745 & 1051 & 2242 & 2120 \\ 4547 & 642 & 3562 & 1498 & 1234 \\ 1545 & 3285 & 671 & 2722 & 2920 \\ 1281 & 4132 & 1584 & 3338 & 3602 \end{bmatrix}$$

- Compute inverse matrix of A

$$\boldsymbol{A^{-1}} = \begin{bmatrix} \mathbf{-31/168} & \mathbf{1/56} & \mathbf{1/6} & \mathbf{0} & \mathbf{0} \\ \mathbf{1/56} & \mathbf{-3/70} & \mathbf{0} & \mathbf{1/40} & \mathbf{0} \\ \mathbf{1/6} & \mathbf{0} & \mathbf{-59/372} & \mathbf{0} & \mathbf{1/124} \\ \mathbf{0} & \mathbf{1/40} & \mathbf{0} & \mathbf{-31/440} & \mathbf{1/22} \\ \mathbf{0} & \mathbf{0} & \mathbf{1/124} & \mathbf{1/22} & \mathbf{-51/1364} \end{bmatrix}$$

- Now find the B^* matrix with the help of $B^* = \boldsymbol{A^{-1}} * N$

$$\boldsymbol{B}^* = \begin{bmatrix} -31/168 & 1/56 & 1/6 & 0 & 0 \\ 1/56 & -3/70 & 0 & 1/40 & 0 \\ 1/6 & 0 & -59/372 & 0 & 1/124 \\ 0 & 1/40 & 0 & -31/440 & 1/22 \\ 0 & 0 & 1/124 & 1/22 & -51/1364 \end{bmatrix} \times$$

$$\begin{bmatrix} 4265 & 597 & 3319 & 1570 & 1000 \\ 2025 & 1745 & 1051 & 2242 & 2120 \\ 4547 & 642 & 3562 & 1498 & 1234 \\ 1545 & 3285 & 671 & 2722 & 2920 \\ 1281 & 4132 & 1584 & 3338 & 3602 \end{bmatrix}$$

$$\boldsymbol{B}^* = \begin{bmatrix} 7 & 28 & 0 & 0 & 59 \\ 28 & 18 & 31 & 0 & 0 \\ 0 & 31 & 1 & 51 & 0 \\ 0 & 0 & 51 & 16 & 11 \\ 59 & 0 & 0 & 11 & 8 \end{bmatrix}$$

- Now we got diagonal entries of matrix B* as 7 18 1 16 8 ,then decode the numerical values,

We get 7 = G, 18 = R, 1 = A, 16 = P, 8 = H.

Hence the original text is “GRAPH”.

CHAPTER 6

Conclusion

Chapter 6

Conclusion

In this project we discussed some encryption algorithms for secure transmission of message using some special corona graphs. In the first algorithm, encryption and decryption is performed by using a specific corona graph $C_n \odot K_1$ along with some basic algebraic properties. In second algorithm, we used a certain labeling of vertices and edges of the star graph $K_1 \odot \overline{K_n}$.

Also we discussed about the algorithm using adjacent matrix of graph to obtain keys for encryption and decryption. This algorithm is secured by "Double Transposition column" method with graph as a key has the various advantages over simple algorithm. It is more difficult to cryptanalyst. Due to the use of graph for developing of key$_2$, the result (plaintext) cannot be cracked and hence security is enhanced.

Further, we studied about an encryption technique for encrypting the message with the use of complete graph and a cycle to generate a ciphertext using 2 keys one of them is formed by the use of Hamiltonian cycle.

Therefore, a multilayered hiding of the original plain text is obtained using the concepts from Graph Theory which gives a much hidden ciphertext serving the purpose of a highly safe data transfer.

References

[1] Amudha P, Charles Sagayaraj A.C, Shantha Sheela A.C, “*An Application of Graph Theory in Cryptography*”, International Journal of Pure and Applied Mathematics, Vol. 119 No. 13, 2018.

[2] Baizhu Ni, Rabiha Qazi, Shafiq Ur Rehman and Ghulam Farid, “*Some Graph-Based Encryption Schemes*”, Hindawi Journal of Mathematics, 2021.

[3] Balakrishna R, Ranganathan K, “*A Textbook of Graph Theory*”, Springer Verlag, (2000)

[4] Behrouz A Forouzan, Debdeep Mukhopadhyay, “*Cryptography and Network Security*” 3\E McGraw Hill Education (India) private limited, (2017)

[5] Dharmendra Kumar Gurjar, Auparajita Krishnaa, “*Complete Graph and Hamiltonian Cycle in Encryption and Decryption*”, International Journal of Mathematics Trends and Technology Vol. 67, No.12, 2021.

[6] Gurusharan Kaur, Namrata Tripathi, “*Applying Graph Theory to Secure Data by Cryptography*”, International Journal of Linguistics and Computational Applications (IJLCA) Vol. 8, No. 1, 2021.

[7] Wael Mahmoud Al Etaiwi, “*Encryption Algorithm Using Graph Theory*”, Journal of Scientific Research & Reports Vol.3, No. 19, 2014.

[8] Yamuna M, Meenal Gogia, Ashish Sikka, Jazib Hayat Khan. Md, “*Encryption using graph theory and linear algebra*”, International Journal of Computer Application Vol. 5 No. 2, 2012.