Project Report

On

MATHEMATICAL TOOLS USING IN CRYPTOGRAPHY

Submitted

in partial fulfilment of the requirements for the degree of

BACHELOR OF SCIENCE

in

MATHEMATICS

by

ANU UDAYAN

(AB20BMAT028)

Under the Supervision of

DR. ELIZABETH RESHMA MT

DEPARTMENT OF MATHEMATICS

ST. TERESA'S COLLEGE (AUTONOMOUS)

ERNAKULAM, KOCHI - 682011

APRIL 2023

ST. TERESA'S COLLEGE (AUTONOMOUS), ERNAKULAM

CERTIFICATE

This is to certify that the dissertation entitled, **MATHEMATICAL TOOLS USING IN CRYPTOGRAPHY** is a bonafide record of the work done by **ANU UDAYAN** under my guidance as partial fulfillment of the award of the degree of **Bachelor of Science in Mathematics** at St. Teresa's College (Autonomous), Ernakulam affiliated to Mahatma Gandhi University, Kottayam. No part of this work has been submitted for any other degree elsewhere.

Date:21/02/2023
Place: Ernakulam

Dr. Elizabeth Reshma MT
Assistant Professor,
Department of Mathematics,
St. Teresa's College(Autonomous),
Ernakulam.

Dr.Ursala Paul
Assistant Professor and Head ,
Department of Mathematics,
St. Teresa's College(Autonomous),
Ernakulam.

External Examiners

1:..... 2: .....

DECLARATION

I hereby declare that the work presented in this project is based on the original work done by me under the guidance of Dr.Elizabeth Reshma MT, Assistant Professor, Department of Mathematics, St.Teresa's College(Autonomous), Ernakulam and has not been included in any other project submitted previously for the award of any degree.

Place: Ernakulam. **ANU UDAYAN**

Date: 21/02/2023 **AB20BMAT028**

ACKNOWLEDGEMENT

I must mention several individuals who encouraged me to carry this work. Their continuous invaluable knowledgably guidance throughout the course of this study helped us to complete the work up to this stage.

I am very grateful to our project guide Dr.Elizabeth Reshma MT for her guidance and support throughout the work.I also want to express our gratitude to our classmates, who assisted me in formulating our research topics by sharing their knowledge. Last but not least, I would like to express our heartfelt gratitude to God Almighty for always being our emotional rock and teaching us how to confront every challenge with intelligence and confidence.

Place: Ernakulam. ANU UDAYAN

Date:21/02/2023 **AB20BMAT028**

Contents

Chapter 1

INTRODUCTION

Cryptography is an art of communication between two people by keeping the information not known to others. It is based upon two factors, namely encryption and decryption. Encryption means the process of transformation of information into a secret code, which hides the true meaning. On the other hand, Decryption means the transformation of the coded message back to original form. Encryption and decryption require a secret code which is known only to the sender and the receiver. This secret code is called a key. Encrypted text transformed from plaintext using encryption algorithm is called cipher text. Cryptography Algorithm is classified mainly into two major types: Symmetric-key cryptography and public-key cryptography. In symmetric-key encryption the message is encrypted using a key and the same key is used to decrypt the message, which makes it easy to use but less secure. The Data Encryption Standard (DES) and the Advance Encryption Standard (AES) are examples of Symmetric-key cryptography methods. In public-key cryptography each sender and receiver uses two different keys- public key and private key to encrypt and decrypt data, the public key is freely distributed while private key is kept secret . It is more secure than the symmetric key cryptography. The message which is to be transmitted is encrypted to cipher text at the encryption process and the secret code is obtained.

1.1 History of Cryptography

The history of cryptography begins thousands of years ago. The art of cryptography is considered to be born along with the art of writing. From ages human had two inherent needs- to share information and to communicate selectively. These needs set off the rise of art of coding in such a way that only intended people can have the access to the information. Unauthorized people can't extract any information, even if the scrambled message is acessed by them.

The first known invented cryptography was found in the 1900 BC in the main chamber of the tomb of the nobleman Khnumhotep II, in Egypt. Hieroglyphs carved into monuments from Egypt's old kingdom (4500+ year ago) is the earliest known use of cryptography found in non-standard. In most majors early Civilization, evidences of some use of cryptography has been identified.“Risalah fi istikhraj al-mu'amma” is the book wrote by Al-kindi(manuscript for the Deciphering Cryptographic Messages), in 850 CE. He was a pioneer in cryptoanalysis and cryptology, and devised new methods of breaking cipher, including the frequency analysis method.Until the development of the poly alphabetic cipher, essentially all ciphers remained vulnerable to the cryptanalytic technique of frequency analysis. Leon Battista Alberti has explained, the polyalphabetic cipher, around the year 1467, for which he was called the “father of Western Cryptology”. Kautilya has written a state craft named “Arthashastra” which describe the assignment given to spice in secret writing. Edgar Allan Poe used systematic methods to solve cipher in the 1840s. He placed a notice of his abilities in the Philadelphia paper, inviting submissions of cipher, of which he proceeded to solve almost all. It created a public stir for some months. Later he wrote an essay on methods of cryptography which is useful in proved introduction for novice British cryptanalysts codes and German codes and cipher during World War I. Teletype cipher which is introduced by Gilbert vernam in 1917, kept a paper tape, is combined character with plaintext message to produce the cypher text. This led to the develop-

ment of electromechanical devices as cipher machines. Mechanical and electromechanical machines were widely used during World War II, although-where such machines were impractical-manual systems continued in use. Nazi Germany widely used the Enigma machine, where as SIGABA was used by British army. The earlier invented method of cryptography is a Roman method popularly known as Ceaser shift method. Around 100 BC, Julius Caesar used a form of encryption, which was later known as Caesar cipher to convey secret message to army generals in war front. During the beginning of the 19th, Century Hebern developed an electro mechanical contraption which was known as Hebern rotor machine. A single router was used in the encryption in which the secret key is embedded in a rotating disc. Later the Enigma machine was invented by a German Engineer Arthur Scherbius during the end of World War I which used three or more rotators for its functioning. This Enigma machine was heavily used by the German forces during the Second World War. In the early 1970s, due to the high demand on encryption by the customers, IBM formed a group "Crypto group" headed by Horst-Feistal and they have the signed a site for called Lucifer. Eventually Lucifer was accepted worldwide and was called DES. Further in 2000, the AES was developed.

1.2 Evolution of Cryptography

After the European Renaissance, various Italian and papal states led the rapid proliferation of cryptographic techniques. Attack techniques and various analysis were researched in this era to break the secret codes. Coding techniques has improved such as Vigenere coding came in to existence in the 15 th century, which offered moving letters in messages with a number of variable places instead of moving them the same number of places.

A technique for encrypting alphabetic text is the Vigenere Cipher. It employs a straightforward method of polyalphabetic substitution. Any substitution-based encryption that employs numerous substitution alphabets is referred to as a polyalphabetic cypher. With the Vigenère

square or Vigenère table, the original text is encrypted.The table has the 26 potential Caesar Ciphers written out 26 times in various rows, with each alphabet shifting cyclically to the left in comparison to the previous alphabet. The cipher switches to an alphabet from one of the rows at various stages of the encryption process.Each point's alphabet is determined by a keyword that appears repeatedly.

After 19th century, cryptography approaches to encryption to the more sophisticated art and science of information security.
At the close of World War I, German engineer Arthur Scherbius created the Enigma machine.There were several distinct Enigma models made, but the German military versions with a plugboard were the most intricate.There were several distinct Enigma models made, but the German military versions with a plugboard were the most intricate. Models from Italy and Japan were also in use. Enigma gained widespread recognition in the military after being adopted (in a somewhat modified version) by the German Navy in 1926 and the German Army and Air Force shortly after. German military strategy prior to World War I focused on quick, mobile units and blitzkrieg tactics, which rely on radio transmission for command and coordination. Radio signals had to be encrypted securely since enemies would probably try to intercept them. The Enigma machine satisfied that need by being small and portable.
In the period of World War II, cryptography and cryptanalysis became excessively mathematical. Government organizations, military units, and some corporate houses started adopting the applications of cryptography. They use cryptography as a guard their secrets from others. The arrival of computers and the internet has bought effective cryptography within the reach of common people.
Quantum computing:These innovative breakthroughs and discoveries in cryptography are fostering a promising future for the discipline. The biggest shift that's supposedly coming is quantum computing. The computer capacity at our disposal can be exponentially increased via quantum computing, which uses the characteristics of the superposi-

tioned particles. This implies that the cryptographic operations that are currently too complex to operate on silicon chips could be made feasible on a quantum device, potentially rendering current encryption obsolete.

Homomorphic Encryption:Nowadays, we encrypt data both during internet transmission and while it is at rest on a storage device. Nevertheless, in order to utilise or analyse data, we must first decrypt it, which poses a security risk. A novel solution to this issue is homomorphic encryption, which enables users to process data without first decrypting it. We handle encrypted data using homomorphic encryption, and we generate encrypted output. Although this is not a new concept, recent advances that significantly increased performance have pushed the prospect of effective encrypted data processing back to the fore.

1.3 Types of Cryptography

Cryptography is broadly classified into two. They are symmetric key cryptography and asymmetric key cryptography.

1.3.1 Symmetric Key Cryptography

The cryptographic method in which same key is used for both encryption and decryption of information is called symmetric key cryptography. Therefore the sender and the receiver will be having access for the key. Since both the parties have access to the secret key, it is considered as a main drawback of the symmetric key encryption compared to the public key encryption. Symmetric key Cryptography is commonly used in today's internet. AES and DES are the common Encryption Algorithm used in symmetric key cryptography. It is faster than asymmetric key cryptography. Symmetric key encryption either uses stream cipher or block cipher. The stream cipher encrypt digits or letters of a message there as block cipher consider bits as a single unit and encrypt them as a whole. Payment applications, generation random number generation or hashing are some if the applications of symmetric key

cryptography.

1.3.2 Asymmetric Key Cryptography

Asymmetric key Cryptography is a public key cryptographic scheme which requires two different keys. One key is used to the encryption process and other is use for the decryption of the cipher text. One of the key in the asymmetric key encryption is a public key which is accessible to the public and the other is kept private which is known as private key. Asymmetric key encryption is also known as public key cryptography. The advantage of asymmetric Cryptography compared to symmetric key cryptography is the non-Reliance on a single point of failure of key. Asymmetric key Cryptography has a increase data security. Since asymmetric key encryption uses a longer key for the encryption process, it results in a slower encryption speed. Digital signature, TLS or SSL handshake, crypto currency are some of the application of asymmetric key cryptography.

1.3.3 Hashing

Hashing is the process of transforming any given key or a string of characters into another value.Implementing hash tables is the most well-liked application of hashing. Value and key pairs are kept in a list that can be accessed by a hash table's index. The hash function would map the keys to the size of the table because value and key pairs are infinite. The index for a given element is then changed to a hash value.Hashing uses functions or algorithms to map object data to a representative integer value. A hash can then be used to narrow down searches when locating these items on that object data map.

1.4 Cryptography in Movies

Some of the movies has been released with Cryptography as its base. Sneakers, The Da Vinci code, Skyfall, The imitation game, A Christmas story are some to mention. Sneakers movie plots the story of a bunch of people who holds the power to unlock any computers encryp-

tion technology. The Da Vinci Code is based on the basiling novel by Dan Brown. It plots the story of a person who crack various encrypted message to solve a crime. Skyfall is a movie by James Bond which features a villain who handles polymorphic encryption techniques. The imitation game movie the story of Alan Turing who is a English mathematician and computer scientist and known for the crypt analysis of the enigma cipher. The movie features Turing's hard work to crack the Enigma code which was a powerful encryption method used by the German during the World War II.

1.5 Python Code for Cryptography

A code has been developed in the python programming language for the encryption of data.We can give the message as input and would recieve the encoded data as output.

```
data = "welcome to python"
la = "abcdefghijklmnopqrstuvwxyz"
ua = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
lra =la[::-1]
ura =ua[::-1]
converted_data = ""
for i in range(0, len(data)):
if data[i] in la:
converted data+=lra[la.index(data[i])]
elif data[i] in ua:
converted_data+=ura[ua.index(data[i])]
else:
converted data+=" "
print(converted data)
```

Chapter 2

MATRICES IN CRYPTOGRAPHY

One of the important applications of inverse of a non-singular square matrix is in cryptography. Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration, but can also be used for user authentication. Encryption and Decryption are the main two factors of Cryptography. Encryption means the process of transformation of an information into an unreadable form. On the other hand, Decryption means the transformation of the coded message back into original form. Encryption and decryption require a secret technique which is known only to the sender and the receiver. This secret is called a key. One way of generating a key is by using a non-singular matrix to encrypt a message by the sender. The receiver decodes (decrypts) the message to retrieve the original message by using the inverse of the matrix. The matrix used for encryption is called encryption matrix (encoding matrix) and that used for decoding is called decryption matrix (decoding matrix).

2.1 Encryption of plain text using matrix.

The plain text which is to be encoded is encrypted by the following steps:

1. The letters of the message is grouped into strings of two or three.

2. Convert each group into a string of numbers by assigning a number to each letter of the divided message. Remember to assign letters to blank spaces.

3. Convert each group of numbers into column matrices.

4. Convert these column matrices into a new set of column matrices by multiplying them with a compatible square matrix of your choice that has an inverse. This new set of numbers or matrices represents the coded message.

2.2 Decryption of cipher text by matrix

The cipher text is decrypted by the following steps:

1. Take the string of coded numbers and multiply it by the inverse of the matrix that was used to encode the message.

2. Associate the numbers with their corresponding letters.

2.3 Illustration

The encryption and decryption process of the given word is illustrated.

ATTACK NOW

It can be solved use 2×2 matrix or 3×3 matrix.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

USING 2×2 MATRIX AS KEY

Use the matrix A = $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ **to encode the message ATTACK NOW**

We divide the letters of message into group of two. The space between words should be indicated.

AT TA CK -N OW

We assign numbers to each letters of the message from above table and blank space is given the number 27.

$$\begin{bmatrix} A \\ T \end{bmatrix} = \begin{bmatrix} 1 \\ 20 \end{bmatrix} \begin{bmatrix} T \\ A \end{bmatrix} = \begin{bmatrix} 20 \\ 1 \end{bmatrix} \begin{bmatrix} C \\ K \end{bmatrix} = \begin{bmatrix} 3 \\ 11 \end{bmatrix} \begin{bmatrix} - \\ N \end{bmatrix} = \begin{bmatrix} 27 \\ 14 \end{bmatrix} \begin{bmatrix} O \\ W \end{bmatrix} = \begin{bmatrix} 15 \\ 23 \end{bmatrix}$$

Now are messages are represented as the 2×1 matrices as follows:

$$\begin{bmatrix} 1 \\ 20 \end{bmatrix} \begin{bmatrix} 20 \\ 1 \end{bmatrix} \begin{bmatrix} 3 \\ 11 \end{bmatrix} \begin{bmatrix} 27 \\ 14 \end{bmatrix} \begin{bmatrix} 15 \\ 23 \end{bmatrix}$$

To encode the message each matrix is multiplied by A

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 1 \\ 20 \end{bmatrix} = \begin{bmatrix} 41 \\ 83 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 20 \\ 1 \end{bmatrix} = \begin{bmatrix} 22 \\ 64 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 3 \\ 11 \end{bmatrix} = \begin{bmatrix} 25 \\ 53 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 27 \\ 14 \end{bmatrix} = \begin{bmatrix} 55 \\ 137 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \begin{bmatrix} 15 \\ 23 \end{bmatrix} = \begin{bmatrix} 61 \\ 137 \end{bmatrix}$$

Hence encoded message is:

$$\begin{bmatrix} 41 \\ 83 \end{bmatrix} \begin{bmatrix} 22 \\ 64 \end{bmatrix} \begin{bmatrix} 25 \\ 53 \end{bmatrix} \begin{bmatrix} 55 \\ 137 \end{bmatrix} \begin{bmatrix} 61 \\ 137 \end{bmatrix}$$

Decoding

To decode message each matrix is multiplied by A^{-1}

$$A^{-1} = \begin{bmatrix} -2 & 1 \\ 3/2 & -1/2 \end{bmatrix}$$

$$\begin{bmatrix} -2 & 1 \\ 3/2 & -1/2 \end{bmatrix} \begin{bmatrix} 41 \\ 83 \end{bmatrix} = \begin{bmatrix} 1 \\ 20 \end{bmatrix}$$

$$\begin{bmatrix} -2 & 1 \\ 3/2 & -1/2 \end{bmatrix} \begin{bmatrix} 22 \\ 64 \end{bmatrix} = \begin{bmatrix} 20 \\ 1 \end{bmatrix}$$

$$\begin{bmatrix} -2 & 1 \\ 3/2 & -1/2 \end{bmatrix} \begin{bmatrix} 25 \\ 53 \end{bmatrix} = \begin{bmatrix} 3 \\ 11 \end{bmatrix}$$

$$\begin{bmatrix} -2 & 1 \\ 3/2 & -1/2 \end{bmatrix} \begin{bmatrix} 55 \\ 137 \end{bmatrix} = \begin{bmatrix} 27 \\ 14 \end{bmatrix}$$

$$\begin{bmatrix} -2 & 1 \\ 3/2 & -1/2 \end{bmatrix} \begin{bmatrix} 61 \\ 137 \end{bmatrix} = \begin{bmatrix} 15 \\ 23 \end{bmatrix}$$

Therefore the matrix corresponding to the plain text is:

$$\begin{bmatrix}1\\20\end{bmatrix}\ \begin{bmatrix}20\\1\end{bmatrix}\ \begin{bmatrix}3\\11\end{bmatrix}\ \begin{bmatrix}27\\14\end{bmatrix}\ \begin{bmatrix}15\\23\end{bmatrix}$$

Now each element in the matrix gives character of message with the help of encoding table.

$$\begin{bmatrix}1\\20\end{bmatrix}=\begin{bmatrix}A\\T\end{bmatrix}\ \begin{bmatrix}20\\1\end{bmatrix}=\begin{bmatrix}T\\A\end{bmatrix}\ \begin{bmatrix}3\\11\end{bmatrix}=\begin{bmatrix}C\\K\end{bmatrix}\ \begin{bmatrix}27\\14\end{bmatrix}=\begin{bmatrix}-\\N\end{bmatrix}\ \begin{bmatrix}15\\23\end{bmatrix}=\begin{bmatrix}O\\W\end{bmatrix}$$

Hence we can decode the message as ATTACK NOW.

USING 3×3 MATRIX AS KEY

Encoding

Use the matrix A = $\begin{bmatrix}1&1&-1\\1&0&1\\2&1&1\end{bmatrix}$ **to encode the message ATTACK NOW**

We divide the letters of message into group of three. The space between words should be indicated.

ATT ACK -NO W- -

We assign numbers to each letters of the message from above table and blank space is given the number 27.

$$\begin{bmatrix}A\\T\\T\end{bmatrix}=\begin{bmatrix}1\\20\\20\end{bmatrix}\ \begin{bmatrix}A\\C\\K\end{bmatrix}=\begin{bmatrix}1\\3\\11\end{bmatrix}\ \begin{bmatrix}-\\N\\O\end{bmatrix}=\begin{bmatrix}27\\14\\15\end{bmatrix}\ \begin{bmatrix}W\\-\\-\end{bmatrix}=\begin{bmatrix}23\\27\\27\end{bmatrix}$$

Now are messages are represented as the 3×1 matrices as follows:

$$\begin{bmatrix} 1 & 2 & -1 \\ -1 & 3 & 2 \\ -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 21 \\ 42 \end{bmatrix} = \begin{bmatrix} 1 \\ 20 \\ 20 \end{bmatrix}$$

To encode the message each matrix is multiplied by A

$$\begin{bmatrix} 1 & 1 & -1 \\ 1 & 0 & 1 \\ 2 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 20 \\ 20 \end{bmatrix} = \begin{bmatrix} 1 \\ 21 \\ 42 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & -1 \\ 1 & 0 & 1 \\ 2 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 3 \\ 11 \end{bmatrix} = \begin{bmatrix} -7 \\ 12 \\ 16 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & -1 \\ 1 & 0 & 1 \\ 2 & 1 & 1 \end{bmatrix} \begin{bmatrix} 27 \\ 14 \\ 15 \end{bmatrix} = \begin{bmatrix} 26 \\ 42 \\ 83 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & -1 \\ 1 & 0 & 1 \\ 2 & 1 & 1 \end{bmatrix} \begin{bmatrix} 23 \\ 27 \\ 27 \end{bmatrix} = \begin{bmatrix} 23 \\ 50 \\ 100 \end{bmatrix}$$

Hence the encoded message is :

$$\begin{bmatrix} 1 \\ 21 \\ 42 \end{bmatrix} \begin{bmatrix} -7 \\ 12 \\ 16 \end{bmatrix} \begin{bmatrix} 26 \\ 42 \\ 83 \end{bmatrix} \begin{bmatrix} 23 \\ 50 \\ 100 \end{bmatrix}$$

Decoding

To decode message each matrix is multiplied by A^{-1}

$$A^{-1} = \begin{bmatrix} 1 & 2 & -1 \\ -1 & 3 & 2 \\ -1 & -1 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 & -1 \\ -1 & 3 & 2 \\ -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 21 \\ 42 \end{bmatrix} = \begin{bmatrix} 1 \\ 20 \\ 20 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 & -1 \\ -1 & 3 & 2 \\ -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} -7 \\ 12 \\ 16 \end{bmatrix} = \begin{bmatrix} 1 \\ 3 \\ 11 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 & -1 \\ -1 & 3 & 2 \\ -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} 26 \\ 42 \\ 83 \end{bmatrix} = \begin{bmatrix} 27 \\ 14 \\ 15 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 & -1 \\ -1 & 3 & 2 \\ -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} 23 \\ 50 \\ 100 \end{bmatrix} = \begin{bmatrix} 23 \\ 27 \\ 27 \end{bmatrix}$$

Therefore the matrix corresponding to the plain text is :

$$\begin{bmatrix} 1 \\ 20 \\ 20 \end{bmatrix} \begin{bmatrix} 1 \\ 3 \\ 11 \end{bmatrix} \begin{bmatrix} 27 \\ 14 \\ 15 \end{bmatrix} \begin{bmatrix} 23 \\ 27 \\ 27 \end{bmatrix}$$

Now each element in the matrix gives character of message with the help of encoding table.

$$\begin{bmatrix} 1 \\ 20 \\ 20 \end{bmatrix} = \begin{bmatrix} A \\ T \\ T \end{bmatrix} \begin{bmatrix} 1 \\ 3 \\ 11 \end{bmatrix} = \begin{bmatrix} A \\ C \\ K \end{bmatrix} \begin{bmatrix} 27 \\ 14 \\ 15 \end{bmatrix} = \begin{bmatrix} - \\ N \\ O \end{bmatrix} \begin{bmatrix} 23 \\ 27 \\ 27 \end{bmatrix} = \begin{bmatrix} W \\ - \\ - \end{bmatrix}$$

Hence we can decode the message as ATTACK NOW.

Chapter 3

GRAPH THEORY IN CRYPTOGRAPHY

Graph theory is the study of graphs, which are mathematical structures used to model pairwise relation between object.An undirected graph G (V, E), where V is the set of vertices and E is the set of edges is considered. A walk in which vertices are not repeated is called path. In a graph, a cycle is a non-empty trail in which only first and last vertices are equal. A graph is called a complete graph when there is an edge between any two vertices of the graph.

A graph can be mainly represented in two ways, adjacency list and adjacency matrices. The representation of graph consisting of array of V list, one for each vertex is called adjacency list. The adjacency list for vertex V contains all the adjacent vertices to it. The adjacency matrix representation consists of matrix V = [g_{ij}] where
for un-weighted graph,

$$g_{ij} = \begin{cases} 1, & (if (i,j) \in E \\ 0, & \textbf{otherwise} \end{cases}$$

and for weighted graph,

$$g_{ij} = \begin{cases} w_{ij}, & (if (i,j) \in E \\ NIL, & \textbf{otherwise} \end{cases}$$

A connected sub-graph which consist all vertices with minimum weight of edges required is called a spanning tree. A minimum spanning tree is a special kind of tree that minimizes the length (or weights) of the edges of the tree.

3.1 Proposed Algorithm

In this algorithm, as first step we represent each character of the message to be encrypted as the vertices of the graph. We keep adding vertices until we form a cyclic graph. By using a keyword, whose length is longer than the message, we encoded the message in such a way that each letter of the message would be converted to the number of letters between it and the corresponding letters of the keyword using the encoding table. Then the weight of each edge is calculated as the distance between the encoded character of the adjacent edges as in the message. If we get the weight as zero we represent it as 27 (which is the last index in the encoding table). Then each vertex in the graph is joined by edges to make the graph a complete graph. For every newly added edge, it has a sequence weight, starting from last index (28, 29, 30. . .) . Add special character A to the starting character. A is encoded as the difference between the corresponding indexes of the remnant character in the keyword and the special character. Adjacency-matrix is constructed from this complete graph. After that Minimum Spanning Tree (MST) is constructed and represented as adjacency-matrix. Then replace the zero diagonal entries by 0,1,2,. . . . Adjacency-matrix of the complete graph is multiplied to the adjacency-matrix of MST. The resultant matrix is multiplied to the key matrix which gives the final matrix which is to be sent to the recipient.

3.1.1 Encryption Algorithm

- **Add vertex for each character in the plain text to the graph.**
- **Vertices of each sequential character are joined by edges until we**

form a cyclic graph.

- **Weight of each edge is calculated as mentioned above.**
- **Add more edges to form a complete graph M_1.**
- **Add special character A to the starting character. A is encoded as the difference between the corresponding indexes of the remnant character in the keyword and the special character A.**
- **Construct adjacency-matrix of M_1.**
- **Then find the Minimum Spanning Tree and its adjacency-matrix M_2.**
- **Then we replace the zero diagonal entries in M_2 matrix by 0,1,2. . . ...**
- **Then we multiply matrices M_1 by M_2 to get M_3.**
- **After that the multiply M_3 by a predefined shared key K to form C,the cipher text.**

3.1.2 Decryption Algorithm

- **The receiver computes M_3 by using the inverse form of shared key K^-1**
- **Then compute M_2 by using the inverse form of M_1.**
- **Then we represent M_2 as a graph.**
- **Then compute the original text from the minimum spanning tree using the keyword.**

Figure given below summarizes the encryption and decryption algorithms.

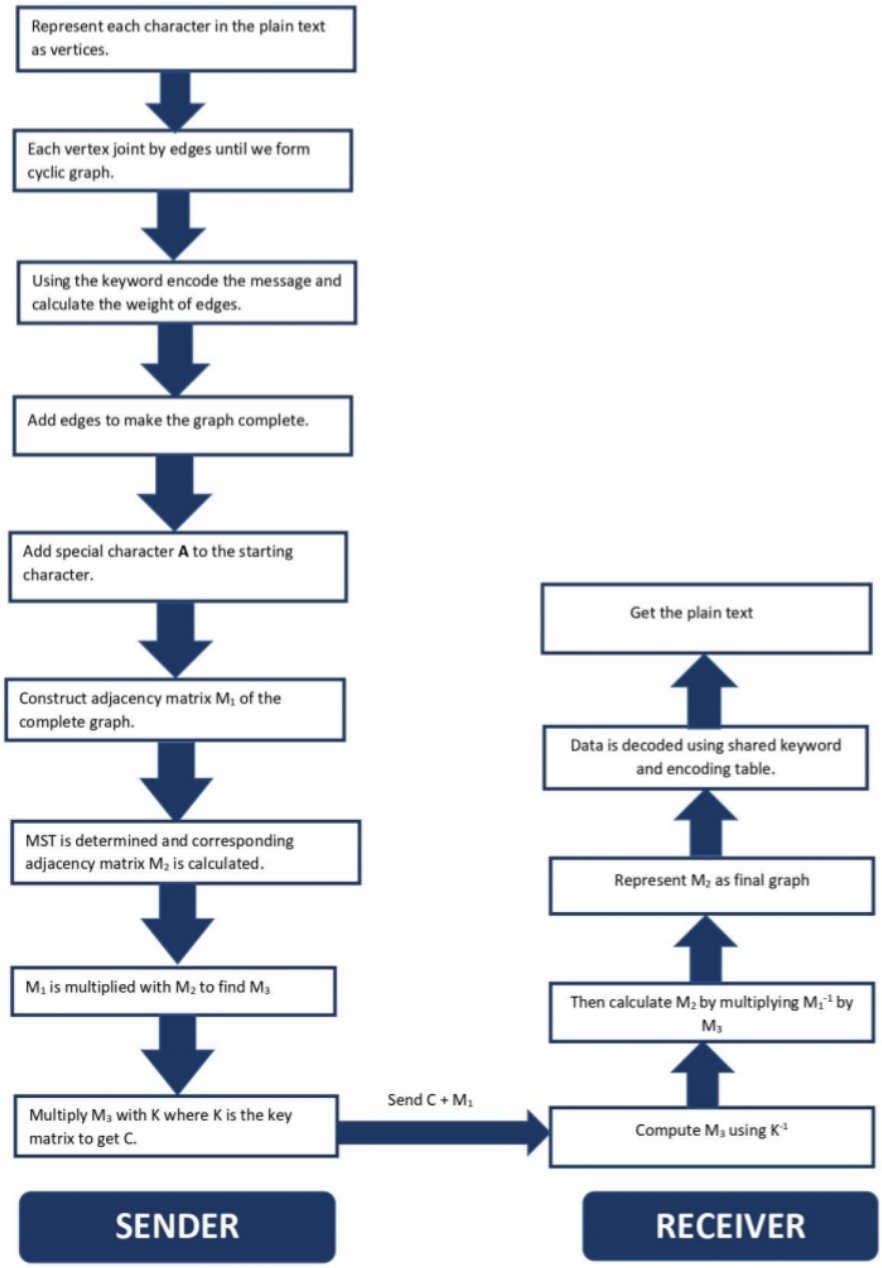

Fig.1 Algorithm Summary

ILLUSTRATION:

Let COLD be the message which has to be send to the receiver. As first step we represent each character of the message to a vertex as shown in Fig. 2.

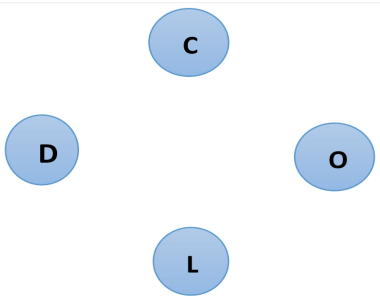

Fig.2 Represent each character as vertex

Then, connect pair of sequential characters by an edge to form a cyclic graph.

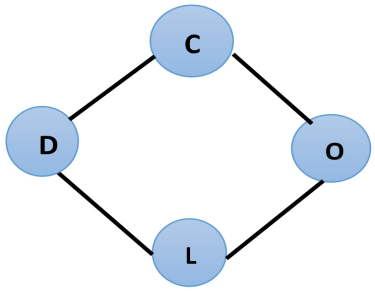

Fig. 3. Graphical representation of plain text to be encrypted

Then using a keyword and encoding table (Table 1) the given message is encoded as shown below.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Table. 1 Encoding table

Let the keyword be SECRET

Then each character in the message to be encrypted is converted to a number, which is the difference between the numbers representing the corresponding letters of the message to be encrypted and the keyword, from Table 1.

Message: C O L D

Encoded message: 16 -10 -9 14

Then weight of each edge is calculated as the difference between the

letters representing the end vertices of that edge. So, the edge connecting vertex C with vertex O has the weight as the distance between the two letters as follows:

Distance = code (O) – code (C)

= -10 -16

= -26

Proceeding as above, we get the graph as in Fig. 4.

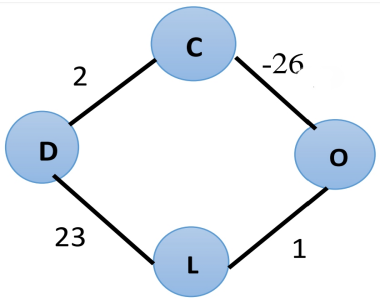

Fig. 4. Graphical representation of the message COLD

As next step, we add edges to fig 4 till we get a complete graph. Every newly added edge has a weight choosing from the sequence 28, 29, 30. . . .

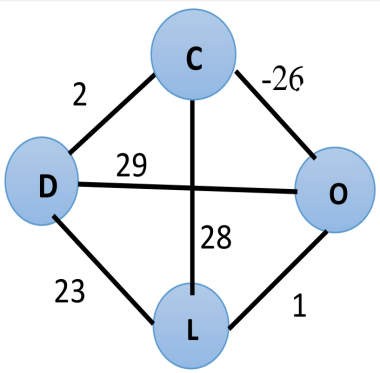

Fig. 5. Complete plain graph

Here we add a special character A before the character C to indicate that C is the first character of the message as shown in Fig .6.

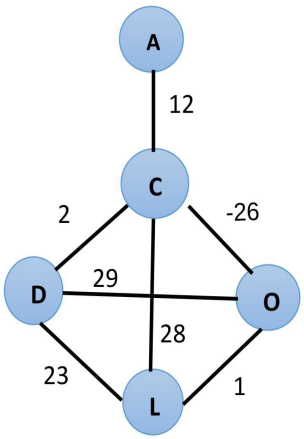

Fig. 6. Complete plain graph with a special character

The complete plain graph in Fig. 6. is represented as a matrix M_1.

$$M_1 = \begin{bmatrix} 0 & 12 & 0 & 0 & 0 \\ 12 & 0 & -26 & 28 & 2 \\ 0 & -26 & 0 & 1 & 29 \\ 0 & 28 & 1 & 0 & 23 \\ 0 & 2 & 29 & 23 & 0 \end{bmatrix}$$

Then we find the minimum spanning tree (MST) as shown in Fig. 7.

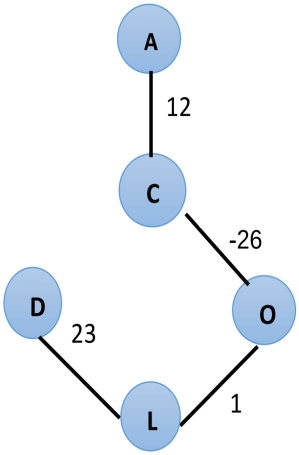

Fig. 7. Minimum Spanning Tree Graph

Adjacency-matrix M_2 of MST is determined, $M_2 = \begin{bmatrix} 0 & 12 & 0 & 0 & 0 \\ 12 & 0 & -26 & 0 & 0 \\ 0 & -26 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 23 \\ 0 & 0 & 0 & 23 & 0 \end{bmatrix}$

Then we change the diagonal entries of M_2 by 0, 1, 2, 3, 4.

So, M_2 modified to $M_2 = \begin{bmatrix} 0 & 12 & 0 & 0 & 0 \\ 12 & 1 & -26 & 0 & 0 \\ 0 & -26 & 2 & 1 & 0 \\ 0 & 0 & 1 & 3 & 23 \\ 0 & 0 & 0 & 23 & 4 \end{bmatrix}$

After that, we multiply matrix M_1 by M_2 to form M_3.

$$M_1M_2 = M_3 = \begin{bmatrix} 144 & 12 & -312 & 0 & 0 \\ 0 & 820 & -24 & 104 & 652 \\ -312 & -26 & 677 & 670 & 139 \\ 336 & 2 & -726 & 530 & 92 \\ 24 & -752 & 29 & 98 & 529 \end{bmatrix}$$

Now, we use the shared-key K to encrypt M_3.

Let K= $\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$

So, the cipher text C = KM_3 = $\begin{bmatrix} 192 & 56 & -356 & 1402 & 1412 \\ 48 & 44 & 44 & 1402 & 1412 \\ 48 & -776 & -20 & 1298 & 760 \\ 360 & -750 & -697 & 628 & 621 \\ 24 & -752 & 29 & 98 & 529 \end{bmatrix}$

Now the data to be sent is C and M_1.

In the receiver side, we get M_3 by multiplying the cipher text with the inverse of the shared key K^{-1}.

$$M_3 = K^{-1}\mathbf{C} = \begin{bmatrix} 144 & 12 & -312 & 0 & 0 \\ 0 & 820 & -24 & 104 & 652 \\ -312 & 2 & -726 & 530 & 92 \\ 336 & 2 & -726 & 530 & 92 \\ 24 & -752 & 29 & 98 & 529 \end{bmatrix}$$

Then M_2 is calculated by multiplying M_3 by M_1^{-1}.

$$M_2 = M_3\ M_1^{-1} = \begin{bmatrix} 0 & 12 & 0 & 0 & 0 \\ 12 & 1 & -26 & 0 & 0 \\ 0 & -26 & 2 & 1 & 0 \\ 0 & 0 & 1 & 3 & 23 \\ 0 & 0 & 0 & 23 & 4 \end{bmatrix}$$

Then, M2 represented as the following final graph (Fig. 8) (discard the diagonal):

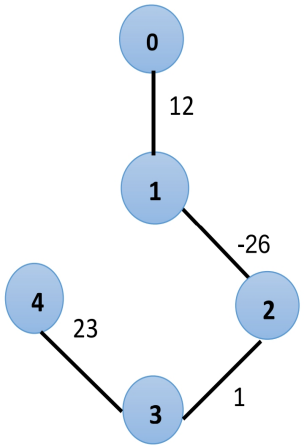

Fig. 8. Final Graph

We use this graph to retrieve the original message as follows :
Let the node 0 be A, so by using the keyword and encoding table,
node 1 = code (A) + 12
code (A)= E - A = 5 − 1 = 4 (using the keyword)

therefore, node 1 = code A + 12 = 4 + 12 = 16

S – 16 =19 – 16 = 3, where 3 represents C (from the encoding table)

And node 2 = code (C) - 26

Code (C) = S - C =19 - 3 = 16

therefore, node 2 = code (C) - 26 =16 -26 = - 10

E - (-10) = 5- -10 = 15, where 15 represents O,

Similarly proceeding , we get the original text COLD.

Chapter 4

CRYPTOGRAPHY IN DAILY LIFE

Cryptography has been used in our daily life. Cryptography plays an important role in each time when we make an online purchase, making an online transaction, sending an email withdrawing money from ATM and so on.Cryptography secures all the information that we transmit through the internet. Cryptographic techniques like digital signature protects our information from forgeries and fraudulent. It ensures authentication of identity,prevent document tampering and establishes the trust between servers. Most of the communication platform have been encrypted. Social media like WhatsApp, Instagram, Telegram has made use of the idea of encryption for transmitting the messages and keeping it secure. Cryptography also helps in encrypting company devices, protecting sensitive data, encrypting databases and securing a website. Https or Secure HyperText Transfer Protocol is used for securing website.

4.1 Cryptography and ATM

Authorized cardholders can withdraw cash and carry out other financial operations at an ATM without having to go to a bank branch because to the convenient and secure service it offers. A secure communications network, also known as encryption, is used by banks to authorise each ATM transaction. This network encrypts data so that only the sender

and the intended recipient can decipher it.

4.1.1 Deficiency in Securities

One typical ATM security flaw includes so-called phantom withdrawals, in which money is withdrawn from a cardholder's account but neither the client nor the bank acknowledges responsibility. Phantom withdrawals can occasionally be the consequence of dishonest behaviour on the part of the consumer, but ATMs can also be made to accept phoney, skimmed, or copied cards. Card issuers utilise an Authorization Request Cryptogram, a coded message generated by ATMs, to authenticate the card and card data.

4.1.2 Data Encryption Standard(DES)

ATMs were the first to encrypt personal identifying numbers using a mathematical formula or algorithm. The 56-bit encryption key used by DES to encrypt data in 64-bit blocks was once an established Federal Information Processing Standard in the United States. However, as personal computer processing power has increased, DES has become less secure for ATM applications; ATMs utilising DES have been compromised in less than a day.

Triple DES

With Triple DES, the encryption key is essentially extended to 168 bits by using two keys and three applications of the DES encryption method. Because it is not practical to search the individual bits of the encryption key to crack the code, Triple DES is much more secure than DES. Since 2002, triple DES encryption has been required, according to the National Credit Union Administration, for all new ATM installations.

4.1.3 Advanced Encryption Standard(AES)

The Advanced Encryption Standard, which was meant to replace DES, was adopted in 2001, according to an announcement made by the National Institute of Standards and Technology. Data is encrypted by AES using 128-bit blocks and a variable-length encryption key with a

length of 128, 192, or 256 bits. AES is substantially more secure than DES or triples DES since the only way for an unauthorised individual to decrypt data encrypted with it is by a method known as a "brute force attack," which tests all possible combinations of the encryption key. The commercial standard for encrypting sensitive digital information, such as the financial data utilised by ATMs, was certified by the US government as the AES standard in 2003.

4.2 Cryptography and Email

Email encryption is a method of authentication that stops messages from being read by an unauthorized or unintended person. The original communication is scrambled and put into an unintelligible or unreadable format. When sending sensitive material over email, encryption is required.

In order to commit crimes like identity theft and fraud, hackers target victims via email and steal data, including personal information like names, addresses, and login credentials. Additionally, while the majority of sent emails are encrypted during transmission, the data is retained in clear text, allowing email providers to access the content. End-to-end encryption is often not offered by well-known free email services, making it simple for hackers to intercept delivered messages.

Public-key cryptography and digital signature technologies are used by email encryption solutions to encrypt email messages. By following this procedure, you may be sure that only the intended recipient will be able to open your emails.

You can encrypt emails when transmitting important information in them. When text is encrypted for email, it is transformed from plain text to scrambled cipher text. Only the receiver has access to the private key and this key will be used to decode the email which enable to view it.

4.2.1 Transport Layer Security (TLS)

A cryptographic protocol called TLS replaced the secure sockets layer (SSL). TLS, another IETF standard, was developed from the original SSL specifications and debuted in 1999. It makes it possible for messages to travel safely through computer networks and is frequently used for email as well as other forms of communication like Voice over Internet Protocol and instant messaging (VoIP).
TLS strives to protect the privacy and data integrity of connections between computer applications. The TLS record and TLS handshake protocols are part of it, which operates at the application layer.
The command STARTTLS, which converts plaintext messages to secure, encrypted communications, is a common variant of TLS. Since STARTTLS requests encryption while emails are in transit. Although this strategy is excellent for thwarting attack vectors like passive monitoring, it may expose businesses to additional dangers like man-in-the-middle (MITM) attacks. S/MIME, short for Secure Multipurpose Internet Mail Extension.
Public-key encryption and digital signatures are delivered using the S/MIME standard, which was developed by the Internet Engineering Task Force (IETF). The majority of contemporary email software systems now include it, which was created by RSA Data Security. S/MIME offers PGP-like capabilities, but it necessitates that users receive keys directly from a particular Certificate Authority (CA).

4.2.2 Pretty Good Privacy (PGP)

Using digital signatures and file encryption methods, the security tool PGP encrypts and decrypts email messages. One of the first publicly accessible, free public-key cryptography programmes, the software was first made available in 1991. PGP is currently widely used to safeguard people and organisations, offering cryptographic authentication and privacy to secure internet communication including email and text messaging.

PGP encrypts data in motion by utilising a variety of hashing algo-

rithms, data compression, symmetric and asymmetric key technology, and cryptography. It provides a viewpoint on the public key infrastructure (PKI) strategy as well. When a user sends a message using their public key, PGP encrypts the data and decrypts it when the recipient unlocks it using their private key. In addition to using S/MIME and TLS to encrypt email, you can also take advantage of encrypted PDFs and web portal encryption.

4.2.3 Encrypted PDF

You can offer consumers protected documents and attachments that they can download to their computers using an encrypted PDF, zip, or Office file. Anyone attempting to intercept and use the information in the email would only receive a random collection of characters as a result. This indicates that all attachments and documents are readable on all devices and arrive to their destinations unharmed. The user can access the attachment later even while they are offline because they downloaded it.

4.2.4 Web Portal Encryption

To read an email that has been encrypted via a web gateway, the recipient must visit a web page. Because the email is protected by a shared key before it is sent to the web portal, this satisfies the definition of email encryption. The user's email programme, such as Outlook, Mailbird, etc., sends the encrypted email directly to the web site. This prevents anyone without the website's login information from reading the email.

By reducing the amount of persons who have access to your company's emails, this type of secure email encryption solution reduces your attack surface. Web portal encryption is a reliable means to stop hackers from accessing critical information sent over the internet, provided that the recipient's password is safe.

4.3 Cryptography and Digital Signature

Just like signature on paper , digital signature has become an important tool in business with the development of technology . Digital signature also has the legal power as hand written signature.
Digital signature is a cryptographic value calculated from the data and a secret key known only by the signer. The message belongs to the sender should be assured to the receiver. this is crucial in business as the chance of dispute over the data exchanges are high.

4.3.1 Importance of Digital Signature

Digital signature is very important tool in cryptography.
Message authentication - The private key is send to the sender. The public key can used by the verifier of the sender to validate that the Digital signature was created by the sender.
Data Integrity - If the data is attacked , there will be a discrepancy in the hash value and won't match with the verification ,Algorithm. Due to this, reject the message by the receiver and declaring a data breach.
Non-repudiation - The signature key is only known to the signer so , naturally they are the only one who can create a specific signature. On any occasion there is a dispute , the data along with the Digital signature can be presented as evidence .

4.4 Other Applications

HTTPS

HyperText Transfer Protocol Secure or https helps to set the information free on a web. It is an everyday application of cryptography. It is a primary protocol which is used to send data between a browser and a website. It is important to be encrypted as uses transmit sensitive data such as details of bank account, email service and so on. A website which require login credential should use https. A browser which does not use https are flagged as non secure.

CRYPTOCURRENCY

Cryptocurrency uses three different cryptographic methods for encryption. Symmetric Encryption asymmetric Encryption and hashing has been used in Crypto currencies. The Bitcoin network uses has function to ensure the security of blockchain and immutability of the transmission. Cryptocurrencies use cryptography which make the transactions anonymous secure and trustless. The identity of the person is not needed for the transaction. Details of bank, credit card company are not collected for the transaction.

TIME STAMPING

Time Stamping is the technique which certify the time when an electronic document or communication was existed or delivered. Encryption model blind signature scheme. The scheme of blind signature helps the sender to receive a message receipted by another person without revealing the information about the message to others. The possible applications of time stamping include patent application, copyright archives and contracts.

ENCRYPTION IN WHATSAPP

Signal protocol is used in WhatsApp for encryption. So it uses a combination of asymmetric key cryptography and symmetric key cryptography algorithms. Confidentiality and integrity is ensured by using symmetric key algorithm whereas authentication and non repudiation goals are achieved by the usage of asymmetric key algorithm.

[1] Al Etaiwi, Wael Mahmoud. "Encryption algorithm using graph theory." Journal of Scientific Research and Reports 3.19 (2014): 2519-2527.

[2] Paszkiewicz A, et al. "Proposals of graph based ciphers, theory and implementations". Proceedings of the Regional Conference on Military Communication and Information Systems. CIS Solutions for an Enlarged NATO, RCMIS, (2001)

[3] Ronald L. Rivest, Belmont; Adi Shamir, Cambridge; Leonard M. Ademan, Arlington, all of Mass "CRYPTOGRAPHIC COMMUNICATIONS SYSTEM AND METHOD" 75 Inventors: Massachusetts Institute of Technology, Cambridge, Mass.(1983)

[4] Steve Lu, Rafail Ostrovsky. Daniel Manchala. "Visual Cryptography on Graphs", Cite Seerx, COCOON. (2008);225-234

[5] Ustimenko VA." On graph-based cryptography and symbolic computations," Serdica. Journal of Computing. (2007);131-156.

[6] Whitefield Diffie; Martin E Hellman "Multiuser cryptographic techniques" Association for Computing Machinery New York,United States (1976)

[7] Yamuna M, Meenal Gogia, Ashish Sikka, Md. Jazib Hayat Khan. "Encryption using graph theory and linear algebra". International Journal of Computer Application.ISSN: (2012)2250-1797