A STUDY OF MATRICES AND NUMBER THEORY IN CRYPTOGRAPHY

PROJECT REPORT

Submitted To

Sri G.V.G Visalakshi College for Women (Autonomous),Udumalpet

Affiliated to Bharathiar University

in Partial fulfillment of the requirements for the award of Degree of

BACHELOR OF SCIENCE IN MATHEMATICS

Submitted by

Ms.P.Abinaya	18BM7443
Ms.R.Gowri	18BM7449
Ms.T.Janani priya	18BM7452
Ms.S.Nivethini	18BM7461
Ms.S.Preethi	18BM7466
Ms.I.Safrin fathima	18BM7468

Under the guidance of

Mrs. M. Kalarani M.Sc., M.Phil.,

Department of Mathematics

Sri G.V.G Visalakshi college for Women (Autonomous)

Udumalpet - 642 128

DECLARATION

DECLARATION

We **P. Abinaya, R. Gowri, T. Janani priya**, **S.Nivethini, S. Preethi, I. Safrin fathima** hereby declare that the project entitled **"A STUDY OF MATRICES AND NUMBER THEORY IN CRYPTOGRAPHY"** submitted to **Sri G.V.G Visalakshi College for Women (Autonomous),Udumalpet,** Affliated to Bharathiar University, In Partial fulfillment of the requirements for the award of Degree of **"BACHELOR OF SCIENCE IN MATHEMATICS"** is a record of original project work done by us during the period August 2020 – December 2020 of our study under the supervision and guidance of **Mrs. M. Kalarani M.Sc., M.Phil.,** and the project has not formed on the basis for the award of any degree/diploma/associate ship/fellowship or other similar title to any other candidate of any university.

Name	**Register number**	**Signature of the Candidate**
Ms .P. Abinaya	18BM7443	_____
Ms .R .Gowri	18BM7449	_____
Ms .T. Janani priya	18BM7452	_____
Ms .S. Nivethini	18BM7461	_____
Ms .S. Preethi	18BM7466	_____
Ms .I .Safrin fathima	18BM7468	_____

Date:

Place: Udumalpet

CERTIFICATE

CERTIFICATE

This is to certify that the project reported entitled **"A STUDY OF MATRICES AND NUMBER THEORY IN CRYPTOGRAPHY"** Submitted to **Sri G.V.G. Visalakshi College for Women(Autonomous), Udumalpet,** Affliated to Bharathiar University, in partial fulfillment of the requirements for the award Degree of **BACHELOR OF SCIENCE IN MATHEMATICS"** is a record of original project work done by P.Abinaya, R. Gowri, T. Janani priya, S. Nivethini, S.Preethi, I. Safrin Fathima during the period August 2020 - December 2020 of their study in the Department of Mathematics, Sri G.V.G. Visalakshi College for Women (Autonomous), Udumalpet under my supervision and guidance and the project has not formed on the basis for award of any degree/diploma/associate ship/ fellowship or other similar title to any other candidate of any University.

Head of the Department **Signature of the guide**

Counter Signed

Submitted for viva-voce examination held on _____ at Sri G.V.G. Visalakshi College For Women,Udumalpet.

Examiners

Internal **External**

CONTENTS

CONTENTS

ABSTRACT

ABSTRACT

Cryptography builds from the field of pure maths known as number theory which deals with integers and matrix theory that is the arrangement of elements in rows and columns. In this project, how matrix theory used to encrypt and decrypt the information in cryptography is studied with examples. Also the application of number theory in the cryptography using the concept of congruence was discussed with examples.

ACKNOWLEDGEMENT

ACKNOWLEDGEMENT

We express our deep sense of gratitude and indebteness to our guide **Mrs.M. Kalarani M.Sc., M.Phil.,** Assistant professor,Department of Mathematics. **Sri G.V.G Visalakshi college for women(Autonomous),** for her valuable suggestions , guidance and constant encouragement right from the beginning till the completion of this project work.

We utilize this opportunity to express our loyal gratitude and sincere thanks to **Mrs.S.KALAISELVI M.Sc.,B.Ed., M.Phil.,PGDCA.,** Principal I/C, **Sri G.V.G Visalakshi collage for women (Autonomous),** for her immeasurable help by providing all sorts of facilities needs to complete this work successfully.

We would like to express our profound and sincere thanks to our Head of the Department **Mrs.B. Pushpa M.Sc., M.Phil.,** Associate Professor Department of Mathematics,**Sri G.V.G visalakshi college for women(Autonomous),** for her untiring efforts and constant encouragement wise council and valuable suggestion in the formation and completion of this project.

We are also thankful to all members of the Department of mathematics,**Sri G.V.G visalakshi college for women(Autonomous),** for extending warm helpful hand and valuable suggestions through this project.

We are also pleased to express our sincere thanks to the Librarian **Mrs.P. Kavitha B.B.A., B.L.I.Sc.,M.L.I.Sc.,M.Phil.,PGDLAN.,** for her timely support and guidance for the reference work to carry out this project.

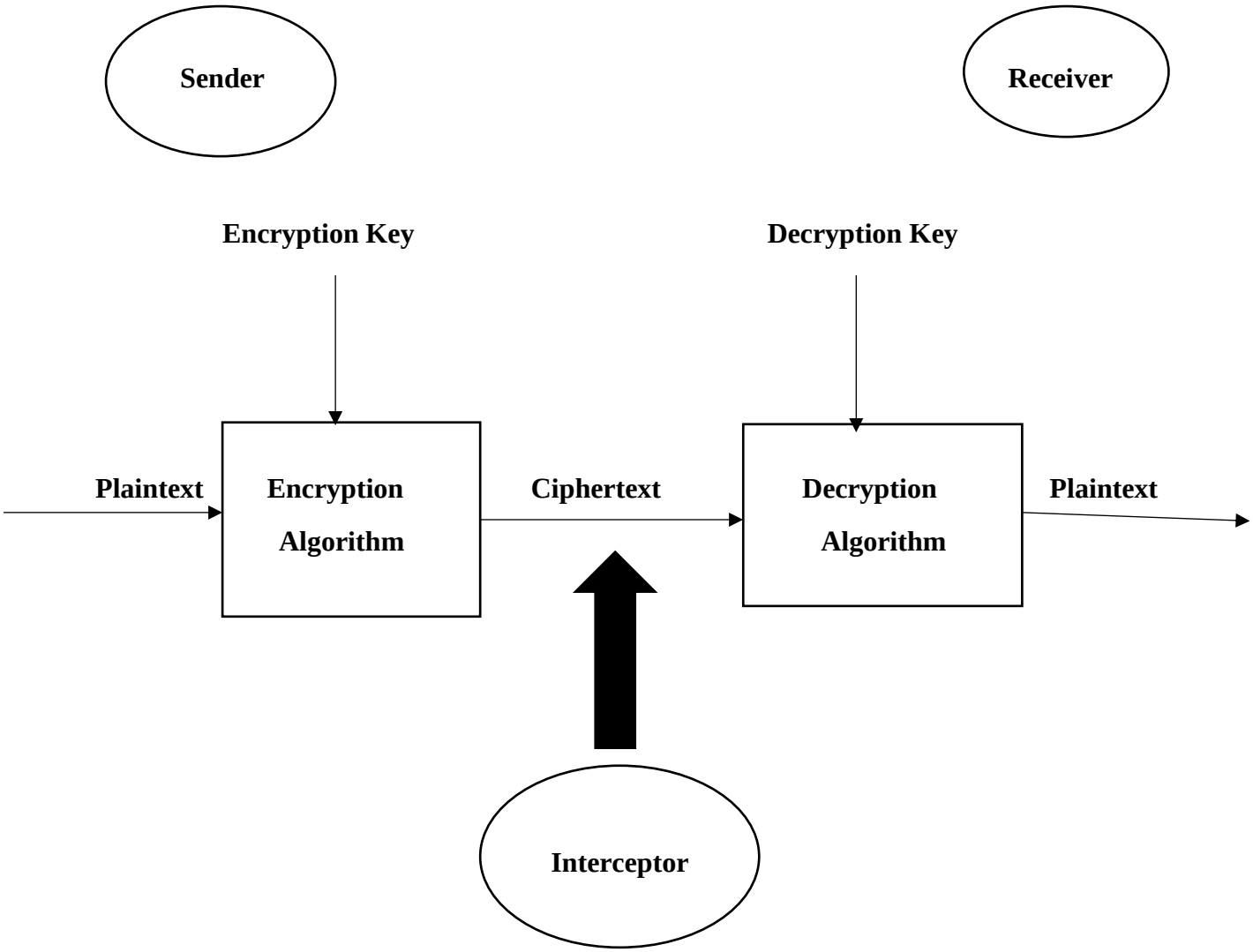
CHAPTER I

CHAPTER I

INTRODUCTION

Cryptography is the science of protecting information by transforming it into a secure format. An example of basic cryptography is a encrypted message in which letters are replaced with other characters. To decode the encrypted contents, one needs a grid or table that defines how the letters are transposed. The goal of modern cryptography is to ensure the preservation of information properties through mathematically sound means. Confidentiality is the assurance that only the intended recipient of a message can read it. Cryptography is a field of maths, specifically Numbers theory. A good example of a cryptography method is public key cryptography which uses two set of keys. One key is public while the other is private which is distributed only to the intended recipient of the information.

Cryptography, or cryptology, is the practice and study of hiding information. When a message is sent using cryptography, it is changed (or encrypted) before it is sent. The method of changing text is called a "code" or, more precisely, a "cipher". The changed text is called "cipher text".


Sender
Receiver
Encryption Key
Decryption Key
Plaintext
Encryption Algorithm
Ciphertext
Decryption Algorithm
Plaintext
Interceptor

CHAPTER II

CHAPTER II

PRELIMINARIES OF CRYPTOGRAPHY

In this chapter provides the basic terms related to Cryptography.

Definition. 2.1

An **encoder** is an electronic device used to convert an analogue signal to a digital signal.

Definition. 2.2

The **decoder** an electronic device that is used to convert digital signal to an analogue signal.

Definition. 2.3

Cipher text is encrypted text. Plaintext is what you have before encryption, and cipher text is the encrypted result. The term cipher is sometimes used as a synonym for cipher text, but it more properly means the method of encryption rather than the result.

Definition. 2.4

Cryptography is the study of methods to send and receive secret message.In private key cryptography, the sender and receiver agree in advance on a secret code, and then send message using the code.In public key cryptography, the encoding method can be published. Each person has a public key used to encrypt message.The original message is called the plain text.The encoded text is called Cipher text.

CHAPTER III

CHAPTER III
MATRICES THEORY IN CRYPTOGRAPHY

This chapter deals with how matrices are used in encoding and decoding process of cryptography.

Definition. 3.1

A matrix is a rectangular array of m×n elements, in which m is the number of rows and n is the number of columns A matrix is normally denoted with a boldface uppercase letter such as A. The element a_{ij} is located in the ith row and jth column . Although the elements can be a set of numbers. We discuss only the matrices with elements in Z.

Matrix A: n columns

$$\text{m rows}\begin{bmatrix} a_{11} & a_{12} & \wedge & a_{1m} \\ a_{21} & a_{22} & \wedge & a_{2m} \\ .. & .. & .. & ... \\ a_{l1} & a_{l2} & \wedge & a_{lm} \end{bmatrix}$$

Definition. 3.2

We can multiply two matrices of different sizes if the number of columns of the first matrix is the same as the number of rows of the second matrix. If A is an l × m matrix and B is an m × p matrix, the product of the two is a matrix C of size 1 × p. If each element of matrix A is called $a_{ij,}$ each element of matrix B is called b_{jk}, then each element of matrix C, C_{ik} can be calculated as

$C_{jk}= \sum a_{ij} \times b_{jk} = a_{il} \times b_{lj} + a_{i2} \times b_{2j} + \ldots.. + a_{im} \times b_{mj}$

Definition. 3.3

Let A denote an n × n symmetric matrix with real entries and let x denote an n × 1 column vector. Then Q = x' Ax is said to be **quadratic form.**

Definition. 3.4

If A is an n × n matrix and I be an n × n identity matrix, then the n × n matrix B (also called as B = A^{-1}) said to be **inverse matrix** such that AB = BA =I.

Definition. 3.5

An n × n matrix A is called **nonsingular or invertible** if and only if there exists an n × n matrix B such that AB = BA = I_n. Where $I_n$is the identity matrix. The matrix B is called the inverse matrix of A.

Definition. 3.6

A Square matrix, all of whose elements, except those in the leading diagonal are zero is called **Diagonal Matrix**

Definition. 3.7

If the transpose of a matrix is equal a to itself, that matrix is said to be **symmetric.** For example: ie, $A=A^T$

Definition.3.8

A **Cofactor** is the number when the column and row of a designated element in a matrix is removed, which is just a numerical grid in the form of a rectangular or a square.

Definition.3.9

The **Adjoint** of a square matrix A= $[a_{ij}]$ n x n is defined as the transpose of the matrix $[A_{ij}]$ n x n, where a_{ij} is the cofactor of the element a_{ij}. Adjoining of the matrix A is denoted by **adj A.**

Theorem. 3.1

A text message of strings of some length / size L can be converted in to a matrix (called a message matrix M)of size m× n where n ‹ m and n is the least such that m × n ≥ l depending up on the length of the message with the help of suitably chosen numerals and zeros.

Proof:

The proof is by enumeration on numbers.

Consider the following, For the text message of length up to l=9; then we have m=3; n=3. Similarly, for the text message of length up to1=12 we have m=4; n=3…..,. Hence the proof

EXAMPLE 3.3.1:

Encoding process:

Consider the message to be sent

PACK MY BAG

STEP 1: Assign the number to the alphabets

Alphabet	A	B	C	D	E	F	G	H	I
Number	1	-1	2	-2	3	-3	4	-4	5

J	K	L	M	N	O	P	Q	R	S
-5	6	-6	7	-7	8	-8	9	-9	10

T	U	V	W	X	Y	Z	Space
-10	11	-11	12	-12	13	-13	0

Also, assign the number 0 to a blank or space between two words.

STEP 2: Convert the text message into numerals.

P A C K M Y B A G

-8 1 2 6 0 7 13 0 -1 1 4

STEP 3: Rearrange these numbers in to a matrix M(Row wise and column wise)

$$M=\begin{pmatrix} -8 & 1 & 2 \\ 6 & 0 & 7 \\ 13 & 0 & -1 \\ 1 & 4 & 0 \end{pmatrix}$$ of order 4 by 3

STEP 4: Multiply this message matrix by the encoder A

$$A=\begin{pmatrix}-1 & -10 & -8\\ -1 & -6 & -5\\ 0 & -1 & -1\end{pmatrix}$$

$$X=MA=\begin{pmatrix}-8 & 1 & 2\\ 6 & 0 & 7\\ 13 & 0 & -1\\ 1 & 4 & 0\end{pmatrix}\begin{pmatrix}-1 & -10 & -8\\ -1 & -6 & -5\\ 0 & -1 & -1\end{pmatrix}$$

$$X=\begin{bmatrix}7 & 72 & 57\\ -6 & -67 & -55\\ -13 & -129 & -103\\ -5 & -34 & -28\end{bmatrix}$$

STEP 5: The encoded numeric messages to be sent

7 72 57 -6 67 -55 -13 -129 -103 -5 -34 -28

Decoding process:

STEP 1: Find the inverse matrix A

$$A=\begin{pmatrix}-1 & -10 & -8\\ -1 & -6 & -5\\ 0 & -1 & -1\end{pmatrix}$$

$$A^{-1}=\frac{1}{|A|}adjA$$

$$|A|=\begin{vmatrix}-1 & -10 & -8\\ -1 & -6 & -5\\ 0 & -1 & -1\end{vmatrix} \quad = -1(6-5) + 10(1+0) -8(1+0)$$

$$= -1(1)+10-8$$

$$= 1$$

$$\text{adjA}=\begin{pmatrix} +\begin{vmatrix}-6 & -5\\ -1 & -1\end{vmatrix} & -\begin{vmatrix}-1 & -5\\ 0 & -1\end{vmatrix} & +\begin{vmatrix}-1 & -6\\ 0 & -1\end{vmatrix} \\ -\begin{vmatrix}-10 & -8\\ -1 & -1\end{vmatrix} & +\begin{vmatrix}-1 & -8\\ 0 & -1\end{vmatrix} & -\begin{vmatrix}-1 & -10\\ 0 & -1\end{vmatrix} \\ +\begin{vmatrix}-10 & -8\\ -6 & -5\end{vmatrix} & -\begin{vmatrix}-1 & -8\\ -1 & -5\end{vmatrix} & +\begin{vmatrix}-1 & -10\\ -1 & -6\end{vmatrix} \end{pmatrix}^{t} = \begin{pmatrix} 1 & -1 & 1 \\ -2 & 1 & -1 \\ 2 & 3 & -4 \end{pmatrix}^{t}$$

$$\text{adjA} = \begin{pmatrix} 1 & -2 & 2 \\ -2 & 1 & -1 \\ 2 & 3 & -4 \end{pmatrix}$$

$$A^{-1} = \frac{1}{|A|}(\text{adjA}) = \frac{1}{1}\begin{pmatrix} 1 & -2 & 2 \\ -1 & 1 & 3 \\ 1 & -1 & -4 \end{pmatrix}$$

$$A^{-1} = \begin{pmatrix} 1 & -2 & 2 \\ -1 & 1 & 3 \\ 1 & -1 & -4 \end{pmatrix}$$

STEP 2: Multiply this encoded matrix by the decoder A^{-1}

$$M = XA^{-1} = \begin{bmatrix} 7 & 72 & 57 \\ -6 & -67 & -55 \\ -13 & -129 & -103 \\ -5 & -34 & -28 \end{bmatrix}\begin{pmatrix} 1 & -2 & 2 \\ -1 & 1 & 3 \\ 1 & -1 & -4 \end{pmatrix}$$

$$M = \begin{pmatrix} -8 & 1 & 2 \\ 6 & 0 & 7 \\ 13 & 0 & -1 \\ 1 & 4 & 0 \end{pmatrix}$$

STEP 3: This stream of numerals converted to the text of the original message.

-8 1 2 6 0 7 13 0 -1 1 4

P A C K M Y B A G

3.4 METHOD 2

A text message of strings of some length/size 1 from the sender is converted in to a stream of numerals with the help of some coding process (Probably may be the standard codes like A - 1, B - 2,…z - 26 and for space - 0) which is again converted in to a matrix (called a message matrix M) of size $m \times n$ where $n < m$ and n is the least such that $m \times n \geq 1$ depending upto the length of the message. In such case the size of the Encoder (The induced

Diagonal matrix of a Quadratic form of suitable variables) becomes N . Then the Encode need not to be an arbitrary matrix where as it may be taken as a diagonal matrix of size n whose inverse can be readily obtained.

Then the message matrix is converted into a New Matrix X (Encoded Matrix) using Matrix Multiplication as X = ME. Then this is sent to the receiver. Then the receiver decodes this matrix with the help of a matrix D (Decoder matrix) which is nothing but the inverse of the encoder (ie, $A=A^{-1}$), to get the message matrix back as $M = XE^{-1}$. Then with the previously used codes the receiver can get back the message in terms of the numerals which again can be converted to the original text message. When the length/size of the text message is too large, the value of n become higher, leading to the need of higher order diagonal matrices induced from the quadratic forms of higher number of variables.

3.3.1: Algorithm

Encoding process

1. Covert the next message of length l in to a stream of Numerals using a user friendly scheme for both the sender and the receiver.
2. Place the numerals into matrix of order $m \times n$ where $n < m$ and n is the least such that $m \geq 1$ where n depends on the size of the message and call this as a Message Matrix M.
3. Multiply this message matrix by the Encoder E of size n. (Normally a induced diagonal matrix compatible for the product X = ME) and get the encoded matrix X.
4. Convert the message matrix in to the stream of numbers that contains the encrypted message and send to the receiver.

Decoding Process:

1. Place the encrypted streams of numbers that represent the encrypted message to a matrix.

2. Multiply the encoded matrix X with the decoder D = E^{-1} (The inverse of E) to get back the message matrix M.

3. Convert this message matrix in to a stream of numbers with the help of originally used scheme.

4. Convert this stream of numerals in to the text of the original message.

EXAMPLE. 3.4.1:

ENCODING PROCESS:

Consider the message to be sent: GOOD MORNING

STEP 1: The standard codes as follows:

A → 1 ; B → 2 ; ……. ; Z → 26 and space → 0

STEP 2: Convert the above message in to a stream of numerical values as follows :

G O O D M O R N I N G

7 15 15 4 0 13 15 18 14 9 14 7

STEP 3: Construct the message matrix M with this stream of numerals as

$$M = \begin{bmatrix} 7 & 15 & 15 \\ 4 & 0 & 13 \\ 15 & 18 & 14 \\ 9 & 14 & 7 \end{bmatrix}$$ Which is of order 4×3.(using theorem)

STEP 4: Based on this, the 3rd order diagonal matrix (The diagonalized matrix of the matrix of a Quadratic form of suitable variables otherwise called the matrix of the canonical form).

Example: If the Quadratic form is $2x_1^2+x_2^2+x_3^2+2x_1x_2-2x_1x_3-4x_2x_3$

then the matrix of the Quadratic form is

$\begin{bmatrix} 2 & 1 & -1 \\ 1 & 1 & -2 \\ -1 & -2 & 1 \end{bmatrix}$. Also , the canonical form is $-y_1^2+y_2^2+4y_3^2$ whose matrix is given by D(-1,1,4)=$\begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 4 \end{bmatrix}$

STEP 5: Then the Encoder as E =$\begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 4 \end{bmatrix}$

STEP 6: Then the encoded matrix is given by

$$X = ME = \begin{bmatrix} 7 & 15 & 15 \\ 4 & 0 & 13 \\ 15 & 18 & 14 \\ 9 & 14 & 7 \end{bmatrix} \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 4 \end{bmatrix} = \begin{bmatrix} -7 & 15 & 60 \\ -4 & 0 & 52 \\ -15 & 18 & 56 \\ -9 & 14 & 28 \end{bmatrix}$$

STEP 7: The encoded numeric message is given by

-7 15 60 -4 0 52 -15 18 56 -9 14 28

DECODING PROCESS:

STEP 1: Find the Decoder E^{-1} is given by

$$E=\begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 4 \end{bmatrix}$$

$$E^{-1}= \frac{1}{|E|} \text{ (adjE)}$$

$$|E|=\begin{vmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 4 \end{vmatrix} = -1(4-0)-0+0 = 4$$

$$\text{AdjE}=\begin{pmatrix} +\begin{vmatrix}1 & 0\\ 0 & 4\end{vmatrix} & -\begin{vmatrix}0 & 0\\ 0 & 4\end{vmatrix} & +\begin{vmatrix}0 & 1\\ 0 & 0\end{vmatrix} \\ -\begin{vmatrix}0 & 0\\ 0 & 4\end{vmatrix} & +\begin{vmatrix}-1 & 0\\ 0 & 4\end{vmatrix} & -\begin{vmatrix}-1 & 0\\ 0 & 0\end{vmatrix} \\ +\begin{vmatrix}0 & 0\\ 1 & 0\end{vmatrix} & -\begin{vmatrix}-1 & 0\\ 0 & 0\end{vmatrix} & +\begin{vmatrix}-1 & 0\\ 0 & 1\end{vmatrix} \end{pmatrix}$$

$$= \begin{bmatrix} 4 & 0 & 0 \\ 0 & -4 & 0 \\ 0 & 0 & -1 \end{bmatrix}$$

$$E^{-1} = \frac{1}{|E|}\ (\text{adjE}) \quad = \frac{1}{-4}\begin{bmatrix} 4 & 0 & 0 \\ 0 & -4 & 0 \\ 0 & 0 & -1 \end{bmatrix} = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \frac{1}{4} \end{bmatrix}$$

STEP 2: The encoded numeric message is to be decoded by first writing the encoded matrix from the received message as

$$M = XE^{-1} = \begin{bmatrix} -7 & 15 & 60 \\ -4 & 0 & 52 \\ -15 & 18 & 56 \\ -9 & 14 & 28 \end{bmatrix}\begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \frac{1}{4} \end{bmatrix} = \begin{bmatrix} 7 & 15 & 15 \\ 4 & 0 & 13 \\ 15 & 18 & 14 \\ 9 & 14 & 7 \end{bmatrix}$$

STEP 3: The matrix M is converted in to numeric message as

7 15 15 4 0 13 15 18 14 9 14 7

STEP 4: This stream of numerals is converted in to the text message as

7 15 15 4 0 13 15 18 14 9 14 7

G O O D M O R N I N G

3.5 METHOD 3:

ALOGRITHM:

ENCODING PROCESS:

1. Convert the text message of length I into a stream of Numerals using a user friendly scheme for both the sender and the receiver again convert the text message into a stream of numerals using the standard codes.
2. First text message is converted into a matrix using A-7,B-6,……,Z-21.Again the text message is converted into matrix using standard codes (A-1,B-2,……Z-26).

3. Standard codes matrix is converted into a confusing message using A-7,B-6,…….Z-21.

DECODING PROCESS:

Reversing the process of encoding.

EXAMPLE. 3.5.1

Instead of using the standard codes

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

Alphabet	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Space
Number	14	15	16	17	18	19	20	21	22	23	24	25	26	0

Use the codes assigned as

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

Alphabet	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	Space
Number	15	16	17	18	19	14	20	26	25	24	23	22	21	0

(In a random way or by using some generator using Number theory or Combinatorics)

By above method we can also solve this for assigned codes

$$M = \begin{bmatrix} 1 & 16 & 16 \\ 4 & 0 & 13 \\ 16 & 19 & 15 \\ 9 & 15 & 1 \end{bmatrix} \quad \text{Instead of} \quad M = \begin{bmatrix} 7 & 15 & 15 \\ 4 & 0 & 13 \\ 15 & 18 & 14 \\ 9 & 14 & 7 \end{bmatrix}$$

Anyone who intervene the communication uses the standard codes for this message matrix will get a confusing like ANNO MNQSISA. So messengers are advised to make use of their convenient system of codes in order to have higher security level.

3.6 OPERATION ON STRINGS:

Define the operator +(The string addition) as usual in the case of addition of strings.

Example: Good+Morning = Good morning.

Using this operation, decompose the message of larger length in to message of shorter lengths and finally these are coined to get the message of larger length.

EXAMPLE 3.6.1:

Consider the message

M: GOOD LUCK AND ALL THE BEST. This message is decomposed in to two message as follows,

M = M1 + M2 Where M1 = GOOD LUCK & M2 = AND ALL THE BEST.

We can also solve this example by above methods.

CHAPTER IV

CHAPTER IV

NUMBER THEORY IN CRYPTOGRAPHY

This chapter deals the concepts of number theory and applications of number theory in encoding and decoding process of cryptography.

4.1 Number Theory:

Number theory is a branch of pure mathematics devoted to the study of the natural numbers and the integers. It is the study of the set of positive whole numbers which are usually called the set of natural numbers. As it holds the foundational plane in the discipline, Number Theory is also called “THE QUEEN OF MATHEMATICS”.

4.2 CAESAR CIPHER KEY CRYPTOGRAPHY

One of the earliest cryptographic system was used by great Roman emperor Julius Caesar around 50 (B.C.). Caesar wrote to Marcus Cicero using a rudimentary substitution cipher in which each letter of the alphabet is replaced by Letter that occurs three places down the alphabet. With the last three letters cycled back to the first three letters. Underneath the plain text letter the substitution alphabet for Caesar cipher is given by

Alphabet	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
Assigning Alphabet	D	E	F	G	H	I	J	K	L	M	N	O	P

Alphabet	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
Assigning Alphabet	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

4.3 Congruence :

Let a and b be two integers and m is any positive integer then a is said to congruent to b modulo m if m divide difference of a and b i.e. m/a-b. It is

denoted by a≡b(mod m)

For example 13≡3(mod 5)

4.3.1 Properties of congruence

1). $a \equiv b \pmod m$ if and only if $b \equiv a \pmod m$

2). $a \equiv b + c \pmod m$ if and only if $a-c \equiv b \pmod m$

3). $a \equiv b \pmod m$ and $a \equiv b \pmod m$ then $a + a \equiv b + b \pmod m$

4). $a \equiv b \pmod m$ and c is any integer then $ca \equiv cb \pmod m$

5). $a \pm mk \equiv a \pmod m$ where k is any integer

4.3.2 Congruence Modulo :

Let m be a positive integer, a is congruent to b(mod m) if m/(a-b) where a and b are integers that is $a = b + km$ and $k \in z$, $a \equiv b \pmod m$ is called congruence relation, the number m is the modulus of congruence.

4.4 METHOD 1:

4.4.1 Algorithm:

Encoding Process:

1. Convert the text message into numerals.
2. By using congruence $C \equiv P+3 \pmod{26}$ numerals values converted into another number value.
3. This numeral values are converted into confusing message.

Decoding Process:

1. Covert the confusing message into Numerals.
2. By using congruence $P \equiv C-3 \pmod{26}$
3. This numeral values are converted into text message.

4.4.2 EXAMPLE:

NUMBER THEORY IS EASY is transformed into QXPEHU WKHRUPLV HDVB with the help of congruence theory Caesar cipher can be easily described. Any plaintext is first expressed numerically by transforming the character of the text into digit by means of some correspondence such as

Alphabet	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
Number	0	1	2	3	4	5	6	7	8	9	10	11	12

Alphabet	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**
Number	13	14	15	16	17	18	19	20	21	22

Alphabet	**X**	**Y**	**Z**
Number	23	24	25

Now if P is the plain text and C is the cipher text then C≡P+3(mod 26)

N U M B E R T H E O R Y I S E A S Y

13 20 12 1 417 19 7 4 14 17 24 8 18 4 0 18 24

Using Congruence C=P+3(mod 26),for each alphabet and corresponding digit we get

16 23 15 4 7 20 22 10 7 17 20 1 11 21 7 3 21 1

Q X P E H U W K H R U B L V H D V B

To recover plain text this procedure is reversed by using C-3=P(mod 26)

That is P≡C-3 (mod 26)

4.5 METHOD 2:

4.5.1 Algorithm:

Encoding Process:

1.Splitting the plaintext into successive letters of three

2.Assigning numeral values to each letter and arrange them as m × n matrix.

3.multiply the message matrix and key matrix A with (mod 26). Where A as a non-singular matrix and get the m × n matrix.

4.This m × n matrix is converted into the text message. The text message is considered as a encrypted message.

Decoding Process:

1.Splitting the encrypted message into successive letters of three.

2.Assigning numeral values to each letter and arrange them as m × n matrix.

3.Multiply the encrypted matrix and inverse of A with (mod 26) and get the m × n matrix.

4.This m × n matrix is converted into the text message. The text message is considered as a decrypted message.

4.5.2 EXAMPLE 1:

As there are 26 letters in alphabet, so taking matrix modulo 26.

Alphabet	A	B	C	D	E	F	G	H	I
Number	1	2	3	4	5	6	7	8	9

Alphabet	J	K	L	M	N	O	P	Q	R
Number	10	11	12	13	14	15	16	17	18

Alphabet	S	T	U	V	W	X	Y	Z
Number	19	20	21	22	23	24	25	26

The encoded matrix can be formed by multiplying a non - singular matrix by the corresponding column vectors. Consider the

Alphabet	A	B	C	D	E	F	G	H	I
Number	1	2	3	4	5	6	7	8	9
	-26	-25	-24	-23	-22	-21	-20	-19	-18

Alphabet	J	K	L	M	N	O	P	Q	R
Number	10	11	12	13	14	15	16	17	18
	-17	-16	-15	-14	-13	-12	-11	-10	-9

Alphabet	S	T	U	V	W	X	Y	Z	space
Number	19	20	21	22	23	24	25	26	0
	-8	-7	-6	-5	-4	-3	-2	-1	0

Encoding process:

Consider the message to be sent

TIT FOR TAT

STEP 1: Spiliting the plaintext into successive letters of three

TIT FOR TAT

STEP 2: Assigning numerical value to each letters from the above table,and arrange them as 3 x 1 matrix

$$\text{TIT} = \begin{bmatrix} 20 \\ 9 \\ 20 \end{bmatrix} \qquad \text{FOR} = \begin{bmatrix} 6 \\ 15 \\ 18 \end{bmatrix} \qquad \text{TAT} = \begin{bmatrix} 20 \\ 1 \\ 20 \end{bmatrix}$$

STEP 3: Multiply this message matrix by the key matrix A with (mod 26)

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix} \begin{bmatrix} 20 \\ 9 \\ 20 \end{bmatrix} \text{mod26} = \begin{bmatrix} 98 \\ 89 \\ 154 \end{bmatrix} \text{mod26} = \begin{bmatrix} 20 \\ 11 \\ 24 \end{bmatrix} \rightarrow \text{ULY}$$

$$\begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix} \begin{bmatrix} 6 \\ 15 \\ 18 \end{bmatrix} \text{mod26} = \begin{bmatrix} 90 \\ 87 \\ 120 \end{bmatrix} \text{mod26} = \begin{bmatrix} 12 \\ 9 \\ 16 \end{bmatrix} \rightarrow \text{MJQ}$$

$$\begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix} \begin{bmatrix} 20 \\ 1 \\ 20 \end{bmatrix} \text{mod26} = \begin{bmatrix} 82 \\ 81 \\ 106 \end{bmatrix} \text{mod26} = \begin{bmatrix} 4 \\ 3 \\ 2 \end{bmatrix} \rightarrow \text{EDC}$$

STEP 4: The encrypted message to be sent is

ULYMJQEDC

Decoding process:

STEP 1: Find the inverse matrix A

$$A=\begin{bmatrix}1 & 2 & 3\\ 0 & 1 & 4\\ 5 & 6 & 0\end{bmatrix}$$

$$A^{-1}=\frac{1}{|A|}(adjA)$$

$$A^{-1}=\begin{bmatrix}-24 & 28 & 5\\ 20 & -15 & -4\\ -5 & 4 & 1\end{bmatrix}$$

$$=\begin{bmatrix}2 & 18 & 5\\ 20 & 11 & 12\\ 21 & 4 & 1\end{bmatrix}$$

STEP 2: Multiply this encrypted matrix by the inverse of key matrix A with (mod26)

$$\begin{bmatrix}2 & 18 & 5\\ 20 & 11 & 22\\ 21 & 4 & 1\end{bmatrix}\begin{bmatrix}U\\ L\\ Y\end{bmatrix}\bmod 26=\begin{bmatrix}2 & 18 & 5\\ 20 & 11 & 22\\ 21 & 4 & 1\end{bmatrix}\begin{bmatrix}20\\ 11\\ 24\end{bmatrix}\bmod 26=\begin{bmatrix}358\\ 1049\\ 488\end{bmatrix}\bmod 26=\begin{bmatrix}20\\ 9\\ 20\end{bmatrix}$$

$\rightarrow$TIT

$$\begin{bmatrix}2 & 18 & 5\\ 20 & 11 & 22\\ 21 & 4 & 1\end{bmatrix}\begin{bmatrix}M\\ J\\ Q\end{bmatrix}\bmod 26=\begin{bmatrix}2 & 18 & 5\\ 20 & 11 & 22\\ 21 & 4 & 1\end{bmatrix}\begin{bmatrix}12\\ 9\\ 16\end{bmatrix}\bmod 26=\begin{bmatrix}266\\ 691\\ 304\end{bmatrix}\bmod 26\begin{bmatrix}6\\ 15\\ 18\end{bmatrix}$$

$\rightarrow$FOR

$$\begin{bmatrix} 2 & 18 & 5 \\ 20 & 11 & 22 \\ 21 & 4 & 1 \end{bmatrix}\begin{bmatrix} E \\ D \\ C \end{bmatrix} \bmod 26 = \begin{bmatrix} 2 & 18 & 5 \\ 20 & 11 & 22 \\ 21 & 4 & 1 \end{bmatrix}\begin{bmatrix} 4 \\ 3 \\ 2 \end{bmatrix} \bmod 26 = \begin{bmatrix} 72 \\ 157 \\ 98 \end{bmatrix} \bmod 26 = \begin{bmatrix} 20 \\ 1 \\ 20 \end{bmatrix}$$

$$\rightarrow \text{TAT}$$

STEP 3: The decrypted message is

TIT FOR TAT

CHAPTER V

CHAPTER V

APPLICATIONS OF CRYPTOGRAPHY IN REAL LIFE

Cryptography in modern living

- **Secure Communications**

  ➔ **Document/Data/email Encryption**

  Cryptography in everyday life' contains a range of situations where the use of cryptography facilitates the provision of a secure service: cash withdrawal from an ATM, Pay TV, email and file storage using Pretty Good Privacy (PGP) freeware, secure web browsing, and use of a GSM mobile phone.

- **Identification and Authentication**

  ➔ **Smart Cards**

  Cryptography allows us to have confidence in our electronic transactions.

- **Electronic Commerce and Payments**

  ➔ **ATMs / Credit Cards**

  ➔ **Net Banking / Web Security**

  Encryption is used in electronic transactions to protect data such as account numbers and transaction amounts, digital signatures replace handwritten signatures or credit card authorizations, and public-key encryption provides confidentiality.

CONCLUSION

CONCLUSION

Keeping a secret is the standard use of cryptography. This is where one wants to either send some information to someone else, or wants to store information in a way that prevents others from snooping the files. Secure network communication, financial, government, medical, even multiplayer games. Applications of number theory allow the development of mathematical algorithms that can make information (data) unintelligible to everyone except for intended users.

BIBLIOGRAPHY

BIBLIOGRAPHY

1. David and M. Burton - Elementary Number Theory, 2nd Edition, USB Publishers.

2. P. Shanmugam and C. Loganathan - Involuntary Matrix in Cryptography, IJRRAS,6(4)(2011).