AMRITA VISHWA VIDYAPEETHAM | School of Engineering

DEEMED TO BE UNIVERSITY

Cryptography with Linear Algebra

CSE-AI, AMRITA VISHWA VIDYAPEETHAM, COIMBATORE AMRITA VISHWA VIDYAPEETHAM, AMRITANNAGAR P.O., COIMBATORE – 641 112

Batch – 06

Penaka Vishnu Reddy (CB.EN.U4AIE20048) & Krishnan KM (CB.EN.U4AIE20031)

ACKNOWLEDGEMENT :

We would like to thank all those who have helped us in completing this project of "CRYPTOGRAPHY WITH LINEAR ALGEBRA" under the subject "MATHEMATICS FOR INTELLIGENT SYSTEMS-1".

We would like to show our sincere gratitude to our professor DR.KP SOMAN without whom the project would not have initiated, who taught us the basics to start and visualise the project and enlightened us with the ideas regarding the project, and helped us by clarifying all the doubts whenever being asked.

We would like to thank ourselves. Both of us were very much involved and gave our best which led us to a positive result. We helped each other and taught each other about various concepts regarding the project which helped in increasing our inner knowledge.

Contents :

Abstract

In this project we are first explaining the basics of Cryptography with explaining the terms related to cryptography.

And then we are explaining what are the different methods used for Cryptography and are explaining some of them briefly.

Then we are particularly going for Hill Cipher technique because it is the Cipher that basics rely on Linear Algebra.

And also we are explaining the terms regarding Linear Algebra.

And then we are briefly explaining how the Hill Cipher technique of Cryptography works and doing with hands.

Then we are explaining the same method using MATLAB as computational tool and through that codes we are explaining Cryptographic method.

And at last we are explaining the Applications of Cryptography in the real world.

Introduction

Basically here we are trying to explain what is Cryptography and how can it be implemented through concepts from Linear Algebra.

So, What is Cryptography !?

Cryptography is a method of protecting communications and other data of information mainly through the use of coded, so that only for whom we are intended to send the information can read and process it.

The Word Cryptography is formed from :

Crypto – hidden

graphy – writing.

In Computer Science, Cryptography techniques are mainly deprived from mathematical concepts and a set of rule-based calculations called algorithms. They are used to transform messages in ways that are hard to decipher.

These algorithms are mainly used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet, and confidential communications such as credit card transactions and email.

So, Where it all began !?

This art of cryptography is considered to be born along with the art of writing. As people civilisation began, as like now people formed different groups and thus they started fighting for the higher positions in each kingdoms. So they began forming political parties and they started to kill each other and started to spy each other. So the secrecy of communication came into importance so they started transferring their information through so many signals, codes and other forms in which only some group of people can only understand.

The first known cryptography technique is believed as ‘Hieroglyph’

This involved replacing alphabets of message with other alphabets with some secret rule. This rule became a key to retrieve the message back from the garbled message.

What all are the advantages of using Cryptography techniques !?

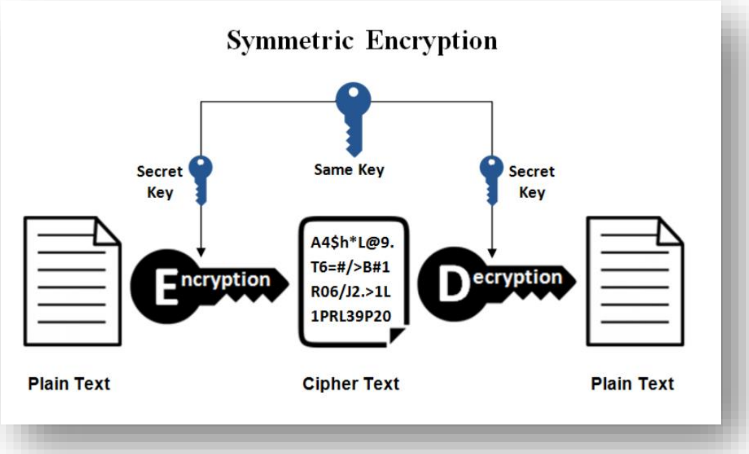
- Confidentiality :
  The information can only be accessed by the person for whom the message is intended. No other person is able to access this.
- Integrity :
  The message or information can't be modified in storage or transition between the sender and receiver without any information other than the message being detected.
- Non – repudiation :
  The denial of the message a sender sent at a future situation is not possible.
- Authentication :
  The identities of sender and receiver as well as the destination of information are safe.

What are the types of cryptography !?

There are three types of cryptography

- Symmetric Key Cryptography (Private/Secret Key Cryptography)
- Asymmetric Key Cryptography (Public Key Cryptography)
- Hash function

Symmetric Key Cryptography :



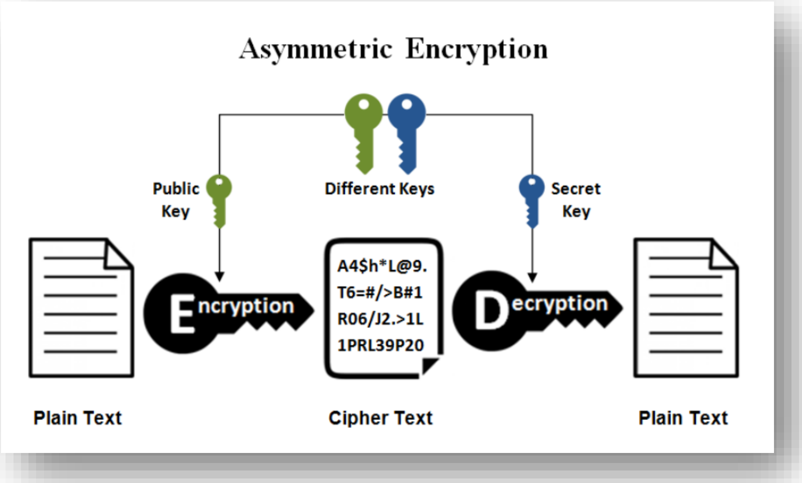
It is a type of cryptography in which the single common key is used by both the sender and receiver for the purpose of encryption and the decryption of the message.

Here it is also known as private or secret key cryptography and AES(Advanced Encryption System) is the most widely uses symmetric key cryptography.

The symmetric key system has one major drawback that the two parties must somehow exchange the key in a secure way that no one should find the key it break the security as there is only one single key for encryption as well as decryption process.

Types : **Hill Cipher**, AES(Advanced Encryption Standard), DES, Triple DES, RC2, RC4, RC5, IDEA, Blowfish, Stream cipher, Block cipher, etc. are the types of symmetric key cryptography.

Asymmetric Key Cryptography :



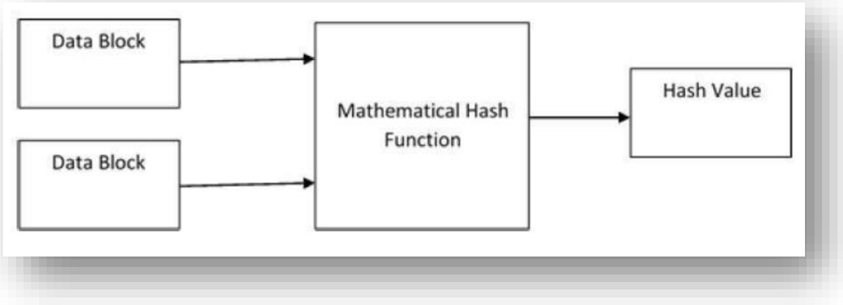
It is a completely different and more secure method than symmetric key cryptography.

Here every user uses two keys or a pair of keys (private and public key) for encryption and decryption process. Private key is kept as a secret with every user and public key is distributed over the network so if anyone wants to send message to any user can use those public keys.

Either of the key can be used to encrypt the message and the one left is used for decryption purpose. Asymmetric key cryptography is also known as public key cryptography and is more secure than symmetric key. RSA is the most popular and widely used asymmetric algorithm.

Types : RSA, DSA, PKCs, Elliptic Curve techniques, etc. are the common types of asymmetric key cryptography.

Hash Function :



A Hash function is a cryptography algorithm that takes input of arbitrary length and gives the output in fixed length. The hash function is also considered as a mathematical equation that takes seed (numeric input) and produce the output that is called hash or message digest. This system operates in one-way manner and does not require any key. Also, it is considered as the building blocks of modern cryptography.

The hash function works in a way that it operates on two blocks of fixed length binary data and then generate a hash code. There are different rounds of hashing functions and each round takes an input of combination of most recent block and the output of the last round.

Types : Some popular hash functions are Message Digest 5 (MD5), SHA (Secure Hash Algorithm), RIPEMD, and Whirlpool. MD5 is the most commonly used hash function to encrypt and protect your passwords and private data.

Terminologies used in Cryptography :

Plain Text :

It refers to the text before encryption. It can be also defined as the information that is being encrypted.

Cipher Text :

It is defined as the message created after using cipher or we can call it as an encrypted message.

Encryption :

Encryption is a process which transforms the original information or data into a disguised form. This new form of the message is entirely different from the original message. Encryption is usually done using key algorithms.

Decryption :

It is exactly opposite to encryption. Decryption is a process of converting encoded/encrypted data in a form that is readable and understood by a human or a computer. This method is performed by un-encrypting the text manually or by using algorithms used to encrypt the original data.

But, What is a Cipher :

Cipher is an algorithm which is applied to plain text to get ciphertext. It is the disguised output of an encryption algorithm. The term “cipher” is sometimes used as an alternative term for ciphertext. Ciphertext is not understandable until it has been converted into plain text using a key.

Earlier cipher algorithms were performed manually and were entirely different from modern algorithms which are generally executed by a machine.

All ciphers involve either transposition or substitution, or a combination of these two mathematical operations—i.e., product ciphers. In transposition cipher systems, elements of the plaintext (e.g., a letter, word, or string of symbols) are rearranged without any change in the identity of the elements. In substitution systems, such elements are replaced by other objects or groups of objects without a change in their sequence. In systems involving product ciphers, transposition and substitution are cascaded; for example, in a system of this type called a fractionation system, a substitution is first made from symbols in the plaintext to multiple symbols in the ciphertext, which is then “superencrypted” by a transposition. All operations or steps involved in the transformation of a message are carried out in accordance to a rule defined by a secret key known only to the sender of the message and the intended receiver.

Cipher devices or machines have commonly been used to encipher and decipher messages. The first cipher device appears to have been employed by the ancient Greeks around 400 BC for secret communications between military commanders. This device, called the scytale, consisted of a tapered baton around which was spirally wrapped a piece of parchment inscribed with the message. When unwrapped the parchment bore an incomprehensible set of letters, but when wrapped around another baton of identical proportions, the original text reappeared.

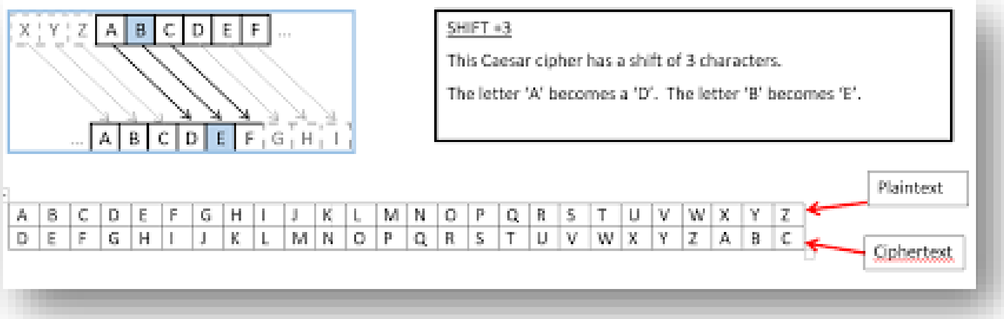
Normally there are lots of types of ciphers available. And each one are differentiated basis on their difficulty level and thus those are also made from different concepts.

Now let us discuss on some of the ciphers.

Here we are discussing about the following ciphers :

- Caesar cipher
- Substitution cipher
- Hill cipher

Caesar Cipher :



SHIFT +3

This Caesar cipher has a shift of 3 characters.

The letter 'A' becomes a 'D'. The letter 'B' becomes 'E'.

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
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

In Caesar cipher, the set of characters of plain text is replaced by any other character, symbols or numbers. It is a very weak technique of hiding text. In Caesar's cipher, each alphabet in the message is replaced by three places down.

Caesar cipher algorithm is as follows:

- Read each alphabet of plain text
- Replace each alphabet by 3 places down.
- Repeat the process for all alphabet in the plain text.

Let us see one example :

Message : THISISMISPROJECT

Encrypted Message : WKLVLVPLVSURMHFW

Substitution Cipher :

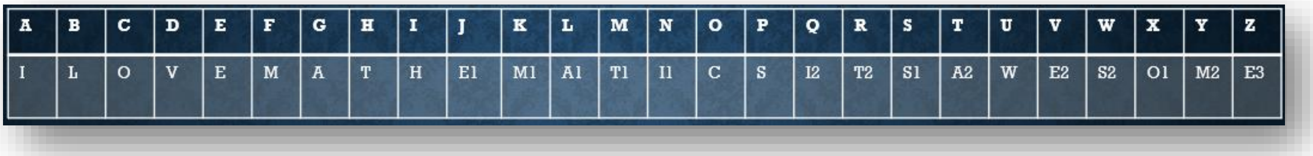
Substitution ciphers encrypt the plaintext by swapping each letter or symbol in the plaintext by a different symbol or letter or number to encrypt a text sequence.

Here we can choose any set of that numbers and thus making a new type of key.

Perhaps the simplest substitution cipher is the Caesar cipher, named after the man who used it.

Technically speaking, the Caesar cipher may be differentiated from other, more complex substitution ciphers by terming it either a shift cipher or a mono-alphabetic cipher; both are correct.

Let us see an example :



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
I	L	O	V	E	M	A	T	H	E1	M1	A1	T1	I1	C	S	I2	T2	S1	A2	W	E2	S2	O1	M2	E3

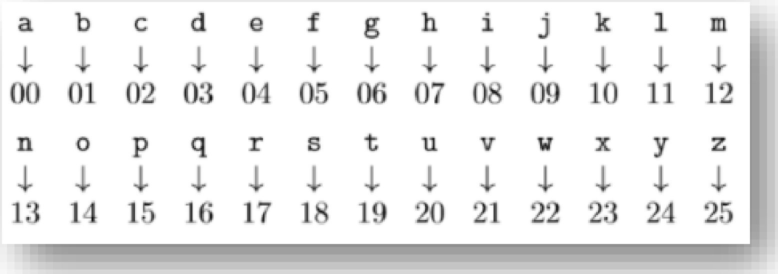
This is a type of substitution cipher we have made and we assigned these certain letters to each alphabet.

Message is : KRISHVISH

Encrypted message is : MT2HSTE2HST

Now we have seen two types of ciphers and now we are really coming to the topic of our project. That is Cryptography with Linear Algebra. So the above ciphers are not used based on the concept of linear algebra but the next cipher, Hill Cipher, is the one which is based on linear algebra.

Hill Cipher :



a	b	c	d	e	f	g	h	i	j	k	l	m
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
00	01	02	03	04	05	06	07	08	09	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
13	14	15	16	17	18	19	20	21	22	23	24	25

Hill cipher works on the multiple alphabets at the same time. Hill cipher works as follows:

1. Assign the number to each alphabet in the plain text. A = 0, B = 1 …. Z = 25
2. Organize the plain text message as a matrix of numbers base on the above step that is in number format. The resultant matrix is called a Plain text matrix.
3. Multiply the plain text matrix with a randomly chosen key. Note that the key matrix must be the size of **n*n** where n stands for the number of rows in a plain text matrix.
4. Multiply both the matrix i.e. step 2 and step 3.
5. Calculate the mod 26 value of the above matrix i.e. matrix results in step 4.
6. Now translate the numbers to alphabets i.e. 0 = A, 1 = B, etc.
7. The result of step 6 becomes our ciphertext.

Here we can use ASCII Code system to convert to encrypted text that is by adding the Cipher numbers (0 to 25) by 65. It will become ASCII Code. So we can use this method in code.

By the way what is ASCII Code System !?

Short for American Standard Code for Information Interexchange

It basically assigns letters, numbers, and other characters in the 256 slots available in the 8 bit code. ASCII decimal (Dec) number is created from binary, which is the language of all computers. So basically we can tell that all the above mentioned characters can be assigned as numbers.

Here we only need the alphabets as ASCII code for Hill Cipher.

So let us see how all the alphabets are assigned in ASCII Codes.

The Capital letters (A to Z) are assigned from 65 to 90 respectively.

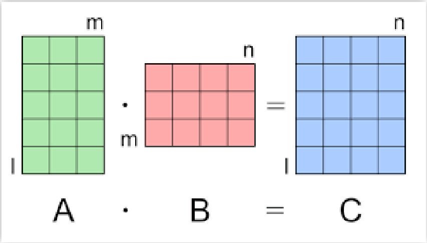
The Small letters (a to z) are assigned from 97 to 122 respectively.

Now we can see what all Linear Algebra concepts are used here :

- Matrix Multiplication
- Modular Arithmetic
- Multiplicative Inverse
- Inverse of a Matrix

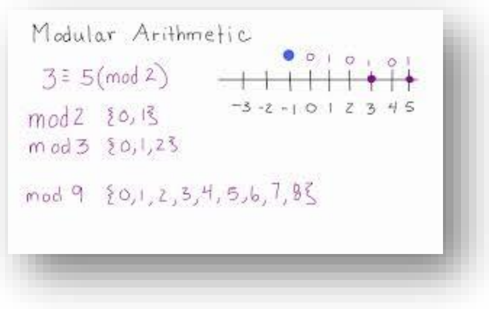
Now let us see each concepts in detail

Matrix multiplication :



- In mathematics, particularly in linear algebra, matrix multiplication is a binary operation that produces a matrix from two matrices.
- For matrix multiplication, the number of columns in the first matrix must be equal to the number of rows in the second matrix.

Modular Arithmetic :

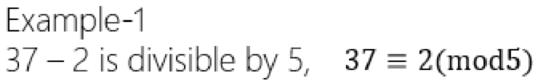


Modular arithmetic is a system of arithmetic for integers, where values reset and begin to increase again, after reaching a certain predefined value, called the modulus or modulo denoted by “Zm”.

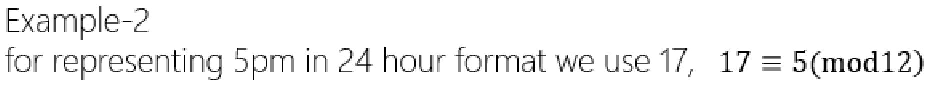
It is basically doing addition (and other operations) not on a line, as you usually do, but on a circle – the values “wrap around”, always staying less than a fixed number called the modulus.

$$y = qp + x$$
$$y \equiv x(\mathrm{mod}p)$$

y is divided by p has remainder x and q belongs to some integer.

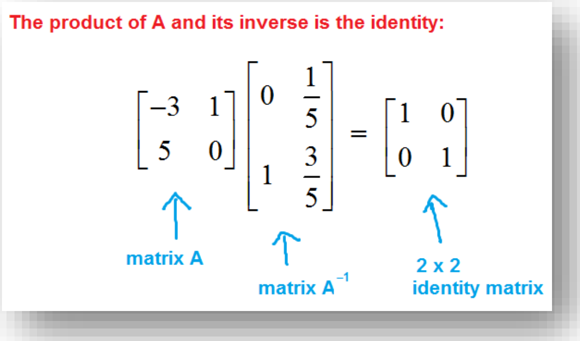


Example-1
37 – 2 is divisible by 5, $37 \equiv 2(\mathrm{mod}5)$



Example-2
for representing 5pm in 24 hour format we use 17, $17 \equiv 5(\mathrm{mod}12)$

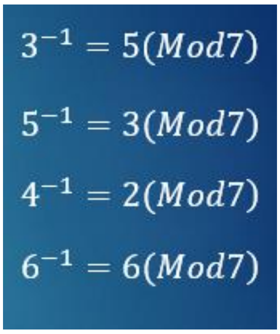
Multiplicative Inverse



The product of A and its inverse is the identity:

$$\begin{bmatrix} -3 & 1 \\ 5 & 0 \end{bmatrix} \begin{bmatrix} 0 & \frac{1}{5} \\ 1 & \frac{3}{5} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

- The multiplicative inverse of a matrix is similar in concept, except that the product of matrix A and its inverse A−1 equals the identity matrix.
- The identity matrix is a square matrix containing ones down the main diagonal and zeros everywhere else.
- Eg ;



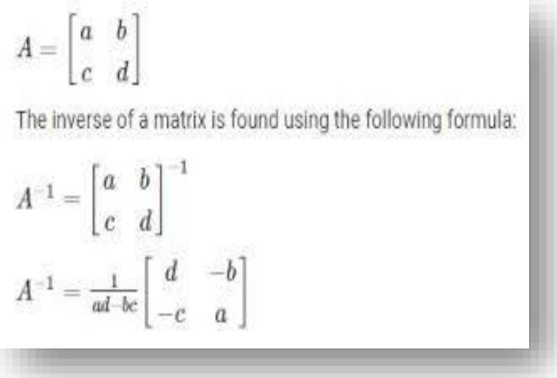
$3^{-1} = 5(Mod7)$

$5^{-1} = 3(Mod7)$

$4^{-1} = 2(Mod7)$

$6^{-1} = 6(Mod7)$

Inverse of a Matrix :



$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

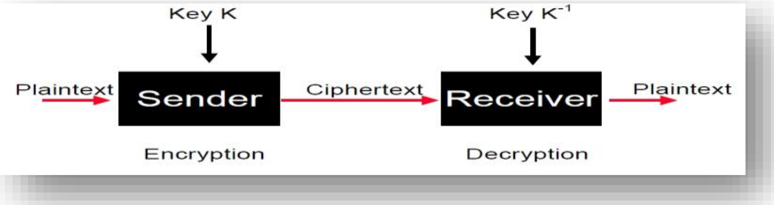
The inverse of a matrix is found using the following formula:

$$A^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1}$$

$$A^{-1} = \frac{1}{ad-bc}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

- The inverse of a matrix A is a matrix that, when multiplied by A results in the identity. The notation for this inverse matrix is A^{-1}.
- The inverse of A is A^{-1} only when: [$A \times A^{-1} = A^{-1} \times A = \mathbf{I}$]
- **Inverse of a Matrix = Adjoint of Matrix / Determinant**

Now we can see how this works !!!



Encryption :

Cipher text = (Plain text x Key)Mod 26

DECRYPTION:

Plain text = (Cipher text x Key^{-1})Mod 26

Now we can see an example !!

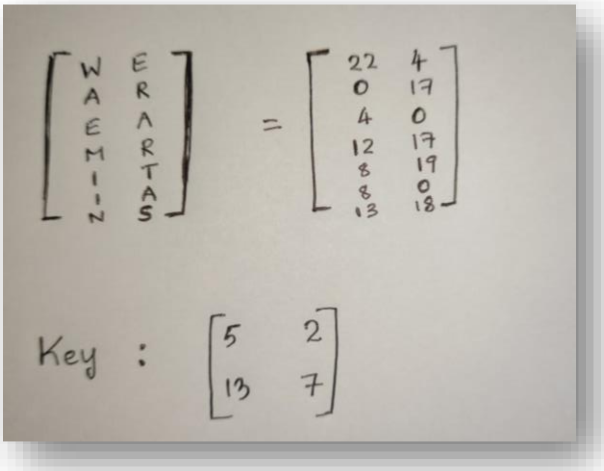
Message : WE ARE AMRITIANS (we don’t have to consider spaces)

Key used : F C N H

//Note : The Key must be invertible.

Encryption :

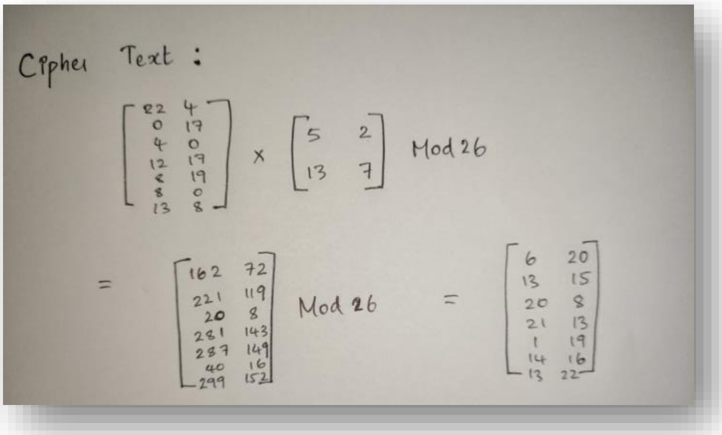
Now we can put our message in matrix form :



$$\begin{bmatrix} W & E \\ A & R \\ E & A \\ M & R \\ I & T \\ I & A \\ N & S \end{bmatrix} = \begin{bmatrix} 22 & 4 \\ 0 & 17 \\ 4 & 0 \\ 12 & 17 \\ 8 & 19 \\ 8 & 0 \\ 13 & 18 \end{bmatrix}$$

Key : $\begin{bmatrix} 5 & 2 \\ 13 & 7 \end{bmatrix}$

Now we can find Cipher text as follows :

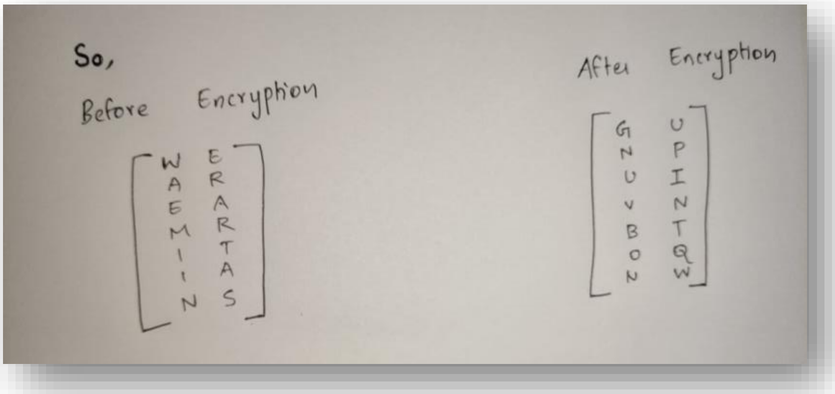


Cipher Text :

$$\begin{bmatrix} 22 & 4 \\ 0 & 17 \\ 4 & 0 \\ 12 & 17 \\ 8 & 19 \\ 8 & 0 \\ 13 & 8 \end{bmatrix} \times \begin{bmatrix} 5 & 2 \\ 13 & 7 \end{bmatrix} \text{ Mod } 26$$

$$= \begin{bmatrix} 162 & 72 \\ 221 & 119 \\ 20 & 8 \\ 281 & 143 \\ 287 & 149 \\ 40 & 16 \\ 299 & 152 \end{bmatrix} \text{ Mod } 26 = \begin{bmatrix} 6 & 20 \\ 13 & 15 \\ 20 & 8 \\ 21 & 13 \\ 1 & 19 \\ 14 & 16 \\ 13 & 22 \end{bmatrix}$$

So now we got Encrypted message :



So,

Before Encryption

$$\begin{bmatrix} W & E \\ A & R \\ E & A \\ M & R \\ I & T \\ I & A \\ N & S \end{bmatrix}$$

After Encryption

$$\begin{bmatrix} G & U \\ N & P \\ U & I \\ V & N \\ B & T \\ O & Q \\ N & W \end{bmatrix}$$

Decryption :

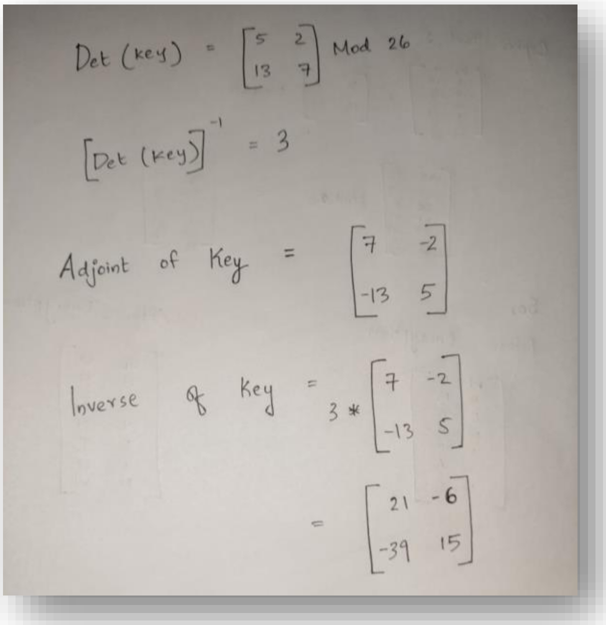
Plain text = (Cipher text x key^{-1})Mod 26

To Find (**key^{-1})**

(key^{-1}) = [Det(key)]$^{-1}$ x Adj(key)

Step-1 : Find determinant of key

Step-2 : Find adjoint of key



$$\text{Det (key)} = \begin{bmatrix} 5 & 2 \\ 13 & 7 \end{bmatrix} \text{Mod } 26$$

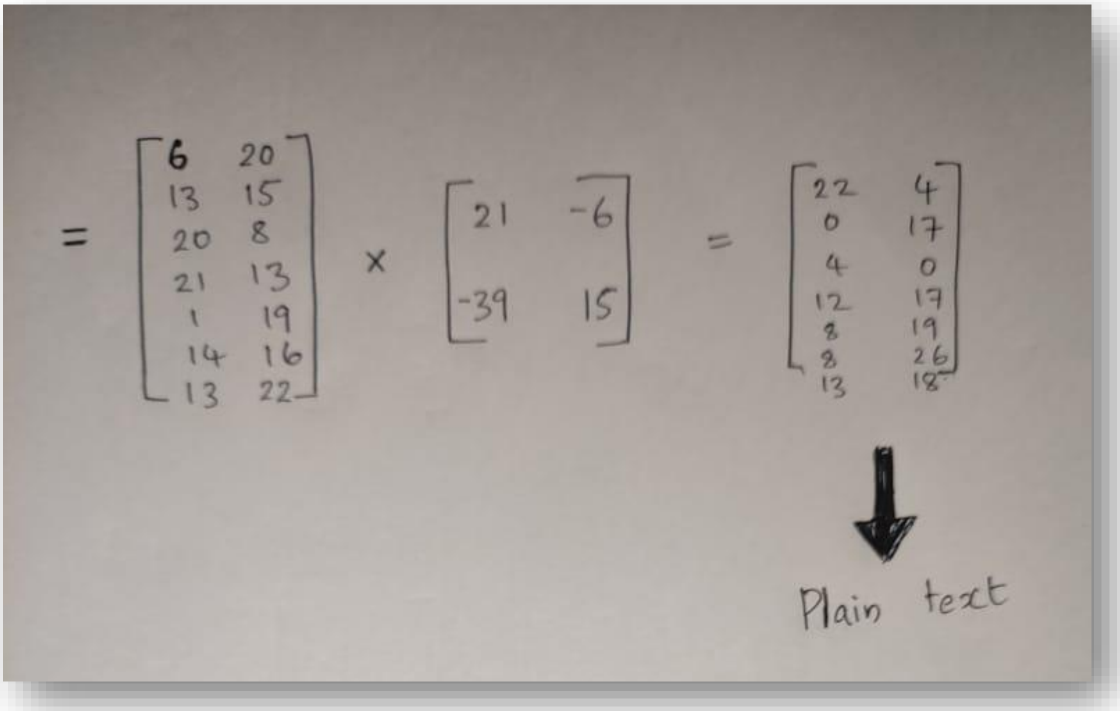
$$\left[\text{Det (key)}\right]^{-1} = 3$$

$$\text{Adjoint of Key} = \begin{bmatrix} 7 & -2 \\ -13 & 5 \end{bmatrix}$$

$$\text{Inverse of Key} = 3 * \begin{bmatrix} 7 & -2 \\ -13 & 5 \end{bmatrix}$$

$$= \begin{bmatrix} 21 & -6 \\ -39 & 15 \end{bmatrix}$$

Now Plain text = (Cipher text x key^{-1})Mod 26



$$= \begin{bmatrix} 6 & 20 \\ 13 & 15 \\ 20 & 8 \\ 21 & 13 \\ 1 & 19 \\ 14 & 16 \\ 13 & 22 \end{bmatrix} \times \begin{bmatrix} 21 & -6 \\ -39 & 15 \end{bmatrix} = \begin{bmatrix} 22 & 4 \\ 0 & 17 \\ 4 & 0 \\ 12 & 17 \\ 8 & 19 \\ 8 & 26 \\ 13 & 18 \end{bmatrix}$$

$$\Big\downarrow$$

Plain text

Now here when we convert this we will get the early processed plain text : **"WEAREAMRITIANS"**

This is how basically Cryptography processing works.

Now we can use MATLAB code to do the same.

MATLAB CODE with OUTPUT :

We have to give following information in Command Window :

Enter The plain Text : WEAREAMRITIANS

Enter the key size : (Must be 4,9,....) : 4

Enter the key: 5

Enter the key: 2

Enter the key: 13

Enter the key: 7

```
clc;clear;close all;

disp(‘************************************************************************’);
```

```
disp(‘*                           Cryptography                              *’);
```

```
*                            Cryptography                                 *
```

```
disp(‘************************************************************************’);
```

```

%Encryption

text=input(‘Enter The plain Text : ‘,’s’); %Input for the plain text
n = input(‘Enter the key size : (Must be 4,9,....) : ‘);%Entering the key size
n=sqrt(n);
upperString=upper(text); %Converting the string to capital letters
charText=char(upperString); %Converting from string to char
Actualtext=charText-65; %Substracting 65 to obtain the letters in the range of 0-25
jk=Actualtext;

%Reshaping the text and making it as a matrix
if(rem(size(Actualtext),n)==[1 0])
    Message=reshape(Actualtext,n,length(Actualtext)/n);
    Message = [Message]’;%Converting a row matrix to a matrix with n columns
else
Actualtext=[Actualtext 25] ;%Adding an extra dummy character at the end
    Message=reshape(Actualtext,n,length(Actualtext)/n);
    Message = [Message]’;
end
```

```
%Now analysing the key and checking whether the key is fine or not
theKey=0;
for i=1:(n^2)
key=input(‘Enter the key: ‘);
theKey=[theKey key];
end
realkey=theKey(2:end);
rrealkey=realkey+65;
Key=char(rrealkey);
Actualkey=reshape(realkey,n,n)’;

%Doing Encryption
if(det(Actualkey) ~= 0)%Checking whether key is invertible or not
    Encmessage=Message*Actualkey;%Multiplying the plain text with the key
    Encmessage=mod(Encmessage,26);%Finding the mod of the multiplied matrix
    Encmessage=[Encmessage]’;
    encmatrix=reshape(Encmessage,1,length(Actualtext));%Changing the matrix back to row
matrix
    encmatrix=encmatrix+65;
    disp(‘ The Encrypted text or Cipher Text is : ‘);
    char(encmatrix)
    Encrypted=char(encmatrix);
else
    disp(‘ The key matrix is not invertible ‘);
end
```

```
 The Encrypted text or Cipher Text is :

ans = ‘GUNPUIVNBTOQNW’
```

```
%Decryption

%Finding determinant of Key
    j=mod(det(Actualkey),26);
    for b = 1:26
        d(b)=j*b;
        h(b)=rem(d(b),26);
    end

%Finding [Det(key)]^-1
    h=uint8(h);
    m=find(h==1);

%Finding inverse of Key by the formula : (key^-1) = [Det(key)]^-1 x Adj(key)
    if(m ~=0)
        invk=m.*adjoint(Actualkey);
    else
        disp(‘Enter Another Key’);
        return;
    end

%Now decrypting the message
```

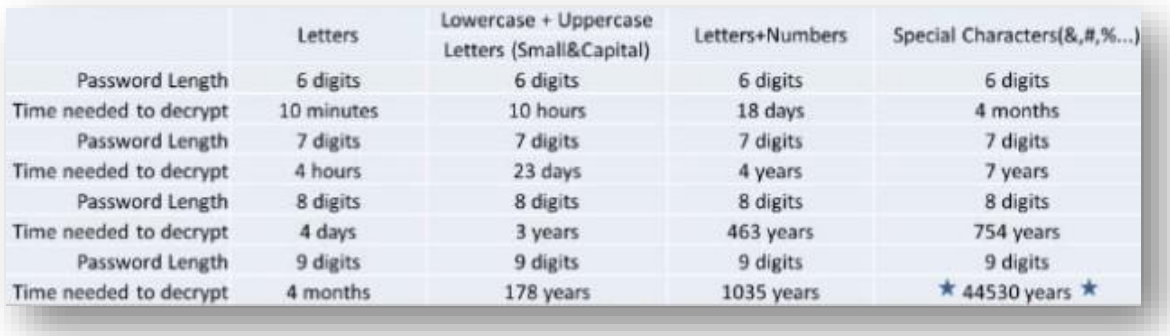
```
Encmessage=[Encmessage]’;
decmsg=Encmessage*invk; %Multiplying inverse with the encrypted message
decmsg=mod(decmsg,26);
decmsg=[decmsg]’;
decmsg=reshape(decmsg,1,length(Actualtext));
decmsg=decmsg+65;
if(rem(length(jk),n)==0)
    decmsg=uint8(decmsg);
    v=find(decmsg==91);
    decmsg(v)=65;
    disp(‘ The Decrypted text is : ‘);
    char(decmsg)
else
    decmsg=decmsg(1:length(Actualtext)-1);
    decmsg=uint8(decmsg);
    v=find(decmsg==91);
    decmsg(v)=65;
    char(decmsg);
end
```

```
 The Decrypted text is :

ans = ‘WEAREAMRITIANS’
```

APPLICATION OF CRYPTOGRAPHY :

1. Secrecy in transmission
2. Secrecy in storage
3. Integrity in transmission
4. Authentication of identity
5. Credentialing systems
6. Digital signatures
7. Electronic money
8. Threshold cryptosystem
9. Secure multi-party computation



	Letters	Lowercase + Uppercase Letters (Small&Capital)	Letters+Numbers	Special Characters(&,#,%...)
Password Length	6 digits	6 digits	6 digits	6 digits
Time needed to decrypt	10 minutes	10 hours	18 days	4 months
Password Length	7 digits	7 digits	7 digits	7 digits
Time needed to decrypt	4 hours	23 days	4 years	7 years
Password Length	8 digits	8 digits	8 digits	8 digits
Time needed to decrypt	4 days	3 years	463 years	754 years
Password Length	9 digits	9 digits	9 digits	9 digits
Time needed to decrypt	4 months	178 years	1035 years	★ 44530 years ★

NOTE:- *This is the time taken to decrypt (crack) a pass-word. So , it's always better to have a long and combinational password.*

These passwords in sites are stored in web using these methods.

WhatsApp is currently one of the most popular mobile messaging software.

The conversations and calls are 'end-to-end' encrypted. Once the client is registered, an encrypted session is created between two clients.

If for example client1 wants to send message to client2 the public keys of the client2 are retrieved from WhatsApp server, and this is used to encrypt the message.

CONCLUSION :

So thus our project is concluded with the detailed explanation of cryptography and its methods and how it can be connected to Linear Algebra concepts and we also see how it can be done using hand and using MATLAB codes.

And from the applications of cryptography, we understood that in this world of betrayal and spying how a cryptography can be utilised perfectly.

And we have seen lots of applications in our real world.

Anyway, this should be done very carefully and with known information of key and with well knowledge anyone can crack these data. So better we follow only the best methods of cryptography and best ciphers for the confidential communication.

So thus, by hoping that upcoming generation will use these methods to do only good deeds, we are concluding the project.

REFERENCE :

Links :

https://www.tutorialspoint.com/

https://www.geeksforgeeks.org/

https://www.thecrazyprogrammer.com/

https://www.computerhope.com/

www.mathworks.com

Books :

The Hill Cipher _A Linear Algebra Perspective

Hill Cipher – Jonaki B Ghosh

Notes :

Slides and Notes given by Dr. Soman KP

Lectures by Dr. Soman KP

Reference Notes sent by Dr. Soman KP
