AMRITA VISHWA VIDYAPEETHAM
ETTIMADAI, COIMBATORE

CRYPTOGRAPHY WITH LINEAR ALGEBRA

DEPARTMENT	**CSE-AI**
COURSE	**MATHEMATICS FOR INTELLIGENT SYSTEMS-1**
SEMESTER	**1**
INSTRUCTOR	**DR. KP SOMAN**

GROUP NUMBER – 17

GROUP MEMBERS

SL.NO	NAME
1.	PINGALI SATHVIKA
2.	BALA KARTHIKEYA

PROJECT REPORT SUBMITTED FOR THE END SEMESTER EXAMINATION OF 19MAT105 ON 27.02.2021

EXTERNAL EXAMINER INTERNAL EXAMINER

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.

INDEX

S. No	TOPIC
1	INTRODUCTION
2	DESCRIPTION
3	TYPES OF CRYPTOGRAPHY
4	TERMINOLOGIES USED IN CRYPTOGRAPHY
5	TYPES OF CIPHERS
6	MULTIPLICATIVE INVERSE,MODULAR ARITHMETIC
7	MATLAB CODE AND RESULTS
8	APPLICATIONS

Introduction: Cryptography is the study of the techniques of writing and decoding messages in code. 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.

Description:

In today's age of computers cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption. The process of conversion of cipher text to plain text this is known as decryption.

- **Types Of Cryptography:**
  In general there are three types Of cryptography:
- **Symmetric Key Cryptography:**
  It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system is Data Encryption System(DES).

- **Hash Functions:**
  Public and private key cryptographic algorithms both involve transforming plaintext into ciphertext and then back into plaintext. By contrast, a hash function is one-way encryption algorithm: once you've encrypted your plaintext, you can't ever recover it from the resulting ciphertext (referred to as a *hash*).
- **Asymmetric Key Cryptography:**
  Under this system a pair of keys is used to encrypt and decrypt information. A public key is used for encryption and a private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone knows the private key.

TERMINOLOGIES USED IN CRYPTOGRAPHY

- Plain Text :
- Cipher Text
- Encryption
- Decryption

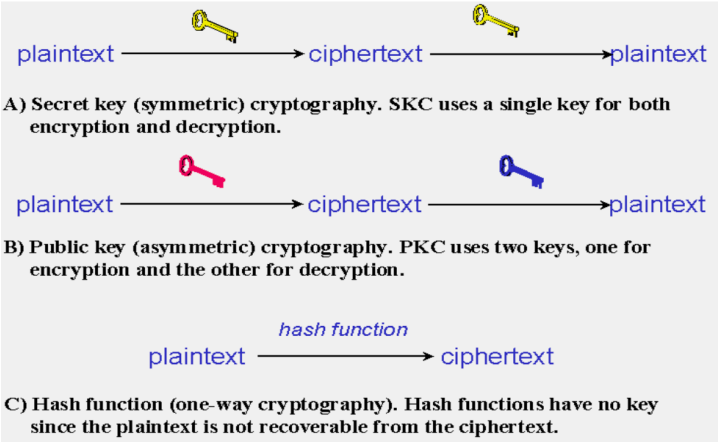
Plain Text: Plain text refers to message before Encryption. It is message or information that is being Encrypted.

Cipher Text: Cipher text is also known encrypted message or the message created after using cipher.

Encryption: Encryption is the process of translating plain text into something that appears to be random and meaningless.

Decryption: Decryption is the reverse of encryption That is converting the disguised form into original form.

- To encrypt more than a small amount of data, symmetric encryption is used. A symmetric key is used during both the encryption and decryption processes. To decrypt a particular piece of ciphertext, the key that was used to encrypt the data must be used.



- A cipher is a method of hiding words of text by replacing the original message with other letters and numbers. It is done by using a key this will be known only to sender and receiver.

TYPES OF CIPHERS

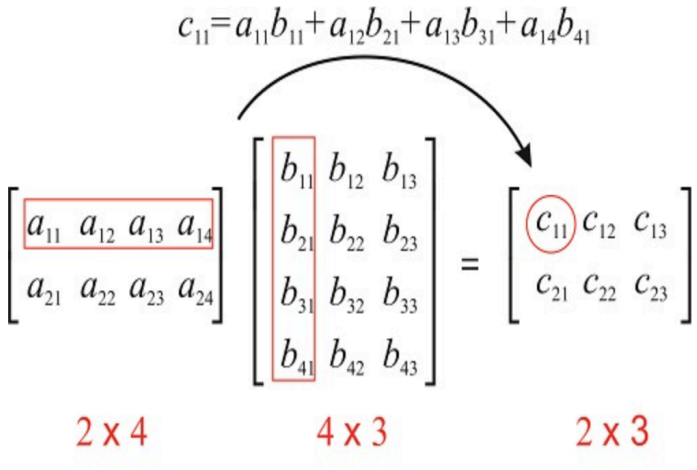
- **Substitution cipher:** Substitution cipher is a type of encryption in which characters of text are replaced by another letter or a number to encrypt a text sequence.

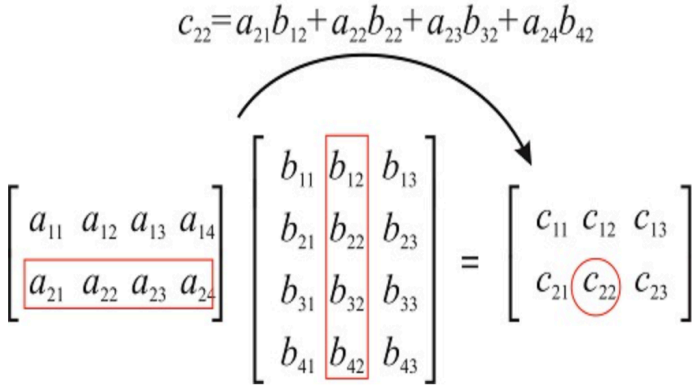
- **Caesar cipher:** In Caesar cipher, we will shift each letter by a fixed unit.
- **Hill cipher:** This system is called as hill cryptosystem, The key or cipher in this system is an invertible matrix of integers mod 26. In Hill cipher cryptosystem, first we will assign numbers to represent each letter of the alphabet.

KEY CONCEPTS USED

- Matrix multiplication
- Inverse of a matrix
- Modular arithmetic
- Multiplicative inverse

MATRIX MULTIPLICATION





INVERSE OF A MATRIX

Inverse of matrix =adjoint of matrix
determinant

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

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

$$A^{-1} = \frac{1}{|A|} \begin{bmatrix} \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} & \begin{vmatrix} a_{13} & a_{12} \\ a_{33} & a_{32} \end{vmatrix} & \begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix} \\ \begin{vmatrix} a_{23} & a_{21} \\ a_{33} & a_{31} \end{vmatrix} & \begin{vmatrix} a_{11} & a_{13} \\ a_{31} & a_{33} \end{vmatrix} & \begin{vmatrix} a_{13} & a_{11} \\ a_{23} & a_{21} \end{vmatrix} \\ \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix} & \begin{vmatrix} a_{12} & a_{11} \\ a_{32} & a_{31} \end{vmatrix} & \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \end{bmatrix}$$

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”.

$$y = qp + x$$

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

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

Example-1 22-2 is divisible by 5

$$22 \equiv 2(\mathrm{mod} 5)$$

MULTIPLICATIVE INVERSE

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

$$3^{-1} = 5(Mod7)$$
$$5^{-1} = 3(Mod7)$$
$$4^{-1} = 2(Mod7)$$
$$6^{-1} = 6(Mod7)$$

COMPUTATION IN MATLAB

```
clc;clear;close all;
disp('MIS PROJECT');
disp('Cryptography Using Linear Algebra');
text=input('Enter The plain Text : ','s'); %Input for the
plain text
n = input('Enter the key size : (Must be 4,9,....) : ');
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;
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
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)
if(det(Actualkey) ~= 0)
```

```
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;
Encrypted=char(encmatrix)
else
disp('The key matrix is not invertible')
end
%Decrypting the message
j=mod(det(Actualkey),26);
for b = 1:26
d(b)=j*b;
h(b)=rem(d(b),26);
end
% m =[3 10 20;20 9 17;9 4 17;]
h=uint8(h);
m=find(h==1);
if(m ~=0)
invk=m.*adjoint(Actualkey);
else
disp('Enter Another Key');
return;
end
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;
char(decmsg)
else
   decmsg=decmsg(1:length(Actualtext)-1);
   decmsg=uint8(decmsg);
   v=find(decmsg==91);
   decmsg(v)=65;
   char(decmsg)
end
```

RESULTS

```
clc;clear;close all;
disp('MIS PROJECT');
```

```
MIS PROJECT
```

```
disp('Cryptography Using Linear Algebra');
```

```
Cryptography Using Linear Algebra
```

```
text=input('Enter The plain Text : ','s'); %Input for the plain text
n = input('Enter the key size : (Must be 4,9,....) : ');
n=sqrt(n);
upperString=upper(text) %Converting the string to capital letters
```

```
upperString = 'MYNAMEISRITHVIK'
```

```
charText=char(upperString) %Converting from string to char
```

```
charText = 'MYNAMEISRITHVIK'
```

```
Actualtext=charText-65 %Substracting 65 to obtain the letters in the range of 0-25
```

```
Actualtext = 1×15
     12    24    13     0    12     4     8    18    17     8    19     7    21     8    10
```

```
jk=Actualtext;
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
```

```
Message = 5×3
     12    24    13
      0    12     4
      8    18    17
      8    19     7
     21     8    10
```

```
theKey=0;
for i=1:(n^2)
key=input('Enter the key: ')
theKey=[theKey key]
end
```

```
key = 3
theKey = 1×2
     0     3
```

```
key = 20
theKey = 1×3
     0     3    20
```

```
key = 9
theKey = 1×4
     0     3    20     9
```

```
key = 10
theKey = 1×5
     0     3    20     9    10
```

```
key = 9
theKey = 1×6
     0     3    20     9    10     9
```

```
key = 4
theKey = 1×7
     0     3    20     9    10     9     4
```

```
key = 20
theKey = 1×8
     0     3    20     9    10     9     4    20
```

```
key = 17
theKey = 1×9
     0     3    20     9    10     9     4    20    17
```

```
key = 17
theKey = 1×10
     0     3    20     9    10     9     4    20    17    17
```

```
rrealkey=realkey+65;
Key=char(rrealkey)
```

```
Key = 'DUJKJEURR'
```

```
Actualkey=reshape(realkey,n,n)
```

```
Actualkey = 3×3
     3    10    20
    20     9    17
     9     4    17
```

```
if(det(Actualkey) ~= 0)
    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;
    Encrypted=char(encmatrix)
else
    disp('The key matrix is not invertible')
end
```

```
Encmessage = 5×3
   633   388   869
   276   124   272
   537   310   755
   467   279   602
   313   322   726

Encmessage = 5×3
     9    24    11
    16    20    12
    17    24     1
    25    19     4
     1    10    24

Encmessage = 3×5
     9    16    17    25     1
    24    20    24    19    10
    11    12     1     4    24

encmatrix = 1×15
     9    24    11    16    20    12    17    24     1    25    19     4     1    10    24

Encrypted = 'JYLQUMRYBZTEBKY'
```

```
%Decrypting the message
    j=mod(det(Actualkey),26);
    for b = 1:26
        d(b)=j*b;
        h(b)=rem(d(b),26);
    end
    % m =[3 10 20;20 9 17;9 4 17;]
    h=uint8(h);
    m=find(h==1);
    if(m ~=0)
        invk=m.*adjoint(Actualkey);
    else
        disp('Enter Another Key');
        return;
    end
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;
char(decmsg)
else
    decmsg=decmsg(1:length(Actualtext)-1);
    decmsg=uint8(decmsg);
    v=find(decmsg==91);
    decmsg(v)=65;
    char(decmsg)
end
```

```
ans = 'MYNAMEISRITHVIK'
```

Applications

- One of the prominent examples of cryptography encryption these days is end-to-end encryption in WhatsApp. This feature is included in WhatsApp through the asymmetry model or via public key methods. Here only the destined member knows about the actual message. Once after the installation of WhatsApp is finished, public keys are registered with the server and then messages are transmitted.
- The next real-time application of cryptography is digital signatures. In the situation that when two clients are necessary to sign documents for a business transaction. But when two clients never come across each other they might not believe each other. Then encryption in the digital signatures ensures enhanced authentication and security.

Conclusion: In this way linear algebra is applied in cryptography and there are various uses of cryptography as mentioned above in real life.