Unit-1

1a) Differentiate between Plain Text and Cipher Text?

Ans: Plain Text is the message or data in a legible, natural format(original text).

Cipher text refers to the encrypted or encoded form of a message or data that has been transformed from its original, readable format (plaintext) into an unreadable format using a cryptographic algorithm and a secret key

1b) Briefly explain about Steganography?

Ans: The technique of hiding message in another message or picture or audio/sound or video or any another source is known as steganography.

- Example for Steganography:

1) **Image Steganography:** Hide message in a message without disturbing the picture.
2) **Audio Steganography:** Hide message in an audio stream without effecting the actual sound
3) **Video Steganography:** Hide message in a video
4) **Invisible ink:** number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper.
5) **Pin Punctures:** Small pin punctures on selected letters are ordinarily not visible unless the paper is held up in front of a light.

1C) Explain with a neat diagram A model for security.

Ans: A Model for Network Security:

- A message is to be transferred from source to destination across some sort of internet. Both the sides must Co-operate for the exchange of the data.
- A logical information channel is established by defining a route through the internet from source to destination.
- All the techniques for providing security have two components.

1. A security related transformation on the information to be sent.
2. Some Secret information shared by the two principles, it is hoped, unknown to the opponent.

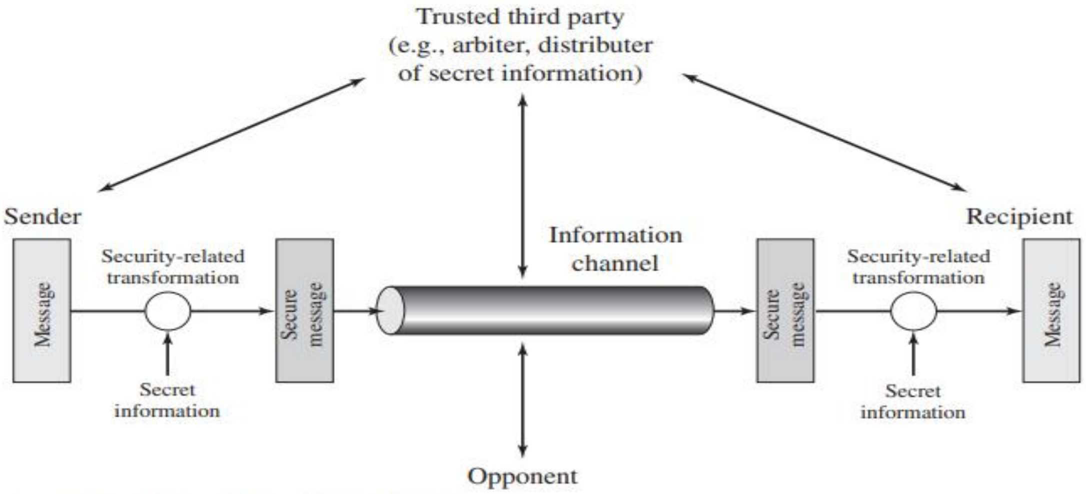


Figure 1.2 Model for Network Security

- A trusted third party is needed to achieve secure transmission.

Basic tasks in designing a particular security service:

1. Design an algorithm for performing the security related transformation.
2. Generate the secret information to be used with the algorithm.
3. Develop methods for the distribution and sharing of the secret information.
4. Specify a protocol to be used by the two principles that makes use of the Security algorithm.

- Another type of unwanted access is the placement in a computer system of logic that exploits vulnerabilities in the system & that can affect application programs as well as utility programs. Programs can present two kinds of threats.

1. **Information access threats:** Intercept or modify data on behalf of users who should not have access to that data.
2. **Service threats:** Exploit Service flows in computer to inhibit use by legitimate user

1d) Differentiate between Symmetric and Asymmetric Key Cryptography

Ans:

Symmetric Key Encryption	**Asymmetric Key Encryption**
It only requires a single key for both encryption and decryption.	It requires two keys, a public key and a private key, one to encrypt and the other to decrypt.
The size of ciphertext is the same or smaller than the original plaintext.	The size of ciphertext is the same or larger than the original plaintext.
The encryption process is very fast.	The encryption process is slow.
It is used when a large amount of data needs to be transferred.	It is used to transfer small amount of data.
It only provides confidentiality.	It provides confidentiality, authenticity, and non-repudiation.
The length of key used is 128 or 256 bits	The length of key used is 2048 or higher
In symmetric key encryption, resource utilization is low compared to asymmetric key encryption.	In asymmetric key encryption, resource utilization is high.

Symmetric Key Encryption	Asymmetric Key Encryption
It is efficient as it is used for handling large amount of data.	It is comparatively less efficient as it can handle a small amount of data.
Security is lower as only one key is used for both encryption and decryption purposes.	Security is higher as two keys are used, one for encryption and the other for decryption.
Examples: 3DES, AES, DES and RC4	Examples: Diffie-Hellman, ECC, El Gamal, DSA and RSA

2a) List the principles of security.

Ans: The following are some of the most important principles of network security:

Confidentiality: This principle ensures that only authorized individuals can access sensitive data.

Integrity: This principle ensures that data is not modified without authorization.

Availability: This principle ensures that data and systems are accessible to authorized users when they need them.

2b) How security services are related to security mechanisms?

Ans: Security services and security mechanisms are closely related. Security services are the high-level goals that security mechanisms are designed to achieve. For example, confidentiality, integrity, and availability are all security services. Security mechanisms are the specific techniques and technologies that are used to implement security services. For example, encryption, access control, and intrusion detection are all security mechanisms.

A security service can be implemented by one or more security mechanisms.

Security Service	Security Mechanisms
Confidentiality	Encryption, access control, physical security
Integrity	Message authentication, checksums, digital signatures
Availability	Fault tolerance, load balancing, redundancy

2c)What is steganography? What are the similarities and differences between steganography and cryptography? What are the relative advantages and disadvantages of steganography?

Ans: The technique of hiding message in another message or picture or audio/sound or video or any another source is known as steganography.

Steganography	**Cryptography**
Steganography means **covered writing.**	Cryptography means **secret writing.**
Steganography is less popular than Cryptography.	While cryptography is more popular than Steganography.
The attack's name in Steganography is **Steganalysis.**	In cryptography, the Attack's name is **Cryptanalysis.**
In steganography, the structure of data is not usually altered.	While in cryptography, the structure of data is altered.
Steganography supports **Confidentiality** and **Authentication** s ecurity principles.	Cryptography supports **Confidentiality** and **Authentication** s ecurity principles as well as **Data integrity** and **Non-repudiation**.
In steganography, the fact that a secret communication is taking place is hidden.	While in cryptography only a secret message is hidden.

Advantages:

- Steganography can be more difficult to detect than cryptography.
- Steganography can be used to hide messages in plain sight, which can be useful insituations where cryptography would be too obvious.
- Steganography can be used to hide multiple messages within a single covertext.

Disadvantages:

- Steganography is less secure than cryptography.
- Steganography can be more difficult to implement and use.
- Steganography can be less efficient than cryptography.

2d) Give the classification of security attacks?

Ans:Attack: Any action that compromises the security of information owned by an organization.

Security attacks are of two types:

1. Passive attacks

2. Active attacks

1. **Passive attacks:**

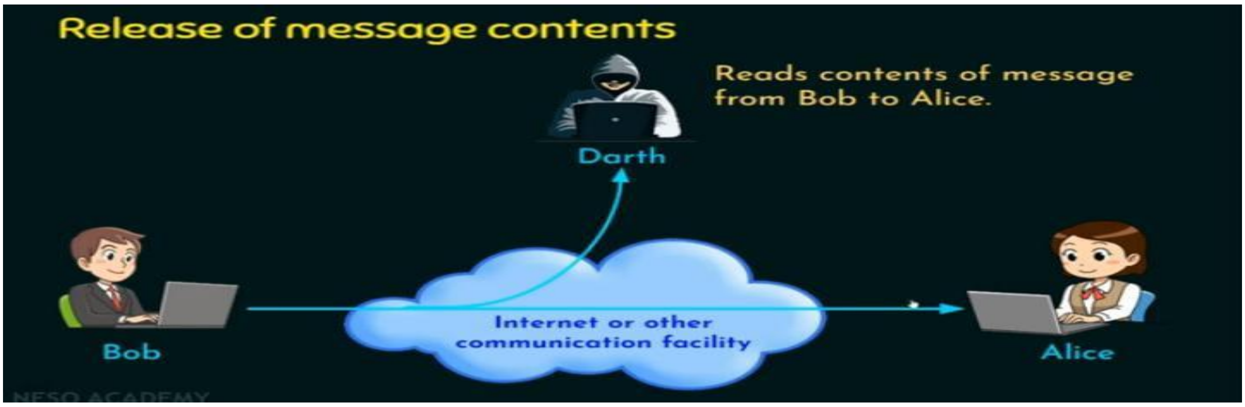
Passive are in the nature of eavesdropping on or monitoring of transmissions. The goal of the opponent is to obtain information that is being transmitted.

Two types of passive attacks are

1. Release of message contents
2. Traffic analysis

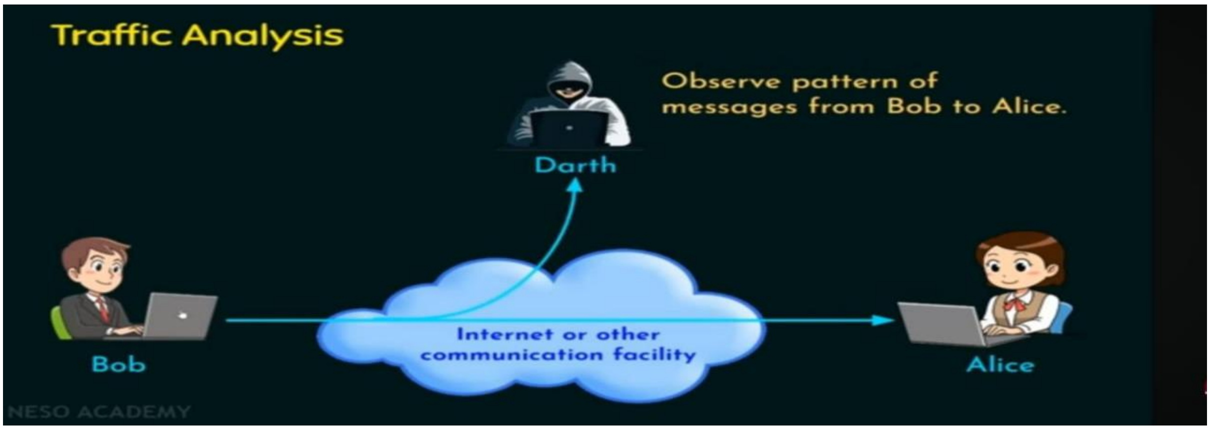
1. **Release of message contents:**

   A telephone conversation, an electronic mail message and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the content of these transmissions.


Release of message contents
Reads contents of message from Bob to Alice.
Darth
Bob
Internet or other communication facility
Alice
NESO ACADEMY

2) **Traffic analysis:**

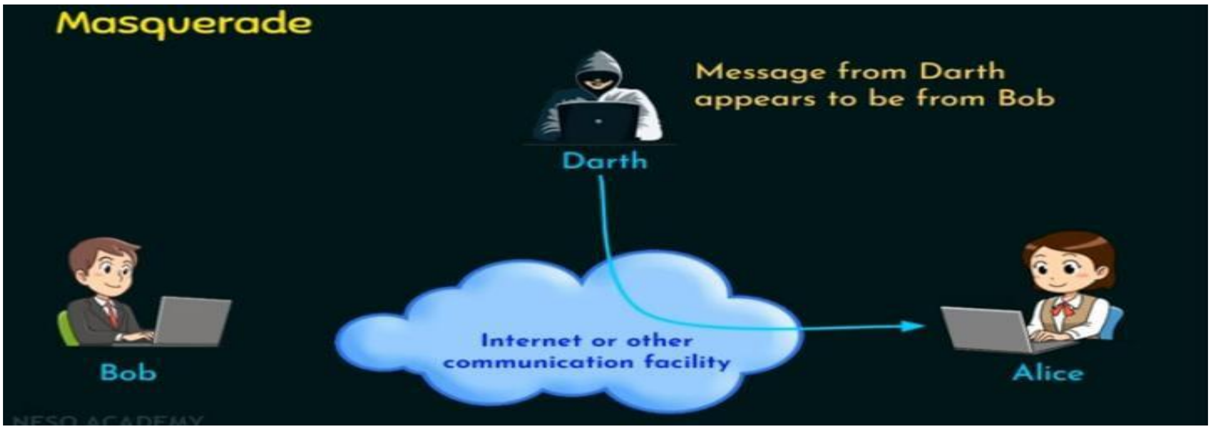
Mask the contents of message so that opponents could not extract the information from the message. Encryption is used for masking.


Traffic Analysis
Observe pattern of messages from Bob to Alice.
Darth
Bob
Internet or other communication facility
Alice
NESO ACADEMY

Active Attack: Active attacks involve some modification of the data stream or the creation of a false stream.

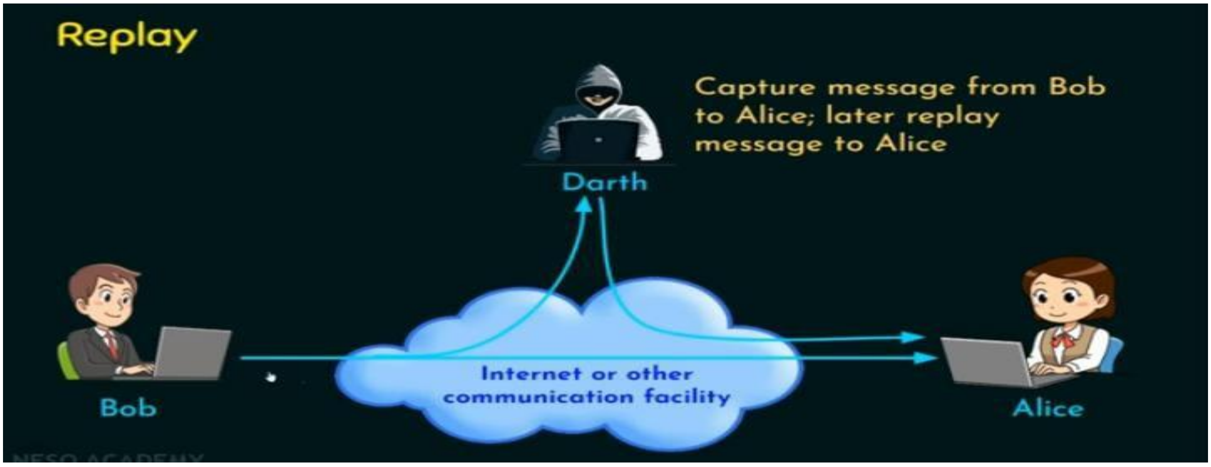
Active attacks can be sub divided into four categories.

1) **masquerade**: It takes place when one entity pretends to be a different entity

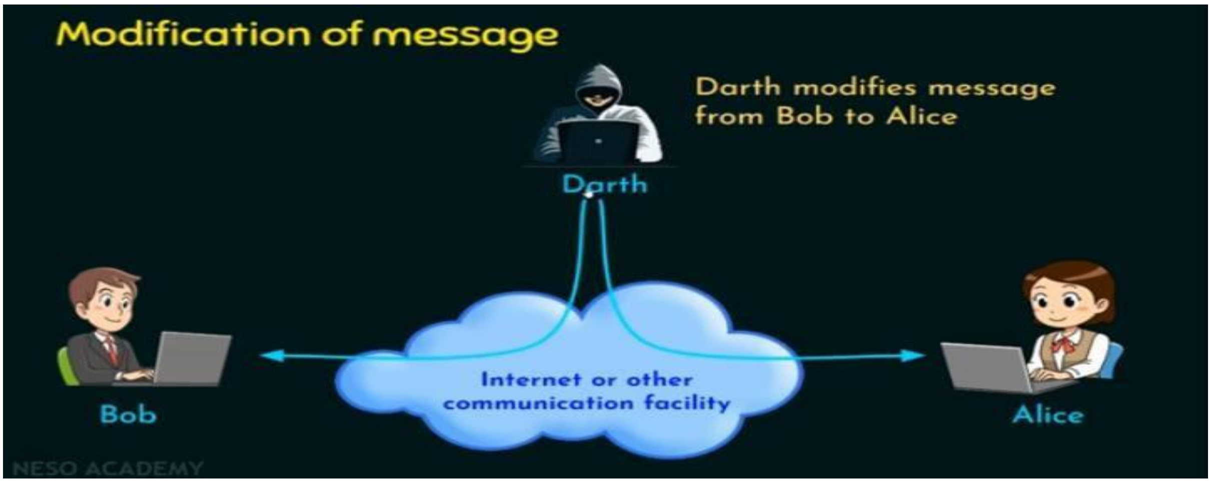


Eg: Authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.Interruption attacks are called as masquerade attacks.

2) **Replay:** It involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

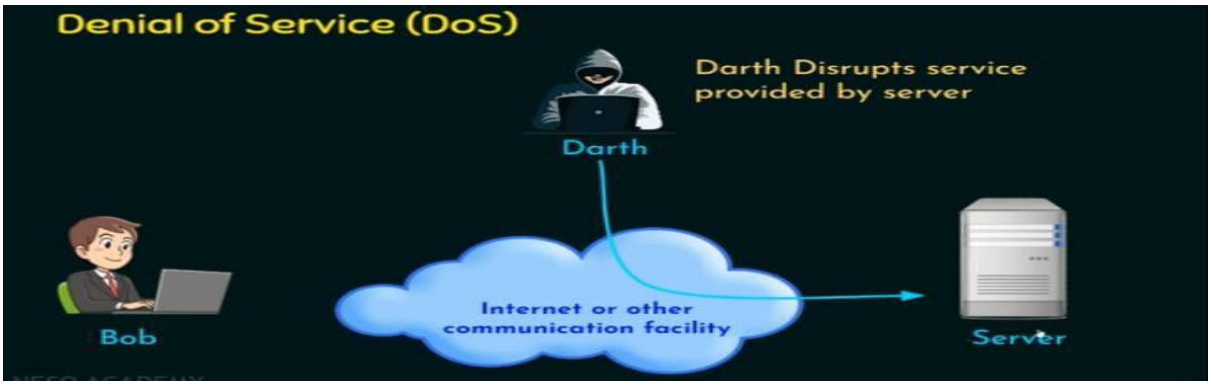


3) **Modification of message:** It involves some change to the original message. It produces an unauthorized effect.



4) Denial of service: It prevents or inhibits the normal use or management of communication facilities. Fabrication causes denial of service attacks.

- Another form of denial service is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.


Denial of Service (DoS)
Darth Disrupts service provided by server
Darth
Bob
Internet or other communication facility
Server

3a)What is Authentication ?

Ans: Authentication is the process of verifying the identity of a user, device, or process be-fore allowing access to a system or resource. It is a fundamental security measure thathelps to protect against unauthorized access, data breaches, and other cyberattacks.

3b) What is cipher text?

Ans:Cipher text refers to the encrypted or encoded form of a message or data that has been transformed from its original, readable format (plaintext) into an unreadable format using a cryptographic algorithm and a secret key. The process of convertingplaintext into ciphertext is known as encryption.

The purpose of using ciphertext is to protect the confidentiality and security of sensitive information during transmission or storage. Without knowledge of the correct decryption key, it should be computationally difficult or practically impossible for unauthorized parties to decipher the ciphertext and recover the original plaintext.

3c) List and briefly explain categories of security services and security mechanisms
Ans:

Security services:

- A Security Service is a service that provides security for data that transferring from source system to destination system.
- X.800 divides security services into different categories.

1. **Authentication:** Authentication means identifying origin of message correctly and it should ensured that identity is not false.

The authentication service is concerned with assuring that a communication is authentic. In public & private computer network, authentication is commonly done through the use of login, passwords.

- Two specific authentication services are defined in X.800
- **Peer entity authentication:** It used in association with a logical connection to provide confidence in the identity of the entities connected.
- **Data origin authentication :** It does not provide protection against the duplication or modification of data units. This type of service supports applications like electronic mail where there are no prior

Interactions between the communicating entities.

2.**Access control:** It is the ability to limit and control the access to host systems and applications via communication links. To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.

3. Data Confidentiality: It is the protection of transmitted data from passive attacks with the respect to the content of a data transmission, several levels of protection can be identified.

- The other aspect of confidentiality is the protection of traffic flow from analysis.
- This requires that an attacker not be able to observe the source & destination, frequency, length or other characteristics of the traffic on a communications facility.
- Confidentiality is classified into

i. **Connection confidentiality:** The protection of all user data on a connection
ii. **Connectionless confidentiality:** The protection of all user data in a single data block
iii. **Selective field confidentiality :** The confidentiality of selected fields within the user data on a connection or in a single data block.
iv. **Traffic flow confidentiality :** The protection of the information that might be derived from observation of traffic flows.

4.Data Integrity: message that is sent through network cannot be modifiable by other party.

- Integrity means data that is sent through the secure channel is not altered or tampered by others.
- Altering of message means message may be deleted, edited or new message may be added or delay the transmission etc.
- Integrity ensures that message received is as it is sent.
- Modification causes loss of message integrity.
- Data integrity can be classified as

  i. Connection integrity with recovery
  ii. Connection integrity without recovery
  iii. Selective field connection integrity
  iv. Connectionless integrity
  v. Selective field connectionless integrity

5.Non-repudiation: Once the transaction is completed through secure channel further sender or receiver cannot deny the transmission

- Non-repudiation prevents either sender or receiver from denying a transmitted message.
- When a message is received, the sender can prove that the alleged receiver in fact received the message.

6. **Availability:** A variety of attacks can result in the loss of or reduction in availability. X.800 treats availability as a property to be associated with various security services.

- An availability service is one that protects a system to ensure its availability.

Security Mechanisms:

- To ensure the security we have some mechanisms.

1) Specific security mechanisms: It may be incorporated into the appropriate protocol layer in order to provide some of the OSI Security services

a) **Encipherment:**

- The data will be hidden by cipher.
- The sender will convert the data into a unreadable format means sender hides the data.
- When the receiver, receives the data which is in unreadable that is converted into readable format.

b) **Digital signature:**

- Some special identity which is used for authentication.
- It is like a thumbnail and stamp.
- It is also used to Integrity of data.

c) **Access control:**

- Restricting the permissions to several levels.
- In any organization, upto what extent of permissions can be given to a particular persons.

d) **Authentication Exchange:**

- Declaring the user as an authenticated user by comparing the username and password with the data that we are having in database. Ex: login Instagram.

e) **Traffic Padding:**

- We have to add extra bits in the beginning or in the middle or in the ending in order to confuse the observer or hacker.

f) **Routing control:**

- Enabler selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspended.

g) **Notarization:**

- The use of a trusted third party to assure certain properties of a data exchange.

2.Pervasive security mechanisms: Mechanisms that are not specific to any particular OSI security service or protocol layer.

a) **Trusted functionality:**

- That which is perceived to be correct with respect to some criteria

b) **Event detection :**

- Detection of security relevant events

c) **Security label :**

- The marking bound to resource that names or designates the security attributes of that resource.

d) **Security recovery:**

- Deals with requests from mechanisms, such as event handling and management functions and takes recovery actions.

4a) What is cryptanalysis, cryptography?

Ans: cryptography :Cryptography means secret writing**, i**s the science of converting a message into a coded form that hides the information contained in the message. We encrypt a message before its transmission ,so that can eavesdropper may not get the information contained in the message.

Cryptanalysis: It is the art of deciphering an encrypted message without complete Knowledge of the key required for decryption. An attempted cryptanalysis is called a cryptanalytic attack.

4b) What are possible types of attacks?

Ans: Attack: Any action that compromises the security of information owned by an organization.

Security attacks are of two types:

1. Passive attacks
2. Active attacks

1. **Passive attacks:**

Passive are in the nature of eavesdropping on or monitoring of transmissions. The goal of the opponent is to obtain information that is being transmitted.

Active Attack: Active attacks involve some modification of the data stream or the creation of a false stream.

4 c) Elaborate any four Substitution techniques and list their merits and demerits

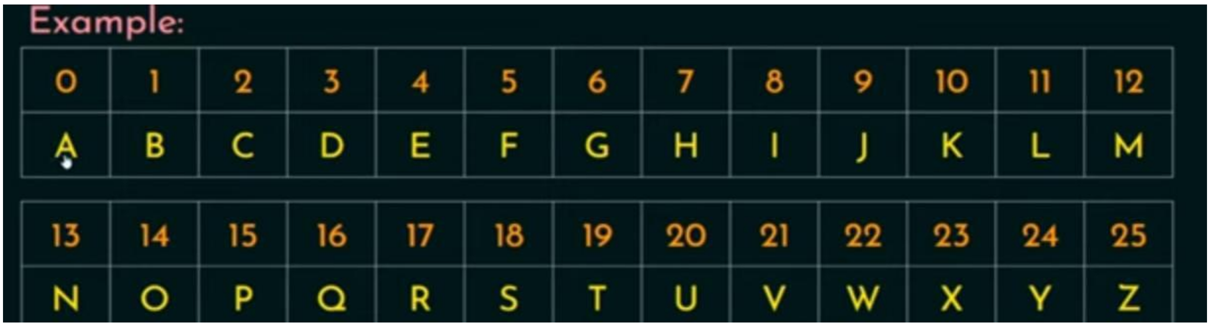
Ans: Substitution Techniques:

A Substitution Technique is one in which the letters of plain text are replaced by other letters or by number or symbols.

The Various substitution Techniques are:

1) **Caeser Cipher:**

- Letters are replaced by other letters.
- The earlier known and simplest method used be Julius Caeser.
- Replacing each letter of the alphabet with the letter standing three places further down the alphabet.



Example:

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

13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Algorithm:

For each plaintext letter ‘p’, substitute the ciphertext letter ‘C’.

C=E(p,k)mod 26= (p+k) mod 26

P=D(C,k)mod 26=(C-k) mod 26

Ex: Let key K=3

word= NEW

N=>m=12, C=(12+3) mod 26=15=>P

E=>m=4, C=(4+3) mod 26=7=>H

W=>m=22, C=(22+3) mod 26=25=>Z

- Caeser cipher is also Known as additive cipher or shift ciphers

Merits:

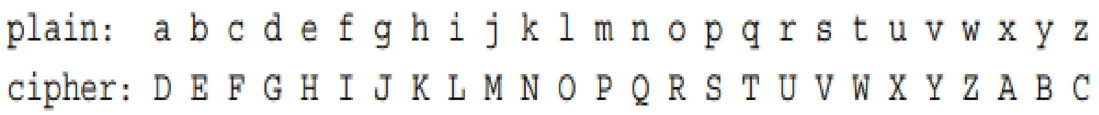
- Easy to implement and use thus, making suitable for beginners to learn about encryption.
- Requires only a small set of pre-shared information.
- Can be modified easily to create a more secure variant, such as by using a multiple shift values or keywords.

Demerits:

- It is not secure against modern decryption methods.
- Vulnerable to known-plaintext attacks, where an attacker has access to both the encrypted and unencrypted versions of the same messages.
- It is not suitable for long text encryption as it would be easy to crack.

2) Monoalphabetic substitution cipher:

- In monoalphabetic substitution, the relationship between a symbol in the plain text to a symbol in the cipher text is always one-to-one.
- After sender and receiver agreed to a single key , that key is used to encrypt each letter in the plain text or decrypt each letter in the cipher text.
- A better solution is to create a mapping between each plain text character and the corresponding cipher text character.
- **An example key for monoalphabetic substitution cipher**



plain:	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
cipher:	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

Eg: Message is machine

Plain text: machine

Cipher text:PDFKLQH

Merits:

- Better Security than Caesar Cipher.
- Provides Encryption and Decryption to data.
- Monoalphabetic Cipher maintains a frequency of letters.

Demerits:

- Monoalphabetic ciphers are easy to break because they reflect the frequency data of the original alphabet.
- Prone to guessing attack using the English letters frequency of occurrence of letters.
- The English Language is used so the nature of plain text is known.

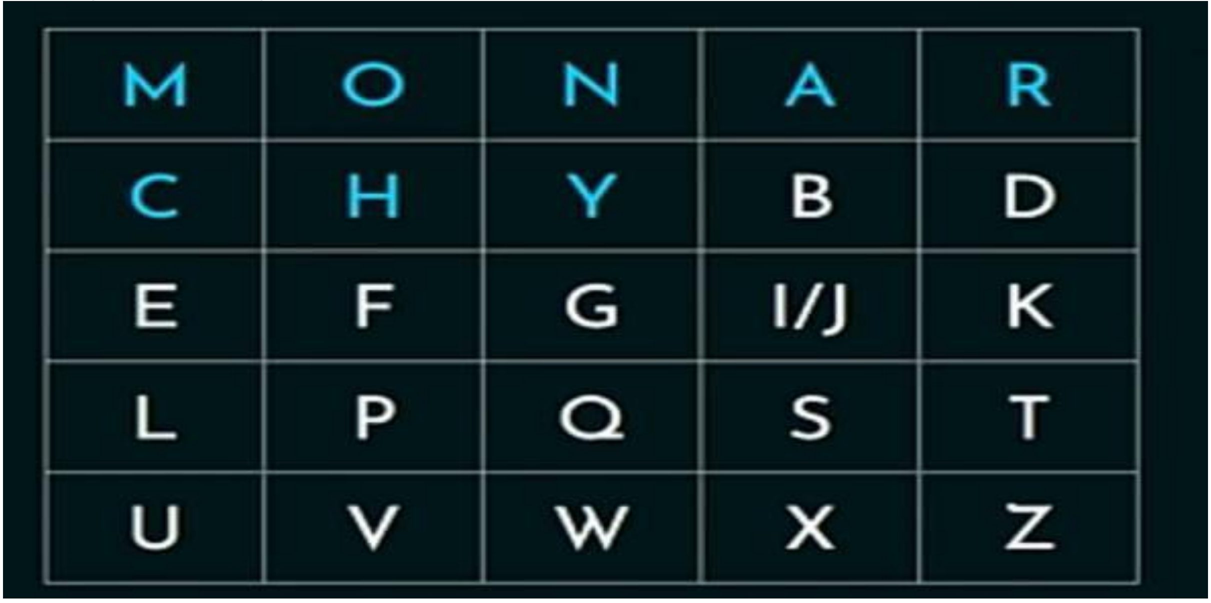
3) Playfair cipher:

- Aka Playfair square or Wheatstone-Playfair cipher.
- Manual symmetric encryption technique.
- The first literal digraphs substitution cipher.
- Invented in 1854 by Charles Wheatstone.

The Playfair Cipher Encryption Algorithm:
The Algorithm consists of 2 steps:

1) **Generate the key Square(5×5):**
The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table (as the table can hold only 25 alphabets). If the plaintext contains J, then it is replaced by I.
The initial alphabets in the key square are the unique alphabets of the key in the order in which they appear followed by the remaining letters of the alphabet in order.

Ex: key is Monarchy



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

2) Algorithm to encrypt the plain text: The plaintext is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter.

For example:

PlainText: "instruments"
After Split: 'in' 'st' 'ru' 'me' 'nt' 'sz'

i) Pair cannot be made with same letter. Break the letter in single and add a bogus letter to the previous letter.

Plain Text: “hello”
After Split: ‘he’ ‘lx’ ‘lo’

Here **‘x’** is the bogus letter.

ii) If the letter is standing alone in the process of pairing, then add an extra bogus letter with the alone letter

Plain Text: “helloe”

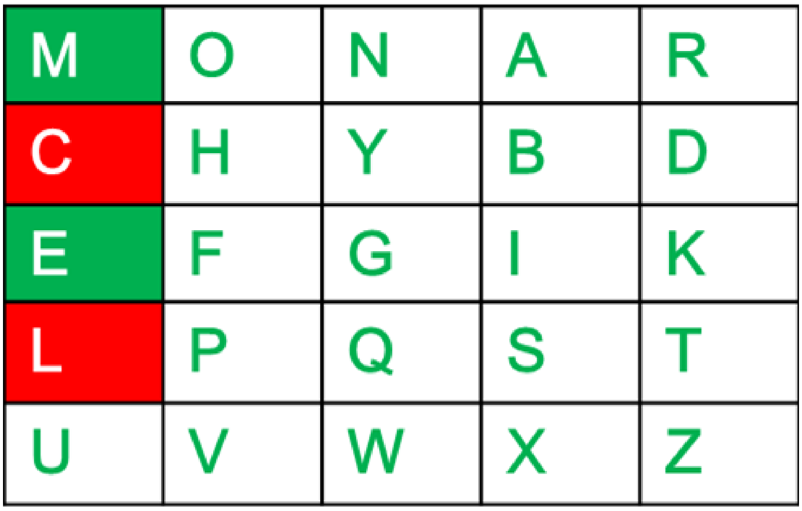
AfterSplit: ‘he’ ‘lx’ ‘lo’ ‘ez’

Here **‘z’** is the bogus letter.

Rules for Encryption:

1) If both the letters are in the same column: Take the letter below each one (going back to the top if at the bottom).

For example:



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

Diagraph: "me“

Encrypted Text: cl

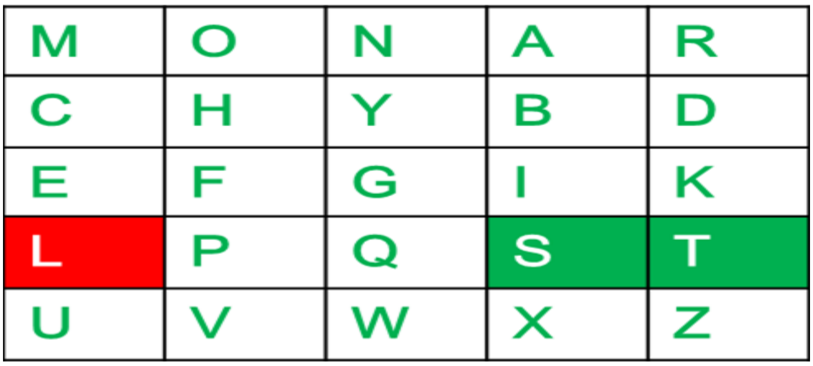
Encryption:

m -> c

e -> l

2) **If both the letters are in the same row**: Take the letter to the right of each one (going back to the leftmost if at the rightmost position).

For example:



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

Diagraph: "st"

Encrypted Text: tl

Encryption:

s -> t

t -> l

3) If neither of the above rules is true: Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

For example:

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

Diagraph: "nt"

Encrypted Text: rq

Encryption:

n -> r

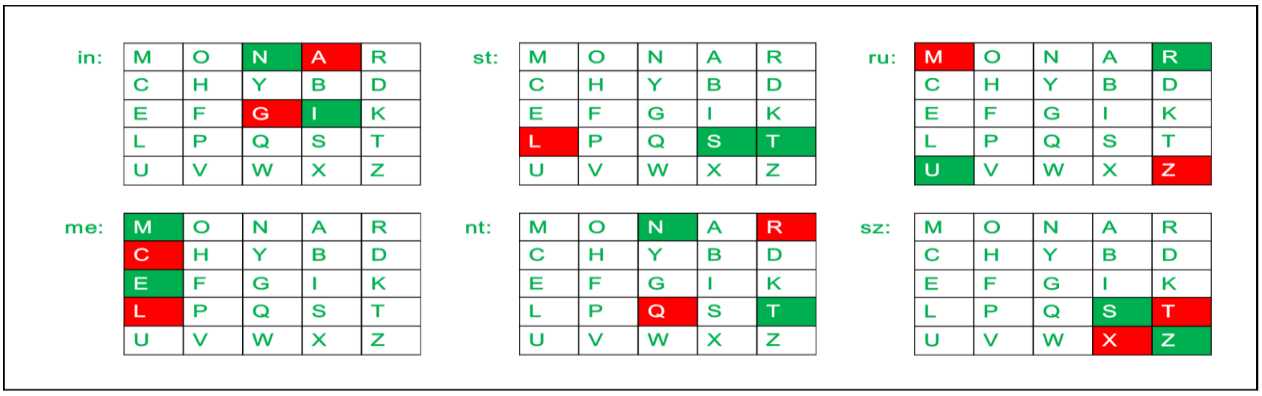
t -> q

For example:

Plain Text: "instruments“

Keyword: Monarchy

After split: in st ru me nt sz



Encrypted Text: gatlmzclrqtx

Merits:

- Diverse ciphertext if we scrutinize the Algorithm, we can notice at every Stage we are getting diverse ciphertext, thus more trouble to cryptanalyst.
- Brute force attack does not affect it.
- Cryptanalyze (the process of decoding cipher without knowing key) is not possible.
- Easy to perform the substitution.

Demerits:

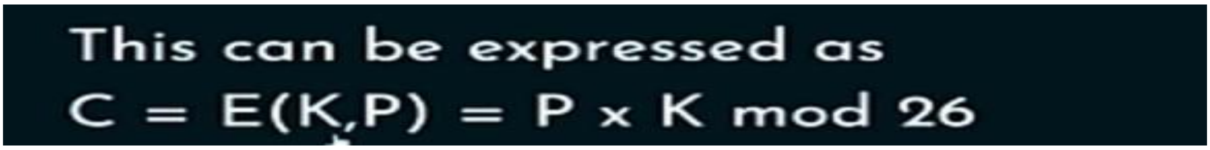
- Only 25 alphabets are supported.
- It does not support numeric characters.
- It does not support other languages, except English.
- Encryption of media files is also not supported.

4) Hill Cipher:

- The hill cipher takes a mathematical approach to Multi-letter substitution.
- A numerical value assigned to each letter of the alphabet.
- Ex: Integers 0 through 25 -→ A through Z

Hill Algorithm:

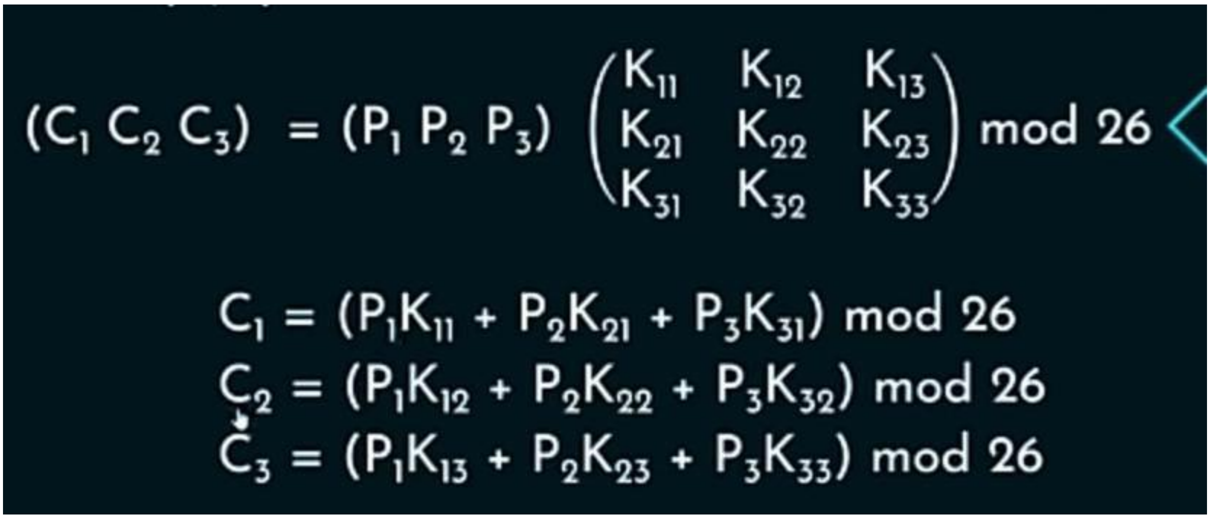
Encryption:



This can be expressed as

$C = E(K,P) = P \times K \bmod 26$

Here C:Cipher E:Encryption K:Key P:Plain text



$$(C_1\ C_2\ C_3) = (P_1\ P_2\ P_3)\begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \bmod 26$$

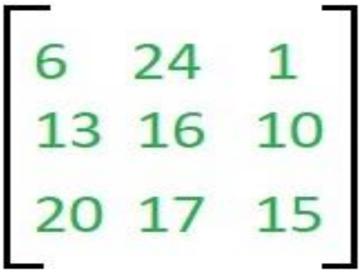
$$C_1 = (P_1K_{11} + P_2K_{21} + P_3K_{31}) \bmod 26$$
$$C_2 = (P_1K_{12} + P_2K_{22} + P_3K_{32}) \bmod 26$$
$$C_3 = (P_1K_{13} + P_2K_{23} + P_3K_{33}) \bmod 26$$

Hill Cipher example:

Plaintext: ACT

Key: GYBNQKURP

- We have to encrypt the message 'ACT' (n=3).The key is 'GYBNQKURP' which can be written as the nxn matrix:Here G-> 6 number, Y->24 number,B->1 number so…on



$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

- The message 'ACT' is written as vector:Here A->0 number,C->2 number,T->19 number

$$\begin{bmatrix}0\\2\\19\end{bmatrix}$$

The enciphered vector is given as:

$$\begin{bmatrix}6&24&1\\13&16&10\\20&17&15\end{bmatrix}\begin{bmatrix}0\\2\\19\end{bmatrix}$$

MOD 26

$$=\begin{bmatrix}67\\222\\319\end{bmatrix}$$

MOD 26

$$\equiv\begin{bmatrix}15\\14\\7\end{bmatrix}$$

- Here 15->P,14->O,7->H, so cipher text is POH

  Merits:

  - **Conceals single-letter frequencies:** The Hill cipher can hide single-letter frequencies.
  - **Tamper resistant:** The Hill cipher is resistant to tampering without being detected.
  - **High diffusion:** The Hill cipher has high diffusion**.**
  - **Useful for hiding information:** The Hill cipher can be used to hide single-letter or two-letter frequency information.

Demerits:

- **Susceptible to known-plaintext attack:** The Hill cipher is vulnerable to known-plaintext attacks due to its linear nature.

- **Key matrix may not be invertible:** The inverse of the key matrix used to encrypt plaintext may not always exist. If the key matrix is not invertible, the encrypted text cannot be decrypted.

5a) What is the need for security?

Ans: Security is the act of protecting a person, property or organization from an attack.

- Security provider privacy for your data means no other party can view your data.
- Security is required because the widespread use of data processing equipment, the security of information felt to be valuable to an organization.
- Network Security measures are needed to protect data during their transmission.

5b) Explain key size and key range

Ans: The simplest type of attack is brute force attack in which all types of substitution techniques are used to fetch original message.

- A Brute force attack works on a principle of trying every possible key from the key range. Key range is different concept from key size.
- A key range may contain individual single arbitrary quantity whereas key size defines the total or maximum capacity of all the keys.

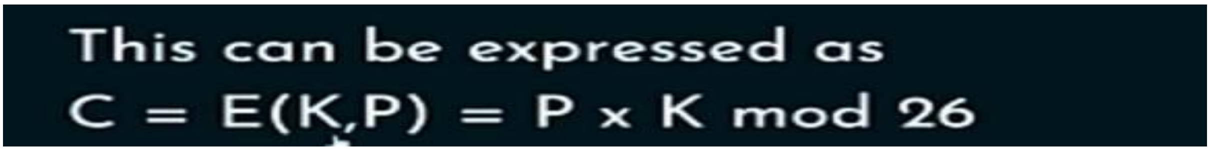
- The most commonly used key sizes are 128-bit, 192-bit, and 256-bit.
- "Key range" refers to the set of all possible keys that can be used in cryptography.
- The range is determined by the key size and the underlying algorithm, and it affects the security of the encryption.

5c) Explain hill cipher with an example.
Ans: Hill Cipher:

- The hill cipher takes a mathematical approach to Multi-letter substitution.
- A numerical value assigned to each letter of the alphabet.
- Ex: Integers 0 through 25 -→ A through Z

Hill Algorithm:

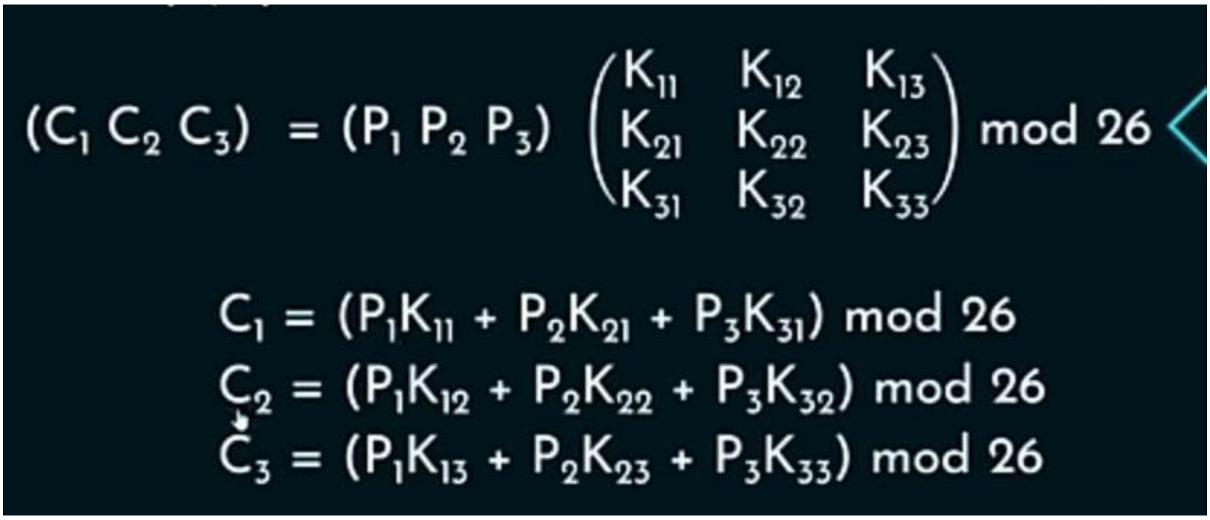
Encryption:



This can be expressed as

$$C = E(K,P) = P \times K \bmod 26$$

Here C:Cipher E:Encryption K:Key P:Plain text



$$(C_1\ C_2\ C_3) = (P_1\ P_2\ P_3)\begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \bmod 26$$

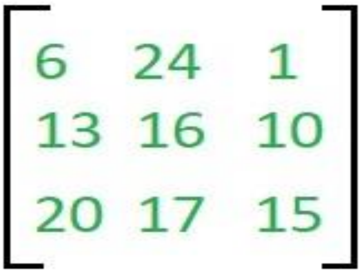
$$C_1 = (P_1K_{11} + P_2K_{21} + P_3K_{31}) \bmod 26$$
$$C_2 = (P_1K_{12} + P_2K_{22} + P_3K_{32}) \bmod 26$$
$$C_3 = (P_1K_{13} + P_2K_{23} + P_3K_{33}) \bmod 26$$

Hill Cipher example:

Plaintext: ACT

Key: GYBNQKURP

- We have to encrypt the message ‘ACT’ (n=3).The key is ‘GYBNQKURP’ which can be written as the nxn matrix:Here G-> 6 number, Y->24 number,B->1 number so…on



$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

- The message ‘ACT’ is written as vector:Here A->0 number,C->2 number,T->19 number

$$\begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

The enciphered vector is given as:

[redacted]

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix}$$

MOD 26

$$= \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix}$$

MOD 26

$$\equiv \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix}$$

- Here 15->P,14->O,7->H, so cipher text is POH

  Merits:

  - **Conceals single-letter frequencies:** The Hill cipher can hide single-letter frequencies.
  - **Tamper resistant:** The Hill cipher is resistant to tampering without being detected.
  - **High diffusion:** The Hill cipher has high diffusion**.**
  - **Useful for hiding information:** The Hill cipher can be used to hide single-letter or two-letter frequency information.

Demerits:

- **Susceptible to known-plaintext attack:** The Hill cipher is vulnerable to known-plaintext attacks due to its linear nature.

- **Key matrix may not be invertible:** The inverse of the key matrix used to encrypt plaintext may not always exist. If the key matrix is not invertible, the encrypted text cannot be decrypted.

6a)What is simple columnar technique?

Ans: Row Column Transposition(Simple columnar):

- A More Complex Scheme.
- Create Rectangle box.
- Write : Row by Row
- Read :Column by Column

Example: Encrypt the message " Guard leaves at fifteen hours"

- Plaintext: Guard leaves at fifteen hour
- Key : 5263174

5 2 6 3 1 7 4

G	U	A	R	D	L	E
A	V	E	S	A	T	F
I	F	T	E	E	N	H
O	U	R	S	X	Y	Z

Ciphertext: DAEXUVFURSESEFHZGAIOAETRLTNY

6b) Differentiate between Active attacks and Passive attacks.

Ans:

In an active attack, Modification in information takes place.	While in a passive attack, Modification in the information does not take place.

Active Attack is a danger to **Integrity** as well as **availability**.	Passive Attack is a danger to **Confidentiality**.
Due to active attacks, the execution system is always damaged.	While due to passive attack, there is no harm to the system.
In an active attack, System resources can be changed.	While in passive attack, System resources are not changing.
Active attack influences the services of the system.	While in a passive attack, information and messages in the system or network are acquired.
In an active attack, information collected through passive attacks is used during execution.	While passive attacks are performed by collecting information such as passwords, and messages by themselves.
An active attack is tough to restrict from entering systems or networks.	Passive Attack is easy to prohibit in comparison to active attack.
Can be easily detected.	Very difficult to detect.
In an active attack, the original information is modified.	In passive attack original information is Unaffected.
The duration of an active attack is short.	The duration of a passive attack is long.
Complexity is High	Complexity is low.

6c) Discuss playfair cipher with an example.

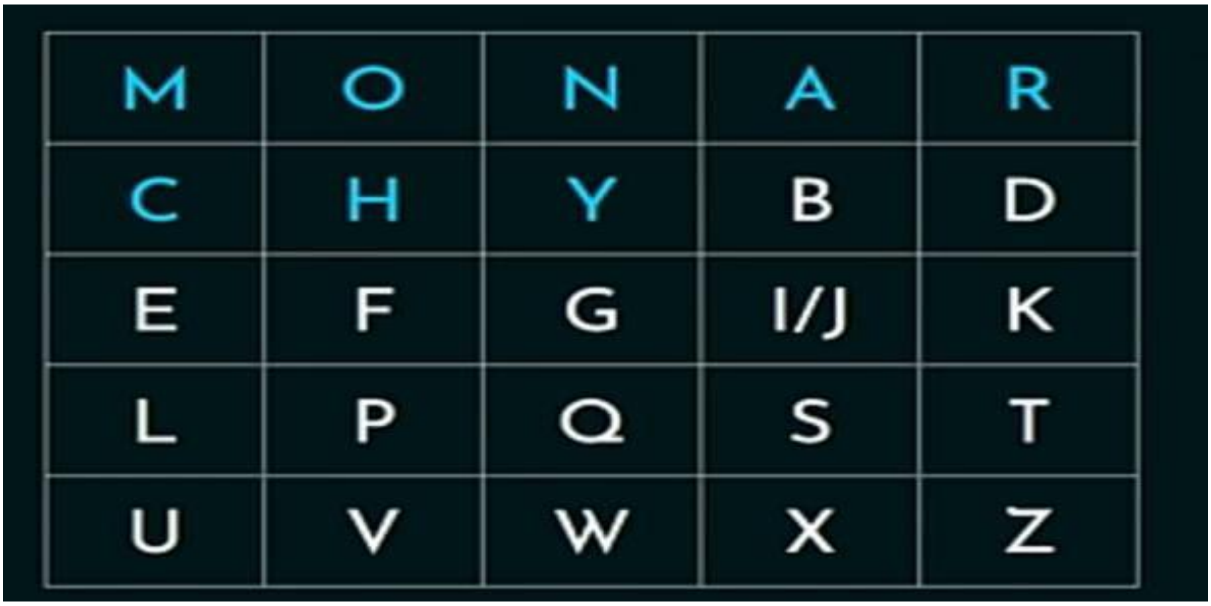
Ans: Playfair cipher:

- Aka Playfair square or Wheatstone-Playfair cipher.
- Manual symmetric encryption technique.
- The first literal digraphs substitution cipher.
- Invented in 1854 by Charles Wheatstone.

The Playfair Cipher Encryption Algorithm:
The Algorithm consists of 2 steps:

3) **Generate the key Square(5×5):**
The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table (as the table can hold only 25 alphabets). If the plaintext contains J, then it is replaced by I.
The initial alphabets in the key square are the unique alphabets of the key in the order in which they appear followed by the remaining letters of the alphabet in order.

Ex: key is Monarchy



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

2) Algorithm to encrypt the plain text: The plaintext is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter.

For example:

PlainText: "instruments"

After Split: 'in' 'st' 'ru' 'me' 'nt' 'sz'

i) Pair cannot be made with same letter. Break the letter in single and add a bogus letter to the previous letter.

Plain Text: “hello”

After Split: ‘he’ ‘lx’ ‘lo’

Here **‘x’** is the bogus letter.

ii) If the letter is standing alone in the process of pairing, then add an extra bogus letter with the alone letter

Plain Text: “helloe”

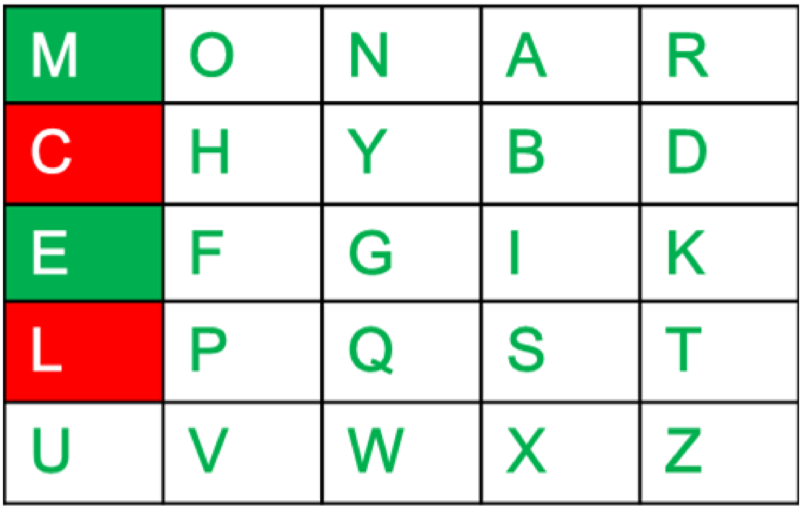
AfterSplit: ‘he’ ‘lx’ ‘lo’ ‘ez’

Here **‘z’** is the bogus letter.

Rules for Encryption:

1) If both the letters are in the same column: Take the letter below each one (going back to the top if at the bottom).

For example:



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

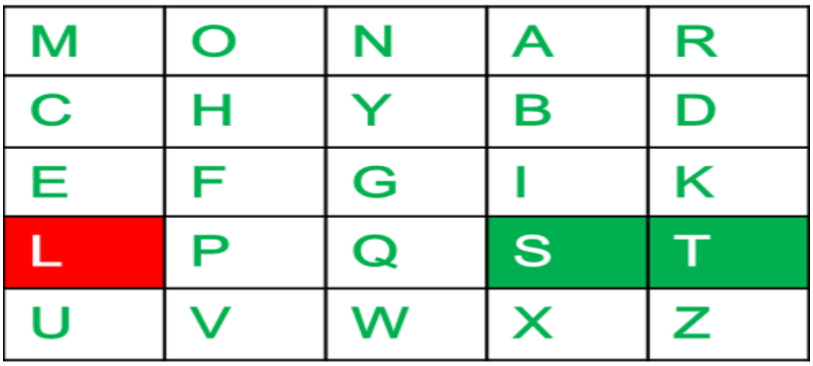
Diagraph: "me“

Encrypted Text: cl

Encryption:

m -> c
e -> l

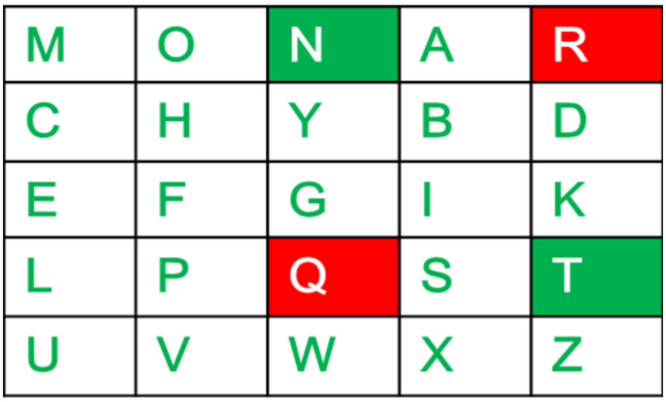
4) **If both the letters are in the same row**: Take the letter to the right of each one (going back to the leftmost if at the rightmost position).
For example:



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

Diagraph: "st"
Encrypted Text: tl
Encryption:
s -> t
t -> l

3) **If neither of the above rules is true**: Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.
For example:



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

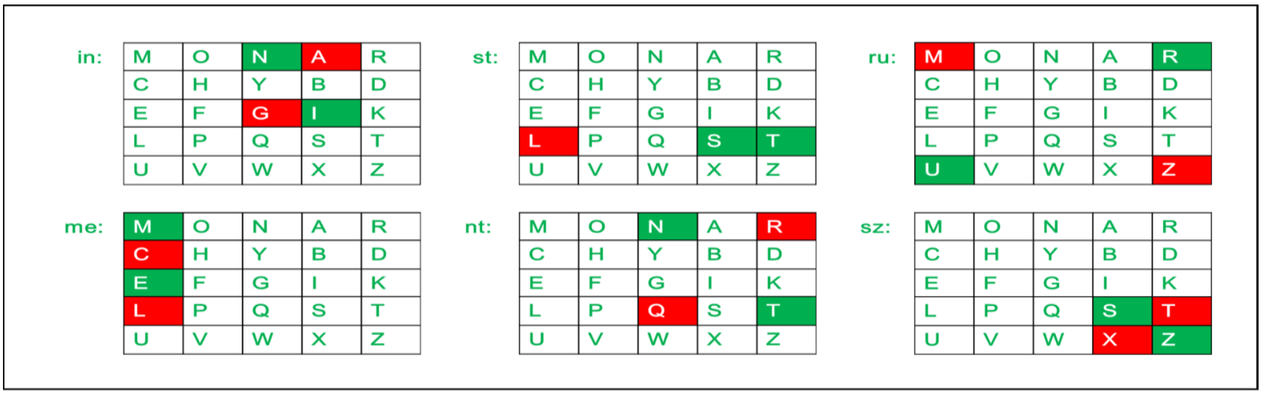
Diagraph: "nt"
Encrypted Text: rq
Encryption:
n -> r
t -> q

For example:

Plain Text: "instruments“

Keyword: Monarchy

After split: in st ru me nt sz



in:

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

st:

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

ru:

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

me:

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

nt:

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

sz:

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

Encrypted Text: gatlmzclrqtx

Merits:

- Diverse ciphertext if we scrutinize the Algorithm, we can notice at every Stage we are getting diverse ciphertext, thus more trouble to cryptanalyst.
- Brute force attack does not affect it.
- Cryptanalyze (the process of decoding cipher without knowing key) is not possible.
- Easy to perform the substitution.

Demerits:

- Only 25 alphabets are supported.
- It does not support numeric characters.
- It does not support other languages, except English.
- Encryption of media files is also not supported.