Experiment - 02

Aim - Implement Playfair Cipher Technique

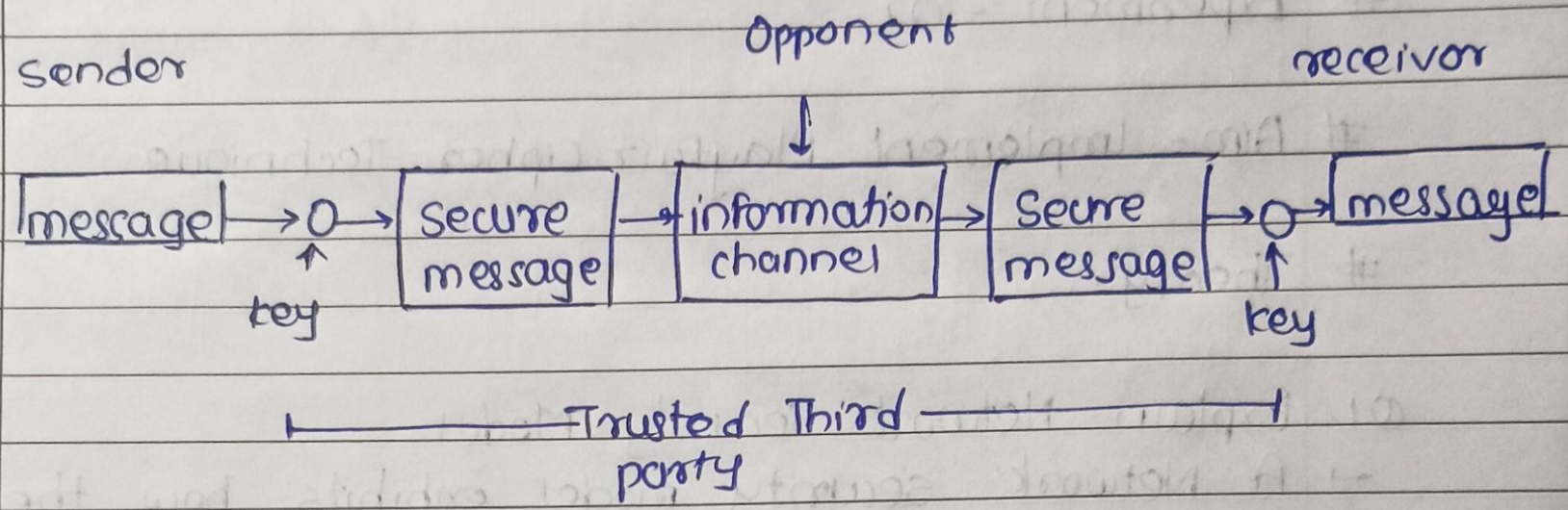
Theory -

Q1. Explain Network Security Model

→ A Network security model exhibits how the security services has been designed over the network to prevent opponent from causing a threat to the confidentiality or authenticity of the information that is being transmitted through the network.

Any security service would have 3 component below

1. Transformation - Transformation of the information which has to be sent to the receivor. So, that any opponent present at the information channel is unable to read the message. This indicates encryption of message
2. Sharing the security information betn sender and receivor of which the opponent must not have any due. ie encryption key. Which is used during the encryption of message at sender end and decryption at receivor end
3. There must be trusted third party which sould take the responsiblity of distributing the key to both communicating parties and also prevent it from opponent.



Network Security model

Q2. Explain OSI security model

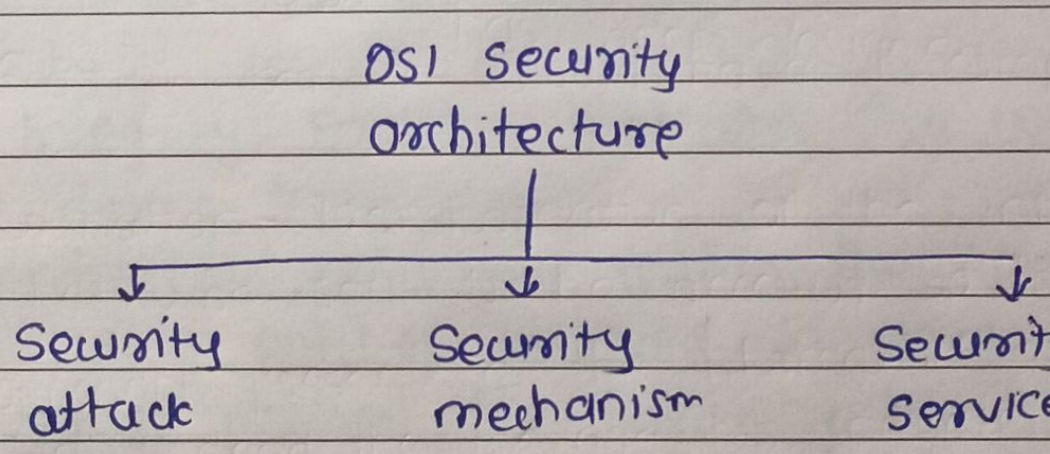
→ OSI security refers to set of protocol, standards and techniques used to ensure the security of data and communication in a network environment based on the OSI model. The ISO established this model to provide a conceptual framework for understanding how different network protocol interact with layered architectured.

OSI focus on

a Security attack

b. Security mechanism

c Security Service



• Advantages -

I. Providing Security- It provides the needed safety and security, preventing threats and risks

II. Organising task- It makes easy for manager to build model for clients which is based on strong security principles

III. Meets International Standards-

IV. Interoperablity - By dividing the network function into multiple layer, its easy for diff. hardware and software to work together.

V. Salability - The layerd method makes network scalable, which help in adding or implementing

new technologies without disturbing the system.

vi. Flexiblity - Each layer can evolve seperately providing flexiblity for technology and application changes.

Q3 Explain Security Mechanisms and Services

→ Security Mechanisms-

Security Mechanisms are methods or technologies designed to protect data and system from unauthorised access, attacks, and other threats. Some mechanisms are

a. Enciphment - This involves transforming the data into an unreadable format using algorithms

b. Access Control - This restricts unathorised user from accessing data. Methods include passwords, Firewalls and PINS

c. Notarization - Involves a trusted third party to mediate communication, reducing conflicts and ensuring authenticity

d. Data Integrity - Ensures that data has not been altered during transmission

e. Authentication Exchange - Verifies the identify of ~~protocol using~~ entities involved in communication often using protocol like two-way handshakes

f. Digital Signature - Provides a way to verify the sender's identity and ensure the message hasn't tampered

g. Bit stuffing - Add extra bit to data to ensure it can be checked for integrity at receiving end

Security Services -

Security services are the goal or objective that need to be achieved to ensure a secure enviroment They are often implemented using various security mechanism.

Key Securities Services are -

1. Confidentiality - Ensures that information is accessible

only to those authorize have access.
II. Integrity - Ensure that data is accurate and has not been tempred with
III. Authentication - Verify the identity of user and system. ~~Authentication~~
IV. Non repudiation - Ensure that sender cannot deny having sent a message
V. Access Control - Restrict unauthorized user from accessing resources.
VI Availablity - Ensure that data and resources are available to authorized users when needed.

Q4. Explain Substitution Cipher Technique with Play fair Cipher Method as an Example

→ Substitution Cipher Method-

A substitution Cipher method of encryption where each letter in the plain text is replaced with another letter. The substitution is based on fixed system, which is as simple as shifting letter by 3 number of position in alphabets

Example

Plain Text — HELLO

Shift → 3

Cipher text → KHOOR

To decrypt the cipher text we need to replace the character of CT message by alphabets 3 place backward

Playfair Method-

The playfair Cipher is more complex substitution cipher that encrypts pairs of letters.

~~Let's consider an example~~ Playfair method has 2 parts 1] key Matrix 2] Encryption

let's consider an example-

~~Plain Text — HOLIDAY~~

~~To encrypt key creat a key matrix of 5×5 and insert all the aphabets in matrix row wise~~

Plain Text - It is a sunny day

key - holiday

Now let's create the key matrix with help of key and fill all element of key in matrix rowsise and don't repeat any alphabet.

The matrix is 5x5 matrix

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

Fill the rest of box with remaining alphabets and I and J share the same block

Now Encrypting the plain text

Check the PT such that no 2 similary alphabet are together, if any introduce the element X in between them and divide the PT in pairs.

Now PT- IT IS A SUNNY DAY

Now PT- IT IS AS ON XN YD AY

Now, check each pair and check where it fit the key matrix. There are 3 possiblities

1] Either in same row, then go right by 1 element

2] Either in same column, then go down by 1 element

3] Diff row and diff column then for 1st place consider 1st alphabet row and 2nd alphabet column and for second place consider 1st alphabet column and 2nd alphabet row.

Now PT- IT IS AS ON XN YD AY

CPHER Text - DS CB CP ZF ZM EO YB

This is the playfair method to encrypt plain text.

Q5 Generate the Cipher text for the following Plain text wing Play fair Cipher method
PT→ Today it is raining heavily
key- holiday

→

Step 1 Create a key Matrix OF 5x5 and I & J share same block

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

II – Create the Pair of Plaintext and applying necessary rules.

PT- TODAY IT IS RAINING HEAVILY
New PT-
TO DA YI TI SR AI NX NG HE AV IL YX

III - With the help of key matrix and New PT generating Cipher Text

New PT- TO DA YI TI SR AI NI NG HE AV IL YX
Cipher Text - QD HE CO SD TS CH MD FK DA YU DI CV

This is the required cipher text