ASSIGNMENT NO. 1

A) Explain different servers and mechanisms of security.

→ Various security service are :

1) Data confidentiality :

It is designed to protect data from disclosure attack. The service is very broad and also accompanies confidentiality of the whole message or part of message and also the protection against traffic analyzer.

2) Data integrity :

It is designed to protect data from modification, deletion and replaying by adversory.

3) Authentication :

This service provides the authentication of the party at the other end of the line. In connection oriented communication, it provides authentication of the sender or receiver during connection establishment.

4) Non - Repudiation :

It is the service that protects against repudiation by either the sendr or the receiver of the data used to prove the identity of the sender by receiver.

5) Access control :

Provide protection against unauthorized access to data.

Security Mechanism :-

1) Enchipherment :

Hiding or concealing data can provide confidentiality. It can also be used to complement other mechanism to provide other service. Cryptography and also steganography are used.

2) Data integrity :

Appends ~~to~~ the data a short check value that has been created by a specific process from data itself.

3) Digital signature :

By this the sender can electronically sign the data and receiver can electronically verify the signal. sender uses it's private key and receiver can verify it using the sender's private key.

4> Authorization :

In this mechanism the two entities exchange some messages to prove their identity to each other.

B) What are various types of attacks?

→ **Attacks that threaten confidentiality :**

i> Snooping :

It refers to unauthorised access to or interception of data.
A confidential file being transferred on the internal may be intercepted by an attacker and confidential information can be used by him.

ii> Traffic analysis :

Although enchipherment of data make it non ineligible for the interception, he can obtain some other type of info by monitoring traffic.

Eg. Attacker can find e-mail address of the sender or the receiver. They can collect pairs of request and responses to help him in nature of transaction.

Attacks on threatening integrity :

i> Modification :

After interception, the information the attacker modifies the information to make it beneficial for them.
Eg. A customer sends a message to a bank to do some transaction. The attacker intercepts it and changes the message benefits him.

ii> Masquerading :

When the attacks impersonates eg. attacker can steal bank card and PIN of bank customer and pretend he is customer.

iii> Replaying :

Attacker contains a copy of a message sent by a user and later replays it.
Eg. A customer sends a request to his bank to Ack the payment to the attacker intercept it and sends it again to receive another payment.

A 110