Security Protocols

* What is Protocol ? and Explain different Protocol.

=> A Protocol is a set of rules and conventions that govern how data is exchanged between different entities.

Protocol define the structure and format of data packets or frames.

Protocol often include mechanisms for addressing devices or nodes within a network.

Protocol may include flow control mechanisms to manage the rate of data transmission between sender and receiver.

Protocol play a crucial role in enabling communication and Data transfer across networks.

Protocol provides standardized framework for data transmission.

=> This are the different Protocol.

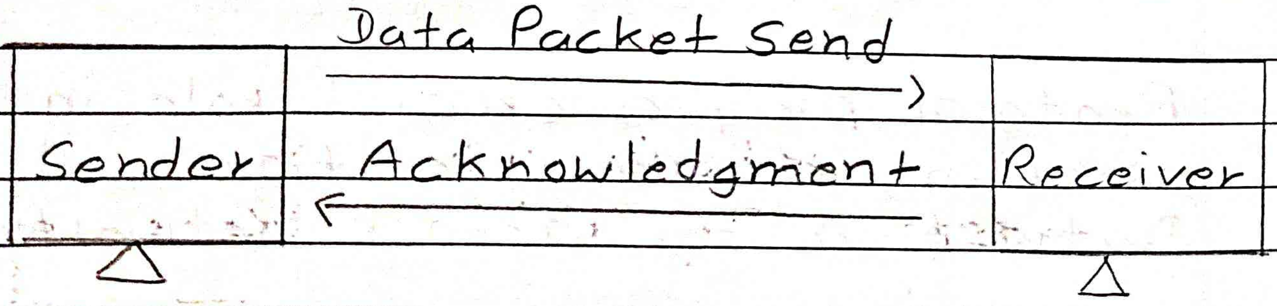
1 Transmission Control Protocol:

TCP is a fundamental protocol in computer For provides Connection-oriented communication between devices.

In TCP, Data Transmission can be done using the create connection between Sender and Receiver.

TCP ensures reliable data delivery by using acknowledgments, retransmission and error detection.

TCP uses acknowledgments to confirm the successful transfer of data packets.



2 User Datagram Protocol :

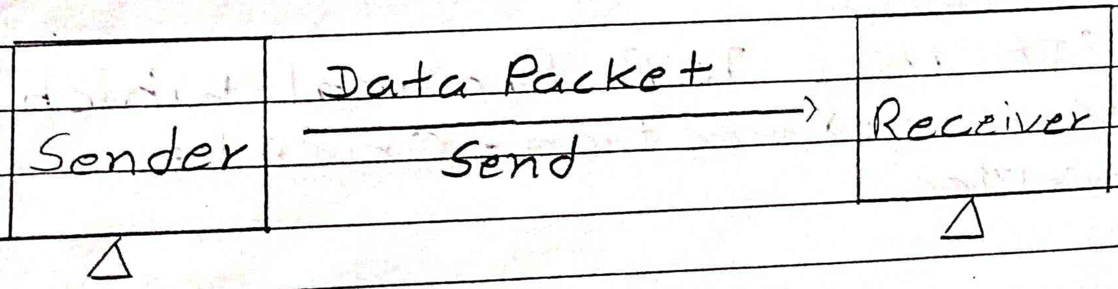
UDP is a connection-less and lightweighted transport protocol in computer network.

UDP Provides a simpler and Faster way to transmit data between two devices.

UDP does not establish a connection before the transfer data between Sender and Receiver.

Each UDP packet known as a datagram is sent independently For making connection-less protocol.

UDP does not provides acknowledgments For data transfer.



3 File Transfer Protocol:

FTP is a standard network protocol used for transferring file between a client and a server on a computer network.

FTP uses two separate channels for communication.

- Command channel
- Data Channel

Command Channel is used for sending command between client and server.

Data channel is used for transfer actual file data over a network.

FTP supports various authentications method to send the data over the network.

FTP uses TCP Protocol which is a connection-oriented service.

4 Trivial File Transfer Protocol:

TFTP is a simple, lightweighted File transfer protocol used For transferring files between devices on a network.

TFTP Operates over UDP Protocol which is a connection-less protocol.

TFTP's minimalist design makes it easy to implement and use For basic File transfer operations.

TFTP does not required authentication For transfer data in network.

5 ICMP : Internet Control Message Protocol.

ICMP is an essential protocol in computer network used for diagnostic and error reporting purposes.

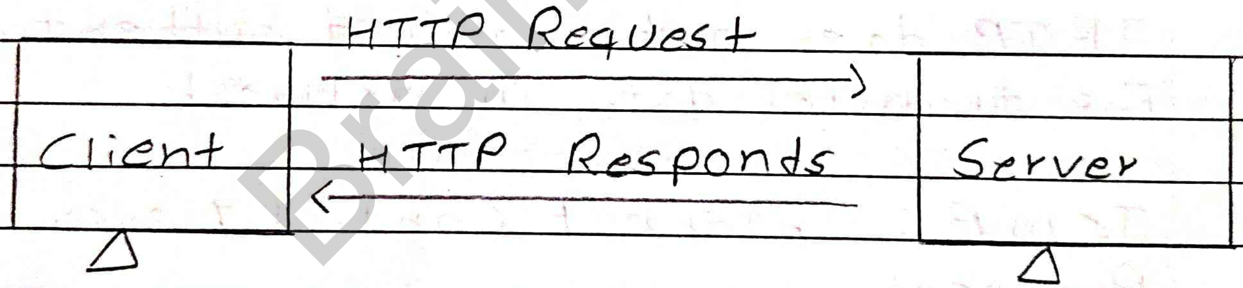
ICMP is responsible For reporting error related to packet delivery.

ICMP ~~net~~ provides essential tools for diagnosing network.

6 HTTP : Hypertext Transfer Protocol

HTTP is an application layer protocol used for transmitting hypertext document,

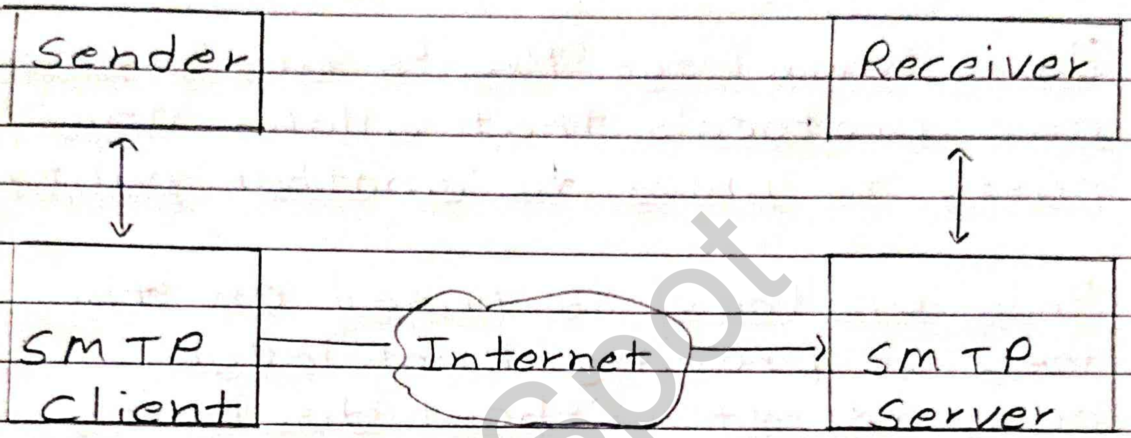
HTTP operates on a Client - Server model where a client sends requests to server and the server responds with the requested resources.



7 SMTP : Simple Mail Transfer Protocol

SMTP is a communication protocol used for transmitting email messages over the network.

SMTP is primarily responsible for sending emails from a sender's email client or server to the receiver's email server.



8 IMAP : Internet Message Access Protocol

IMAP is an email protocol used for retrieving and managing email messages stored on mail server.

IMAP allows for more advanced email management features and synchronization between multiple devices.

* Explain Zero-Knowledge Protocol.

=> Zero-Knowledge Protocol is also known as Zero-Knowledge Proof.

Zero-Knowledge Proofs are cryptographic protocols that allows one party to prove to another party.

This protocol is based on the idea of proving knowledge of a secret without disclosing the secret itself.

In this protocol, the prover aims to prove their identity of the verifier without revealing any information about their identity.

Zero-Knowledge proof protocols are special type of interactive proof system.

In this Protocol, allows one party usually called PROVER, to convince another party called VERIFIER.

Date : / /

=> Example:

Suppose Alice and Bob each have a labeled graph and they want to prove to each other their graphs are isomorphic without revealing the actual labeling or structure of their graphs.

* Explain Blind Signature.

=> A Blind Signature is a cryptographic technique that allows a User to Validate the data.

Blind Signature are Form of digital signature in which the content of the data is hidden before it is signed by any authorized person.

The signer or authorized party generates a key pair which consisting of a private key and create public key for verification

The Public Key is shared with users who wants to obtain blind signatures.

Original data is multiplying with the random blinding factor.

The blinded data is sent to the signer without reveling the original data.

The signer receives the blinded data from the requester and signer performes signature operation on the blind data using their private key and create Blind signature.

The signer sends the blinded signature back to the requester.

The requester unblinds signature using the public key.

Blind Signature can be applied to various Cryptographic protocols.

=) Application

1 Digital Cash System

2 Voting Protocols

3 Anonymous Credential Schemes