NPS - CO-3

Transport layer process to process delivery

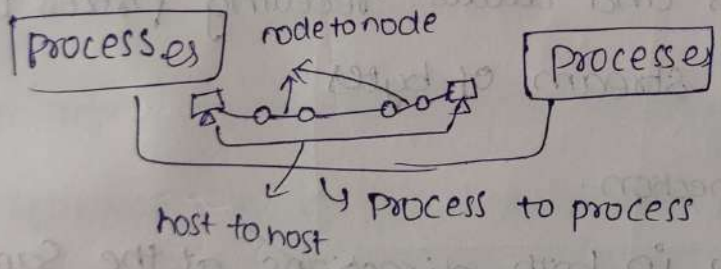
⇒ Transport layer is a 4th layer of OSI model, it provides the communication service.

⇒ Transport layer do process to process delivery

⇒ In Data link layer it helps to deliver frames b/w node to node. Therefore it is node-to-node delivery

⇒ In network layer it helps to deliver datagrams b/w two hosts. Therefore it is host-to-host delivery

⇒ Similarly, Transport layer it helps to deliver packets b/w processes, therefore it is process-to-process delivery



(Sai - slide 3)

⇒ The most common way to achieve process-to-process communication is through client/server paradigm
- → local host
- → local process
- → Remote host
- → Remote process

⇒ IP address + port number ⇒ Socket address

Transmission control protocol (TCP)

⇒ TCP is connection oriented protocol.

⇒ TCP ensures that the data reaches intended destination in the same order it was sent.

⇒ It uses flow and error control mechanism

TCP services

1) Process-to-process communication

⇒ TCP provides process to process communication using port numbers.

2) Stream Delivery service

⇒ TCP allows the sending process to deliver data as a stream of bytes and allows receiving process to obtain data as a stream of bytes

3) Full-duplex Connection:

⇒ Data can flow in both directions at the same time

4) connection-oriented service

⇒ connection is established from 2 TCPs

⇒ data will exchange in both direction

⇒ The connection is terminated

5) Reliable Services

⇒ It ensure that data sent by one computer is received correctly by another.

TCP features: (3)

1) Numbering system
2) Flow control
3) Error control
4) congestion control.

Connection establishment.

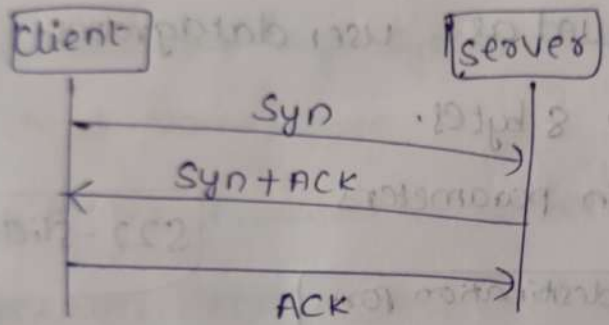
⇒ It is a full duplex mode

⇒ It is a three way hand shaking protocol.

* . flags in Tcp.

URG	ACK	PSH	RST	Syn	FIN

S32 -slide-13



S22-slide-09

⇒ Each TCP need to initialize the communication (Syn) and approval (ACK) from each end to send the data.

Header length of TCP header is min 20 bytes long & max 60bytes

0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7	0 1 2 3 4 5 6 7
Source Port		Destination Port	
Sequence number			
Acknowledge number			
data offset (4)	Reserved 6bits	Flags	window size (16 bits)
Checksum (16 bits)			urgent pointer (16bits)
options and padding			

User Datagram protocol (UDP)

* It is a connectionless protocol, unreliable protocol
* Header length is less than TCP so it is suitable for small messages.
* It is good protocol for data flowing in unidirection.
* UDP takes less time than TCP

User datagram header:

=> UDP packets are called as user datagrams.

=> Header size of length 8 bytes.

=> It contains 4 main parameters

S22-slide-07

Source Port 16 bits	destination port 16 bits
Total length 16 bits	Checksum 16 bits

=> Connectionless services

=> There is no flow control and no window mechanism

=> No error control except for the checksum.

=> To send message from process to another, the UDP protocol encapsulates and decapsulates messages in an IP datagram

=> queues are associated with ports

DNS (Domain Name System)

* It is used for mapping domain name with Ip address

Name Space:

=) It maps each address to unique name

1) Flat name:

=) name is assinged to an address in a sequence of characters without any structure.

=) No suitable for large system

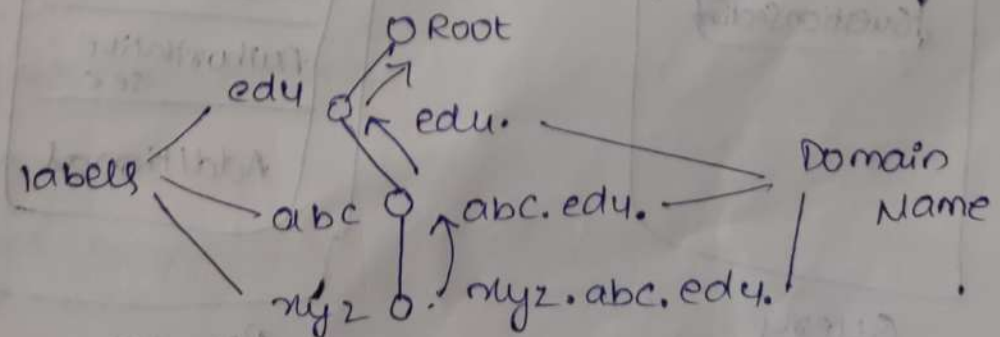
2) Hierarchical Name Space

=) Each name is made up of several parts. For example first part can define nature of the organization, the second part can define name of the organization and so on

Domain Name Space

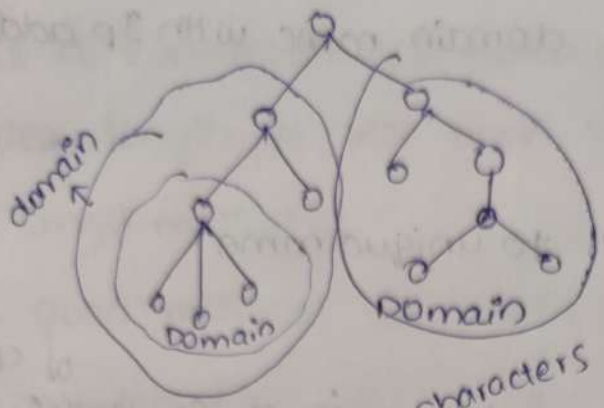
Label: Each node in the tree has a label, root label is a empty string.

Domain Name: Each node in the tree has a domain name. a full domain name is a sequence of labels separated by dots.



Domain: Subtree of domain name space

Eg:



S23-Slide 21 to 23

Resolver - (1)

Mapping Names to IP Add

Mapping IP Address to Names

Resurive resolution - (2)

Catching - (3)

These 3 are resolutions of DNS

DNS in the internet → 3 characters

3 parts → Generic Domain - eg: .edu, .org, .gov, .com

→ County domain - Eg: .us, .in

→ Inverse domain

2 characters

↳ mapping IP address with a domain name reverse process

Fully Qualified domain Name (FQDN) - xyz.abc.edu.

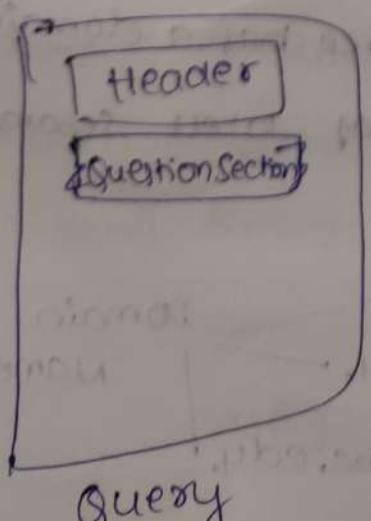
Partially " " " (PQDN) - i) xyz

2) xyz.abc

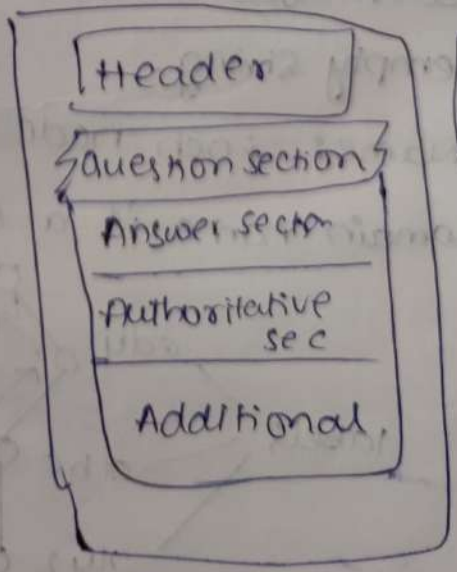
3) xyz.abc.edu

DNS messages — query

response



Query



Response

S23-slide-24

+

S23-slide-25

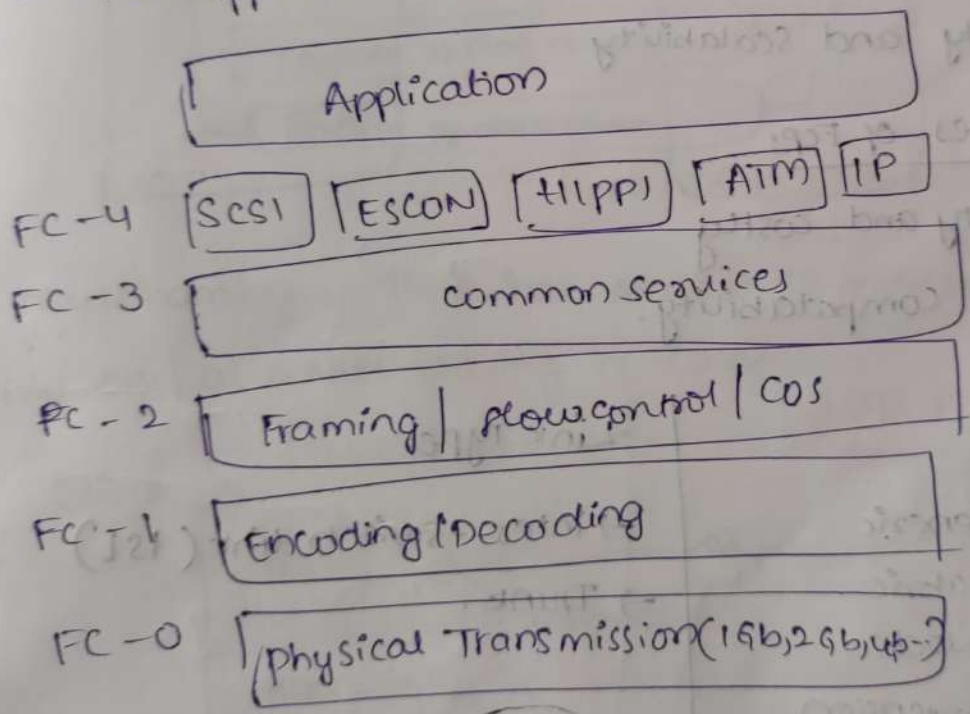
Fibre channel protocol (FCP)

=) Fibre channel is a high-speed networking technology primarily used for transmitting data among data centers.

FC layers

FC-0 - Physical media & connection
FC-1 - Transmission protocol and error control rules
FC-2 - Transport mechanism, framing and service control.
FC-3 - common services for advanced features
FC-4 - Application interfaces and protocol mapping

S24_FCP slide-06



FCP Topologies:

Direct Attached storage (DAS)
Network " " (NAS)
Storage area network (SAN)

⇒ In FCP, WorldWideNames (WWN) are used for addressing. (8)

⇒ There are 2 types in WWN
- World wide Node name
- world wide port name

⇒ FCP uses world wide node names to identify nodes in data storage Network

Advantages of FCP:

⇒ High Speed data transfer
⇒ Reliability and scalability

Disadvantages of FCP:

⇒ Complexity and costly
⇒ Limited compatability

Port types

G Port – Generic
F Port – Fabric
N port – Node.
E Port – Extension

Link Types

→ inter-switch link (ISL)
→ Trunk.

Port – It is a virtual point where the network starts and ends.

⇒ Slide – 22, 23 (S23) – DNS

Stream control Transmission protocol: (SCTP)

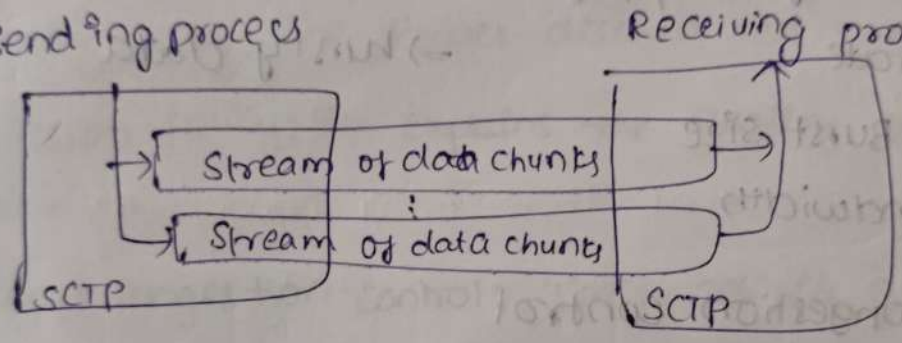
⇒ SCTP is a general purpose transport layer protocol that can handle multimedia and stream traffic

⇒ SCTP combines the features of TCP and UDP.

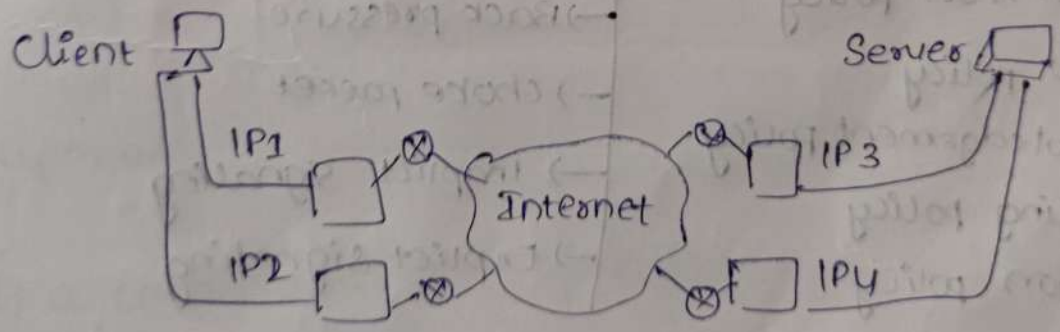
SCTP services:

S24_SCTP slide-06

1) multiple streams



2) multihoming: Host has multiple IP addresses but uses only one at a time during a connection



3) full-duplex communication
4) connection-oriented service
5) Reliable service

} check pg (2)

Header:

(16) Source port	(16) Destination port
Verification tag (32 bits)	
Checksum (32 bits)	

slide-12

Congestion control

⇒ Congestion is a network may occur if the load on the network is greater than capacity of the network

⇒ In congestion control we try avoid traffic congestion

Traffic descriptors

- ⇒ Average data rate
  - Avg = amount of data/time
- ⇒ Peak data rate
- ⇒ Maximum Burst size
- ⇒ Effective Bandwidth

Traffic profiles

- ⇒ constant-bit rate (CBR)
- ⇒ Variable bit rate (VBR)
- ⇒ bursty data

congestion control

- Open loop
  - Retransmission policy
  - Window policy
  - Acknowledgement policy
  - Discarding policy
  - Admission policy
- closed loop
  - Back pressure
  - choke packet
  - Implict signaling
  - Explict signaling

Open loop congestion control : These policies are appiled to prevent congestion before it happens. it can be handeled by source or the destination.

① ~~Retransmis~~

① Retransmission: The sender can retramist if packet is lost or corrupted

② Window policy: we have to use selective reject window method for congestion control.

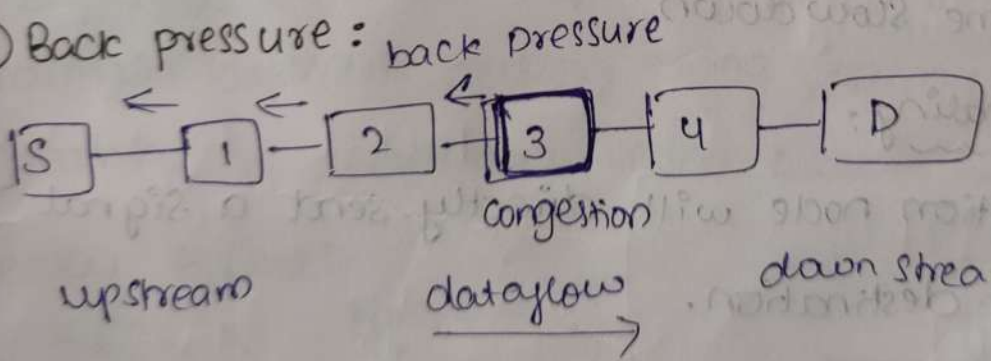
③ Acknowledgement policy: Reciever sends the acknowledgement to the sender

④ Discarding policy: The Router discard less sensitive packets

⑤ Admission policy: ~~It~~ explains ~~the~~ quality of service mechanism.

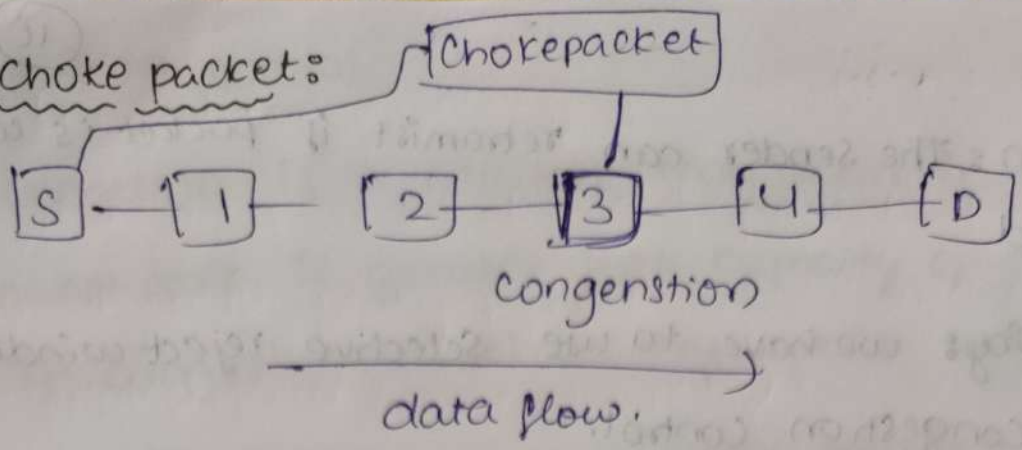
closed loop congestion control: these policies are applied to prevent congestion after it happens (try to remove)

① Back pressure:



=) If a congestion is occured at 3 node it will back pressure to the source node so from 2 - 1 - Source node it will travel then congestion will be removed

② Choke packet:



⇒ Here it will directly inform Chokepacket this choke packet will reach to source. it will not distrub the other nodes.

③ Implicit signaling:

⇒ Source guesses that there is a congestion in network when it does not recieve acknowledgement from the receiver.

⇒ Source become slow down

④ Explicit signaling:

⇒ The congestion node will directly send a signal to the source or destination.

⇒ It can be forward or backward direction

↓ (to D) ↓ (to S)

Quality of service (QoS)

⇒ It is an overall performance measure of computer network.

⇒ flow characteristics of QoS are:

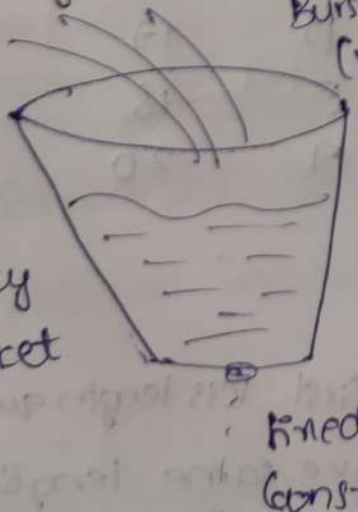
1) Reliability
2) dealy
3) jitter
4) Bandwidth

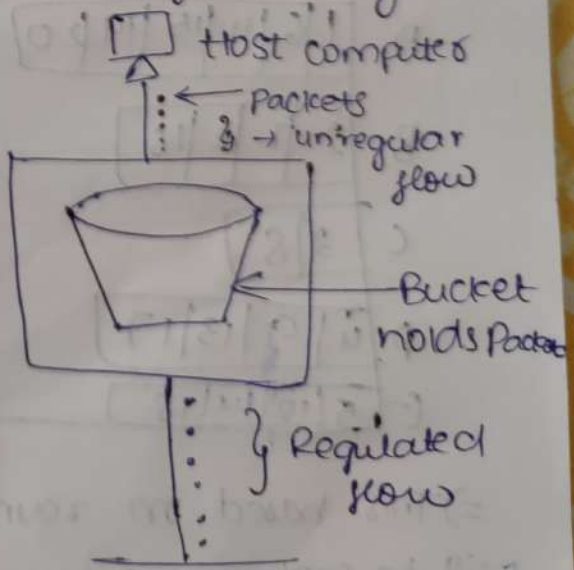
Techniques to improve QoS

⇒ overprovisioning: When you provide more capacity, buffer space and bandwidth in a network router than you really need

⇒ Buffering: It is a temporarily stores incoming data TO maintain consistent delivery timing, crucial for smooth streaming of audio and video content by reducing jitter

Leaky Bucket:





* Computer is sending packets to network

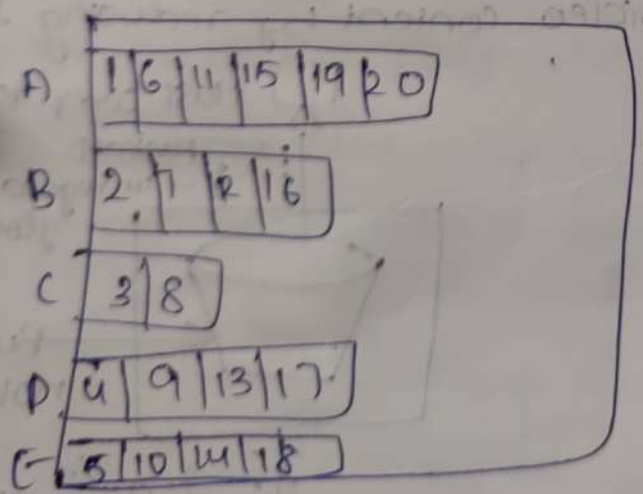
=) when host want to send packets, first it will thrown into leaky bucket those are not in a regulated flow (variable rate) but the bucket leaks at a constant rate that means it send packets in a regulated flow.

=) No matter how many packets host will send Packets will leaky one by one.

Drawback:

=) whenever the bucket filled with packets completely it will overflow and data will be lost.

Packet ~~the~~ Scheduling



Packet	finishing time
C	8
B	16
D	17
E	18
A	20

=) This based on round robin, here first less length queue will be sent, ~~next~~ i.e, C, next B, D, E have same length so ~~Ho~~ follow FCFS then Path will be B→D→E next A (5 length)

Admission control

The sender will send the data with some specifications if that specification is in the route then it will accept otherwise dismissed.

Integrated services (RSVP):

⇒ The main protocol for integrated services architecture is RSVP (Resource reservation protocol)

⇒ Flow of data needs resource such as buffer, bandwidth, CPU time etc...

⇒ QOS can be improved by reserving these resources beforehand

⇒ RSVP helps lots of people send messages to different groups without causing internet congestion.

⇒ It uses multicast routing using spanning trees.

Differentiated Services:

1) Expedited forwarding.

2) Assured forwarding.

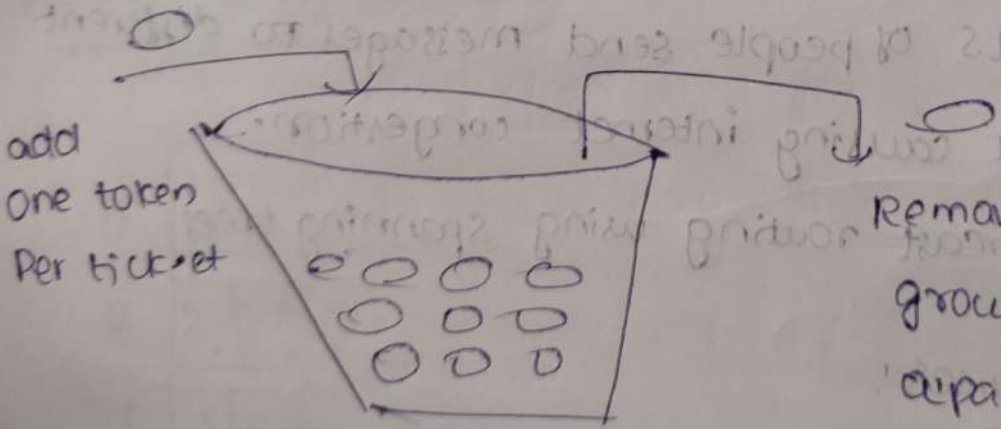
Token bucket algorithm. SEM-Slide-7 (16)

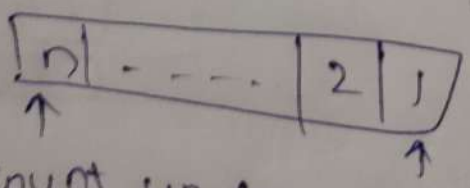
⇒ This is a congestion control algorithm.

⇒ The main aim of token bucket algorithm is data should not be lost like leaky bucket algorithm.

⇒ All tokens are grouped into one packet.

⇒ One by one tokens are placed in bucket if the token is ready then it is taken out; all tokens are grouped into one packet and send to the network. if bucket it stops accepting the token whenever there is space in the bucket, the token are released



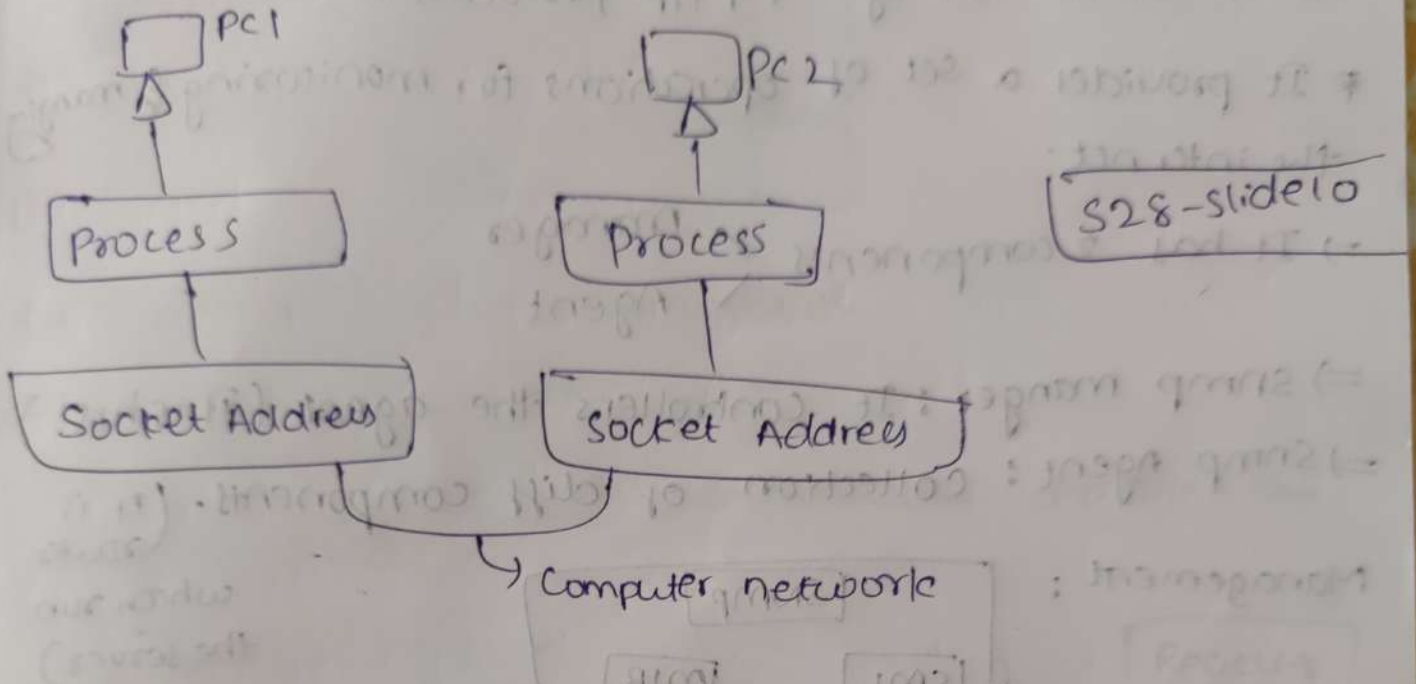


Count up for each ticket

reset

SSL - Secure Socket Layer

⇒ Sockets allow communication b/w 2 process.



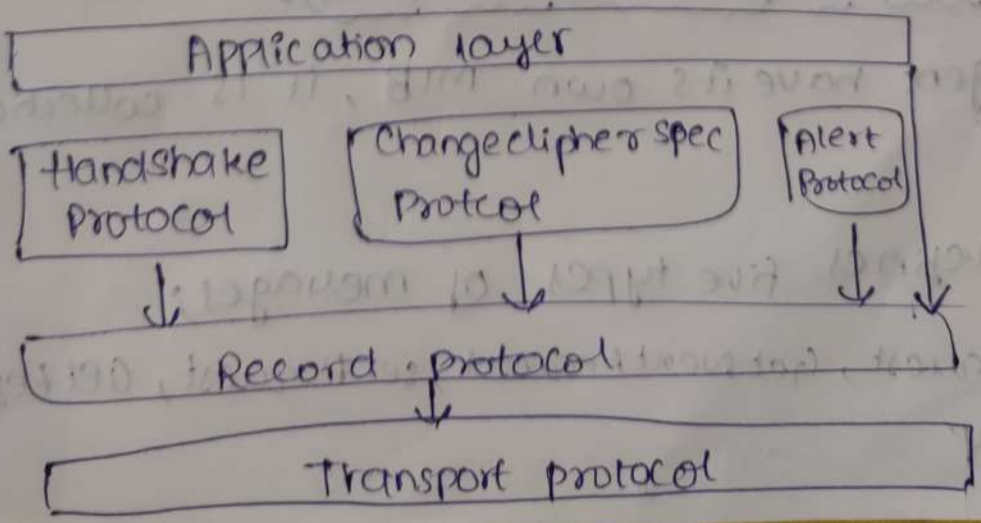
S28-slide10

⇒ For security of transport layer, there are 2 protocols

1) SSL
2) TLS (transport layer security)

→ Both are there in TCP (in b/w Transport layer & application layer)

⇒ http → NO SSL, https: → SSL



Simple Network management protocol (SNMp)

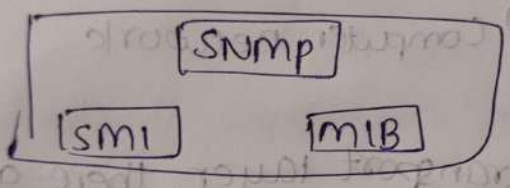
* SNMp is a framework for managing devices in an internet using TCP/IP protocols.
* It provides a set of operations for monitoring & managing the internet.

⇒ It has 2 components { manager, Agent

⇒ Snmp manger : It controllers the agent (It is host)

⇒ Snmp Agent : Collection of diff components. (It is router which run the server)

Management :



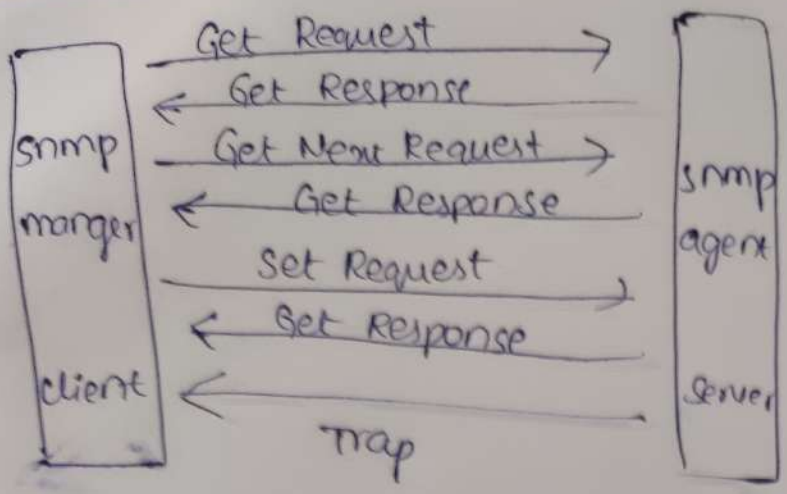
⇒ Structure Of management information (SMI) : It will define the type of data that can be stored in an object and to show how to encode the data.

⇒ Management information base (MIB):

* Each agent have its own MIB, it is collection of objects

⇒ Snmp defines five types of messages;

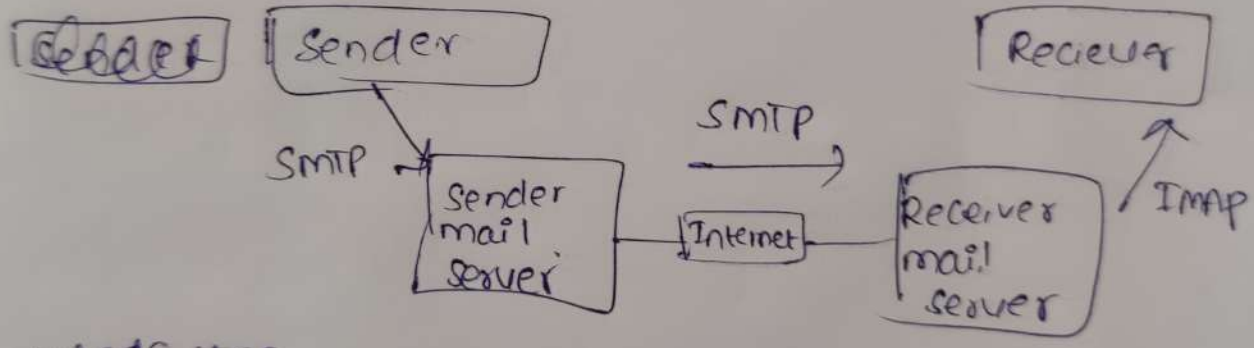
1) Get Request, Get Next Request, set Request, Get Response, and Trap



SMTP - Simple mail transfer protocol

⇒ It is used for sending email.

⇒ A set of commands that authenticates and directs the transfer of email



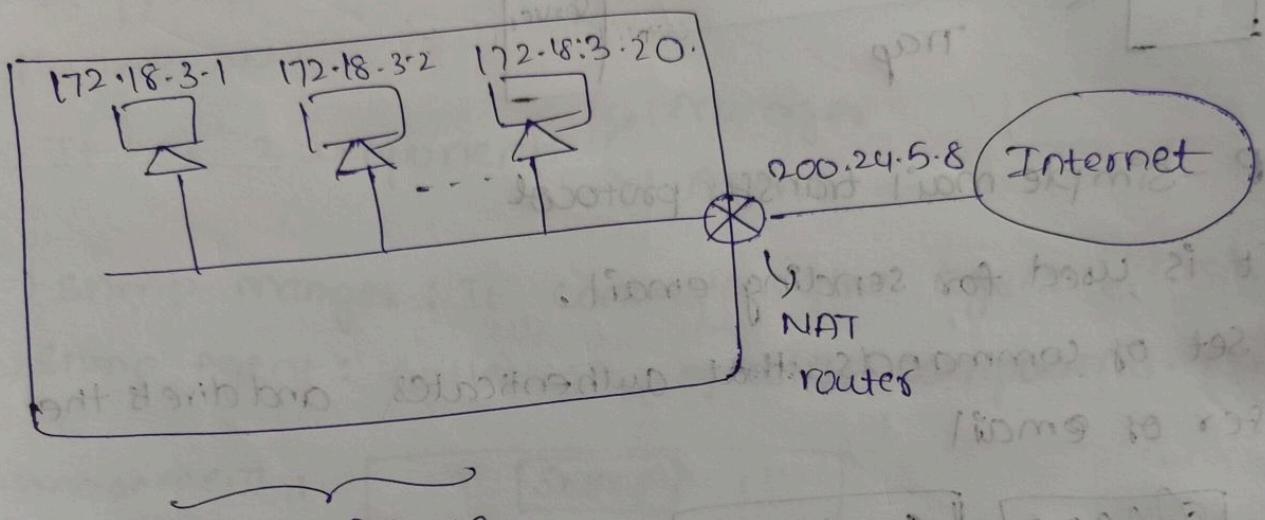
⇒ It useds TCP

S29-slide - 8, 9, 10, 11

CO-2

NAT – Network address Translation

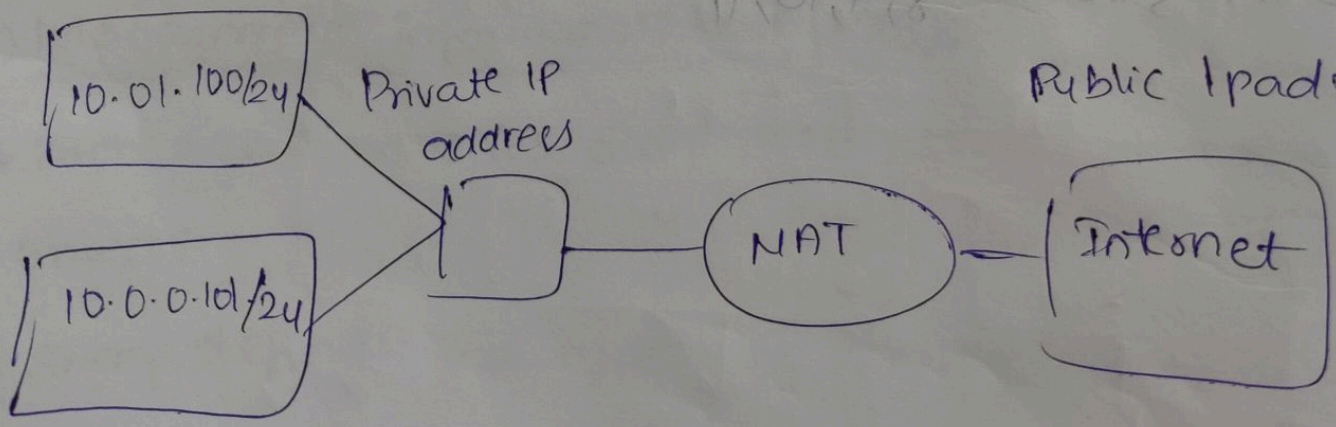
⇒ It used to mate communication with public and private networks



PAT – Port address translation

It is an extension of NAT

⇒ Translate private IP address to public IP address via Port numbers.



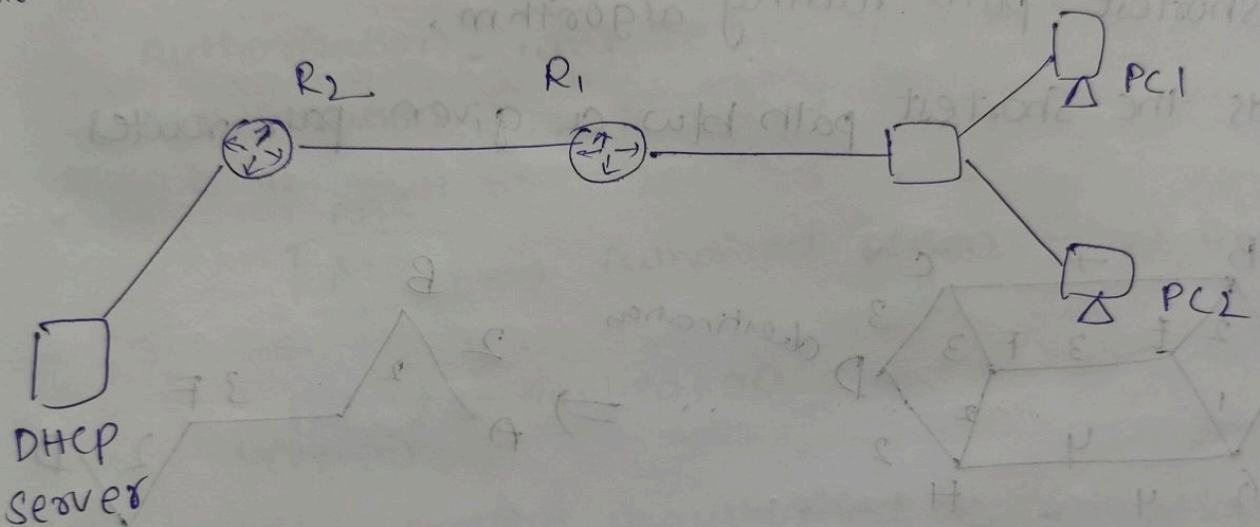
ARP- Address ~~resolution~~ protocol ✓

ARP finds the hardware address, also known as MAC address

IP address → [ARP] → MAC

DHCP-Dynamic Host configuration protocol

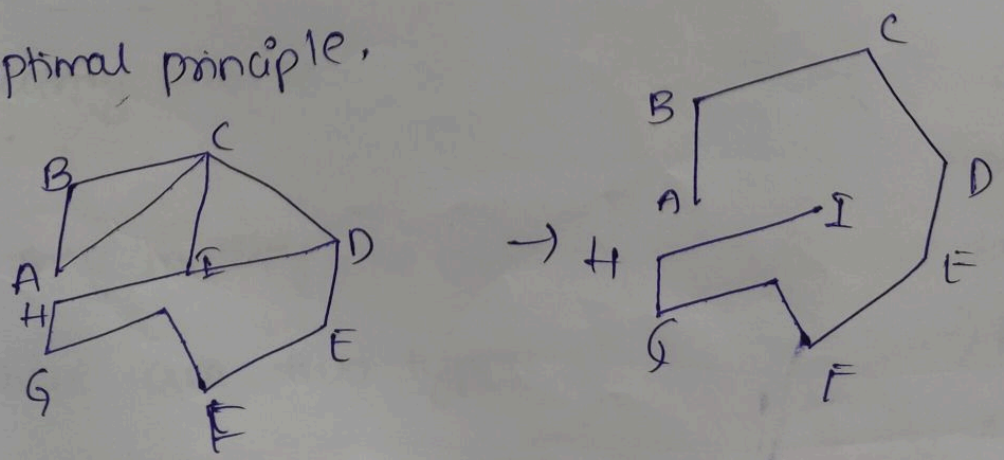
It is used to dynamicaly assign internet protocol (IP) address to each host on our network.



Routing ~~algorithms~~ protocols:

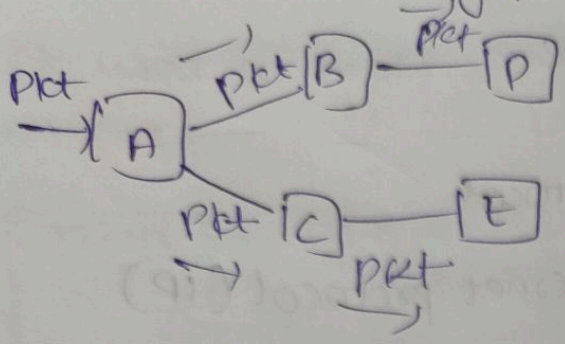
⇒ Routing algorithms
- Non-adaptive
- Adaptive

1) optimal principle.



2) Flooding

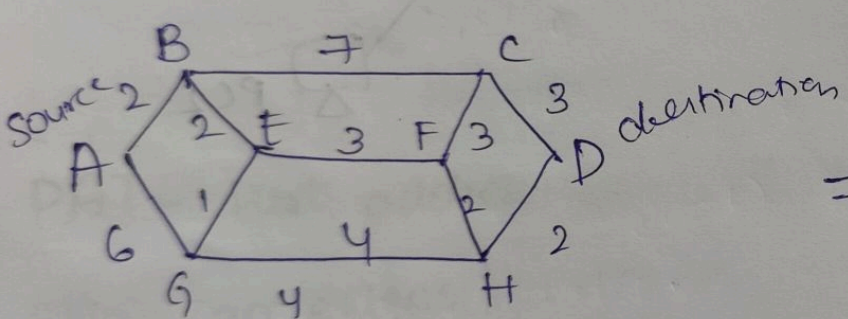
Packets are flooding from source to destination



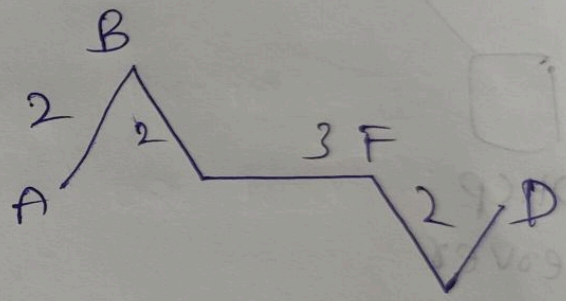
only ~~goog~~ going forward.

3) Shortest path routing algorithm.

⇒ finds the shortest path b/w a given pair routes



⇒



CO-4

Security:

⇒ security services: The processing or communication service that is provided by a system to give protection to system

1) Authentication:

Verification of user identity

Authorization - what the user want to do?

Authentication - who is doing?

ABC

ATM → Authorized person to get the service.

pin → authentication verification

2) Access control - prevent unauthorized access to resources

3) Confidentiality - providing security to the data which is send through network.

4) Integrity: No modification should be ~~doing~~ done during the ~~transmission~~ transmission

---

⇒ Security Attacks: ~~de~~. Gaining the access of data by unauthorized user

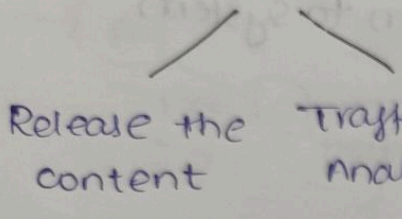
⇒ They modify the data, destroying the data etc...

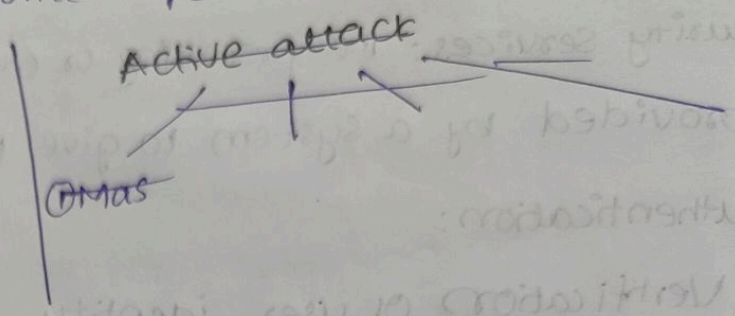
⇒ There are two types of attacks → ~~Passive~~ Passive attack
→ Active attack.

1) Passive attack: Unauthorized person cannot modify the data just they can access.

2) Active attack: Unauthorized person can modify the data

Passive attack





Active attacks:

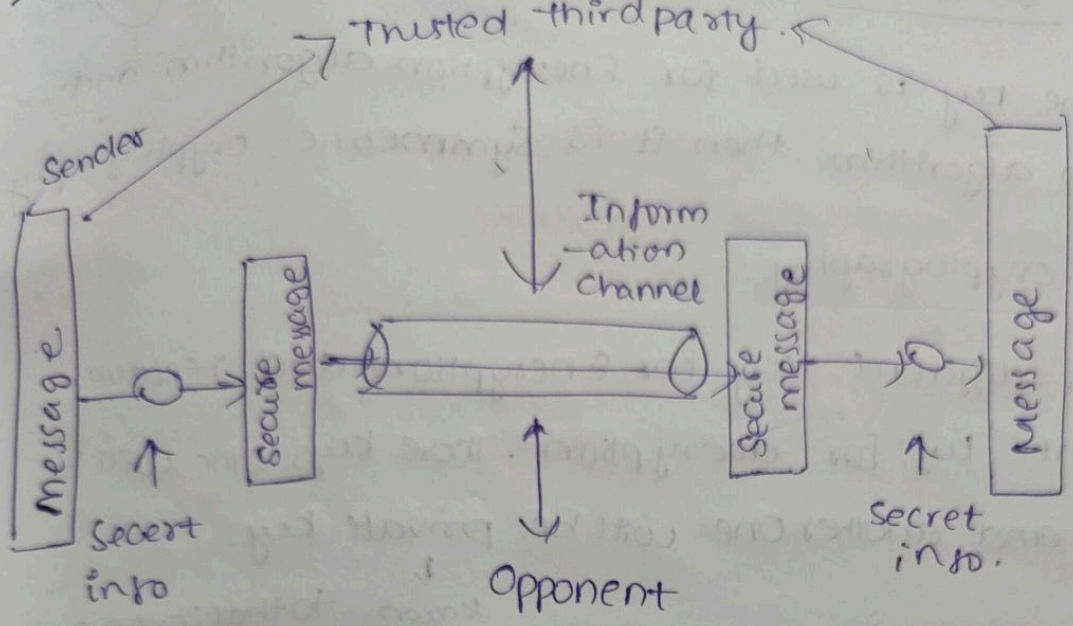
① masquerade: The sender will send the data to receiver but the receiver recieve the data from third party on the name of sender

② Replay attack: The recieuer recieve the message twice, ① is from sender (original) second one from unauthorized person modified data.

③ Data modification: Only modified data will be recevied to receiver from the authorized person.

④ Denial of service: interrupts the services send by the server to the sender.

⇒ A model for Network Security



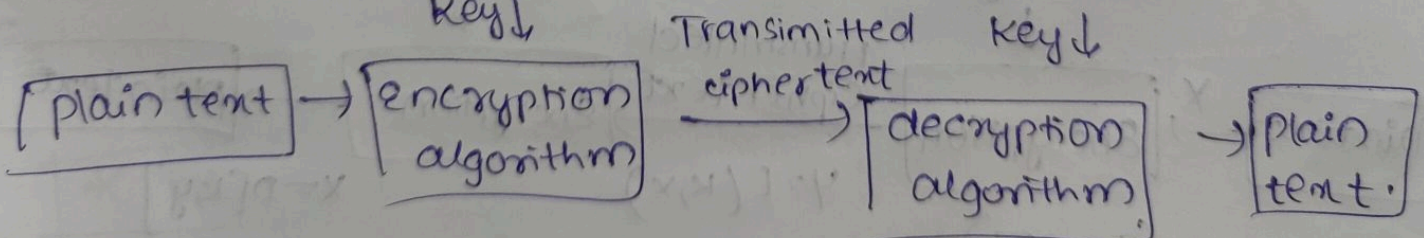
⇒ design an algorithm for security transformations

⇒ Create secret keys for the algorithm

⇒ Establish methods for sharing these secret keys

⇒ define a protocol that enables both sender and receiver

Cryptograph:



Types
- Symmetric Cryptography (Private key cryptography)
- Asymmetric Cryptography (Rublic key cryptography)

Symmetric cryptography:

⇒ If same key is used for encryption algorithm and decryption algorithm then it is symmetric cryptography

ASymmetric cryptography:

Sender uses different key for encryption and reciever use different key for decryption. Those keys one will be public key and another one will be private key

↓ known to everyone

↓ known to that person only

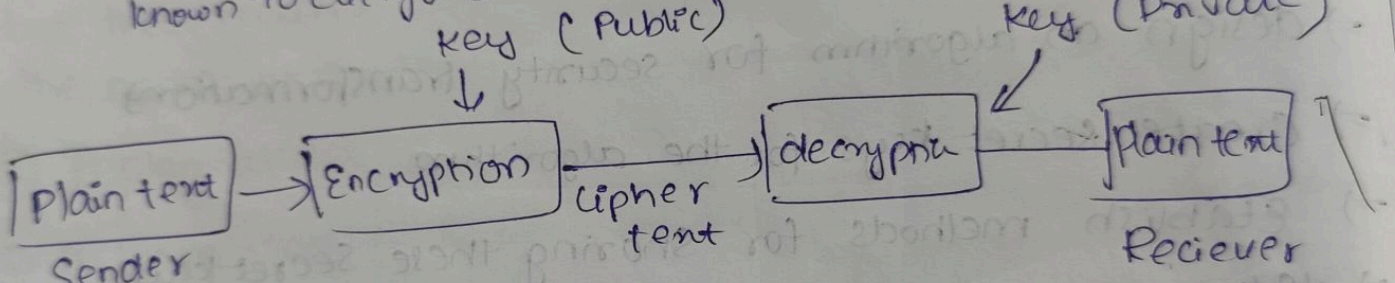
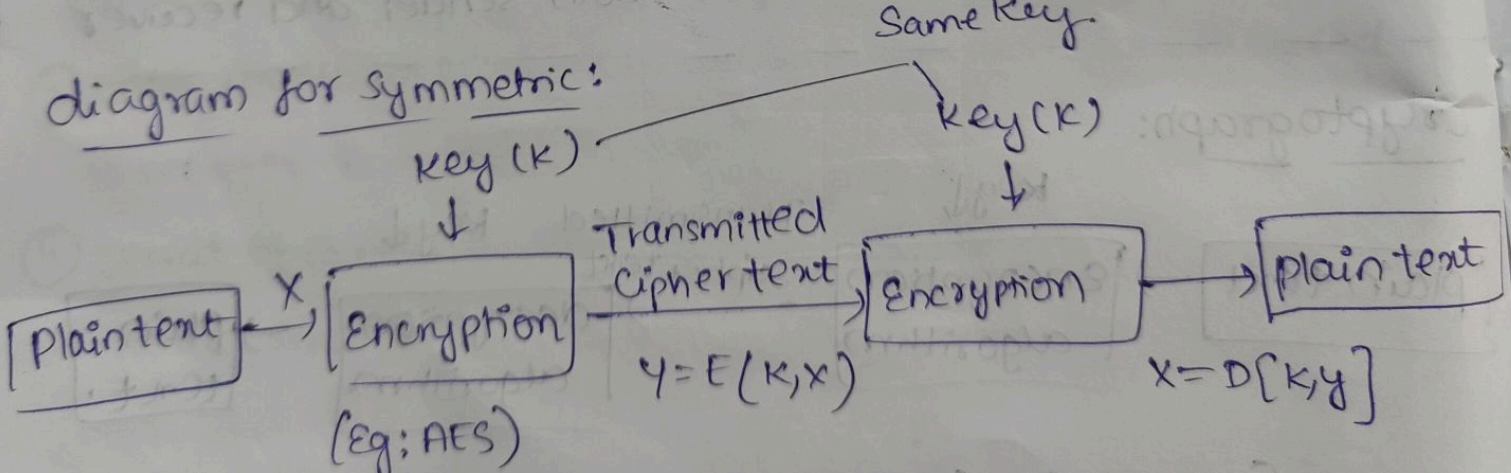


diagram for Symmetric:



Substitution techniques:

=) Substitution techniques are methods of encryption where each character in the text replace with another character based on a rule or key. There are 3 techniques/

① caesar cipher:

=) letters are replaced by other letters or symbol.

=) Replacing each letter of the alphabet with the letter standing three places further down the alphabet

0→25, A→2.

A is replaced with D.

=) For each plaintext 'p' we will replace with ciphertext letter 'c';

key

$c = E(p, k) \bmod 26 = (p+k) \bmod 26$

$p = D(k, c) = (c-k) \bmod 26.$

Eg: encrypt "KL university" with key = 6 (if not given k=3)

K	L	U	N	I	V	E	R	S	I	T	Y
Q	R	A	T	O	B	K	X	Y	O	Z	E

∴ Ciphertext: QRATOBKXYOZE

$c = (10+6) \bmod 26 = 16 \bmod 26 = Q$

$c = (11+6) \bmod 26 = 17 \bmod 26 = 17 = R$

$c = (20+6) \bmod 26 = 26 \bmod 26 = 0 = A$

→ Brute force cryptanalaysis of caesar cipher

cou - s3y - side - 6.

② monoalphabetic cipher:

cou - s3y - sid - 8,9.

③ playfair cipher

⇒ multiple letter encryption cipher

⇒ 5X5 matrix constructed using a keyword (eg: ~~MO~~ 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

ignore repeating alphabets

i/j will combine together.

Rules:

1) diagrams
2) Repeating letters - Filler letter
3) same column (↓)
4) same row (→)
5) rectangle (⇄) swap

① plain text : attack.

diagrams : at ta ck

plain text : neso academy

diagrams : ne so ac ad em y(x) + filler word

Plaintext : balloon

diagram : ba ll oo n

same repeated keep one and next filler word

diagram) : ba lx lo on

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

① plain text : attack

diagrams : at ta ck

at	ta	ck
RS	SR	DE

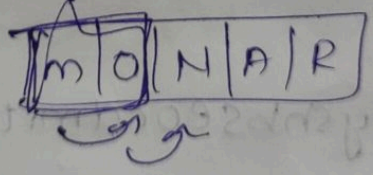
∴ RSSRDE

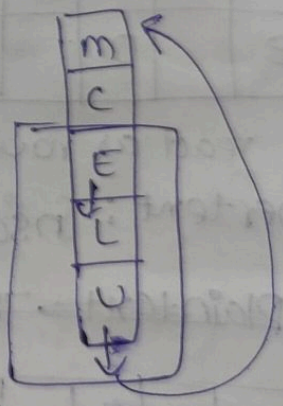
② Text : mosque

mo	sq	ue
ON	TS	ML

→ ONTSML

same row





~~Transport~~.

Transposition Techniques:

⇒ ~~It~~ It is an encryption method which is achieved by performing permutation over the plain text.

⇒ mapping plain text ~~to~~ into cipher text using this technique is called transposition cipher

① Rail fence cipher:

Q) plaintext: neso academy is the best

depth: 2

depth = no. of rows

A) ① represent in diagonal format

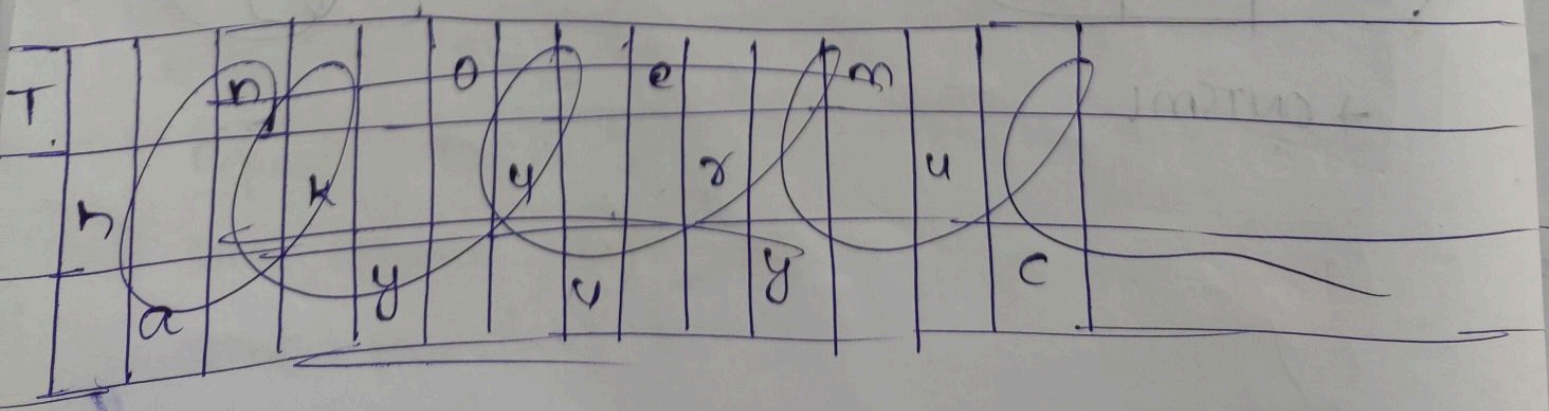
n		s		a		a		e		y		s		h		b		s	
	e		o		c		d		m		i		t		e		e		t

2 rows.

② read as row

ciphertext: nsaaeyshbseocdmiteet.

Q) ~~Plaintext: Thank you very much.~~



2) plain text: Thank you very much.

T				k				v				m		
	h		n		y		u		e		y		u		h
		a				o				r				c	

cipher text: TkVmhnyueyuhaore

② Columnar cipher

Key & plain text will be given. if not give we can give our own order of key.

Q) Apply Columnar transposition cipher method and encrypt the message "The tomato is a plant in the night shade family" using the key word "TOMATO", ~~as~~. Ignore spaces and assume padded character as 'z'. Also show the decryption process and justify how efficient the process is?

⇒ plaintext: Thetomatoisaplant in the nightshadefamily!

T O M A T O Key.

t	h	e	t	o	m
a	t	o	i	s	a
p	l	a	n	t	i
n	t	h	e	n	i
g	h	t	s	h	a
d	e	f	a	m	i
l	y	z	z	z	z
5	3	2	1th	6th	

Follow alphabet order.

Tinesaz/EoOatHfz/HtLthey/mallair/tapngdl/ostNhm2

DES Algorithm:

⇒ It is should to encrypt the data. It the best way to encrypt the data. It provide high security level

⇒ DES is a block cipher.

⇒ It give into 64 bits and convert.

⇒ we use symmetric technique that means same key for encrypt and decrypt, key size = 64 bits.

⇒ No. of rounds are 16 rounds for each round substitution and transposition.

⇒ In each round we provide a sub key i.e size of 48 bits

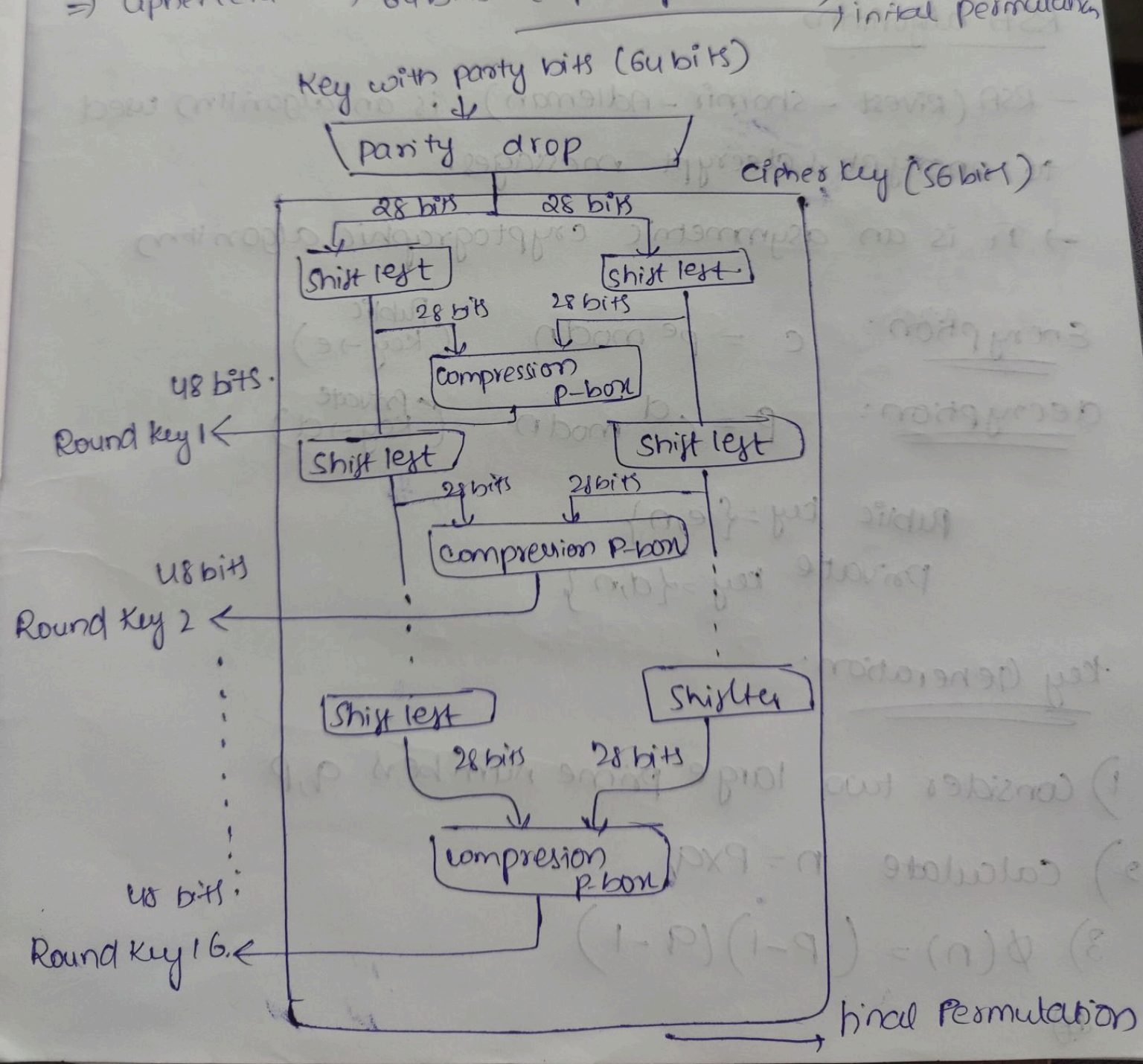
⇒ Block size (Plaintext) ---> 64 bits. (part of)

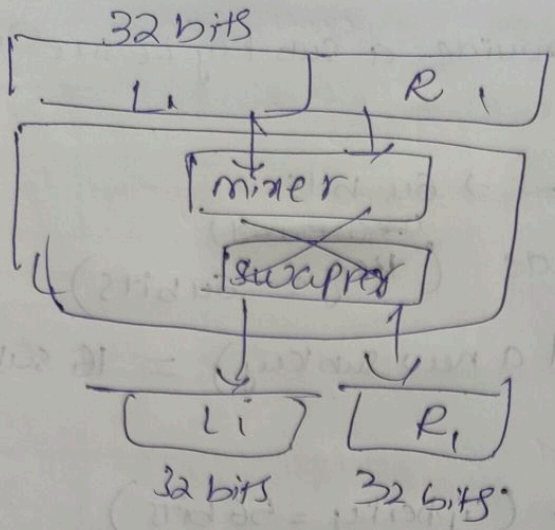
⇒ No. of rounds → 16 rounds (Key = 64 bits).

⇒ No. of subkey (each round a new subkey) = 16 subkeys

↳ size → 48 bits

⇒ ciphertext → 64 bits. (ciphertext = 56 bits)





RSA algorithm

- RSA (Rivest - Shamir - Adleman) is an algorithm used to encrypt & decrypt messages.

→ It is an asymmetric cryptographic algorithm

Encryption: $c = p^e \bmod n$ (Public key → e)

decryption: $p = c^d \bmod n$ (Private key → d)

Public key = {e, n}

Private key = {d, n}

Key Generation:

1) Consider two large prime numbers q, p
2) Calculate $n = p \times q$
3) $\phi(n) = (p-1)(q-1)$

4) choose a small number e, co-prime to $\phi(n)$ with GCD $(\phi(n), e) = 1$ and $1 < e < \phi(n)$

5) find d, such that $d \times e \bmod \phi(n) = 1$

Q) $P = 3, q = 5$

A) $n = P \times q = 3 \times 5 = 15$

$\boxed{n = 15}$

3) $\phi(n) = (P-1)(q-1) = (3-1)(5-1) = 8$

4) Assume e, such that $\gcd(e, \phi(n) = 1)$ & $1 < e < \phi(n)$

$\boxed{e = 3}$

$\gcd(3,8) = 1$
$\gcd(5,8) = 1$
$\gcd(7,8) = 1$

5) Find d.

$d \times e \bmod \phi(n) = 1$

$d \times 3 \bmod 8 = 1$

if $d = 3$

$3 \times 3 \bmod 8 = 1$

$1 = 1$

$\boxed{d = 3}$

Q) Apply RSA algorithm to encrypt and decrypt the message assuming $p=3, q=11, e=7$ and plaintext $=2$ and justify the process over symmetric key encryption.

(36)

Ans:

(1) $n = p \times q = 3 \times 11 = 33$

(2) $\phi(n) = (p-q)(q-1) = (3-1)(11-1) = 2 \times 10 = 20$

(3) $e = 7$

$d \times e \bmod \phi(n) = 1$

$d \times 7 \bmod 20 = 1$

$\therefore \boxed{d = 3}$

To encrypt $= c = p^e \bmod n$

Plaintext $= 2$

$= 2^7 \bmod 33 = 5$

To decrypt : $c = 5$

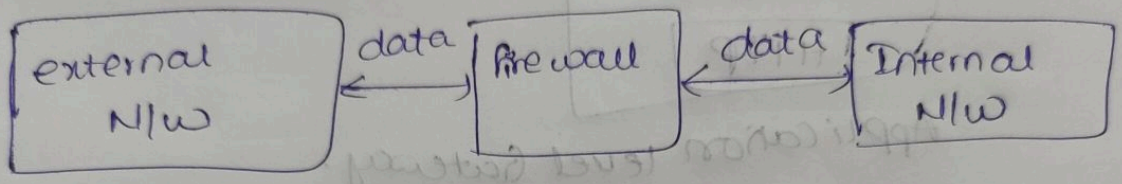
$P = 5^3 \bmod 33 = 2$

Firewalls

⇒ A network device

⇒ All the data passes through the fire wall

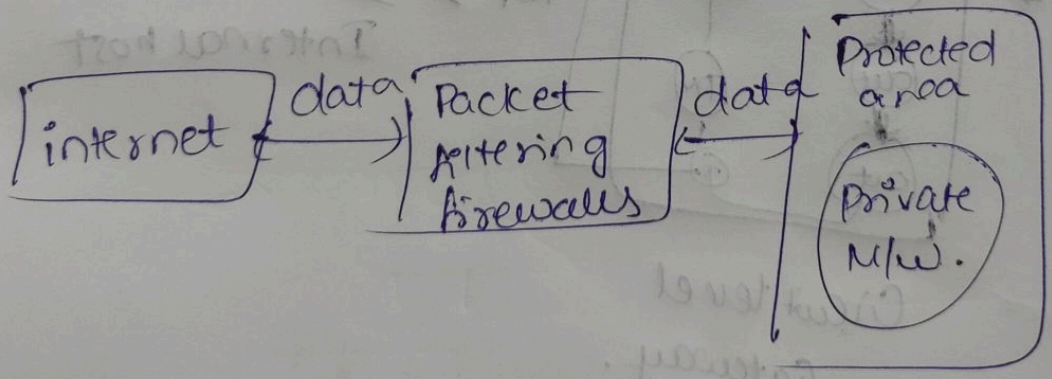
⇒ After examine the data firewall block or pass the data.



Types of ~~free~~ firewalls

1) Packet filtering firewalls
2) Application level Gateways
3) Circuit level Gateways

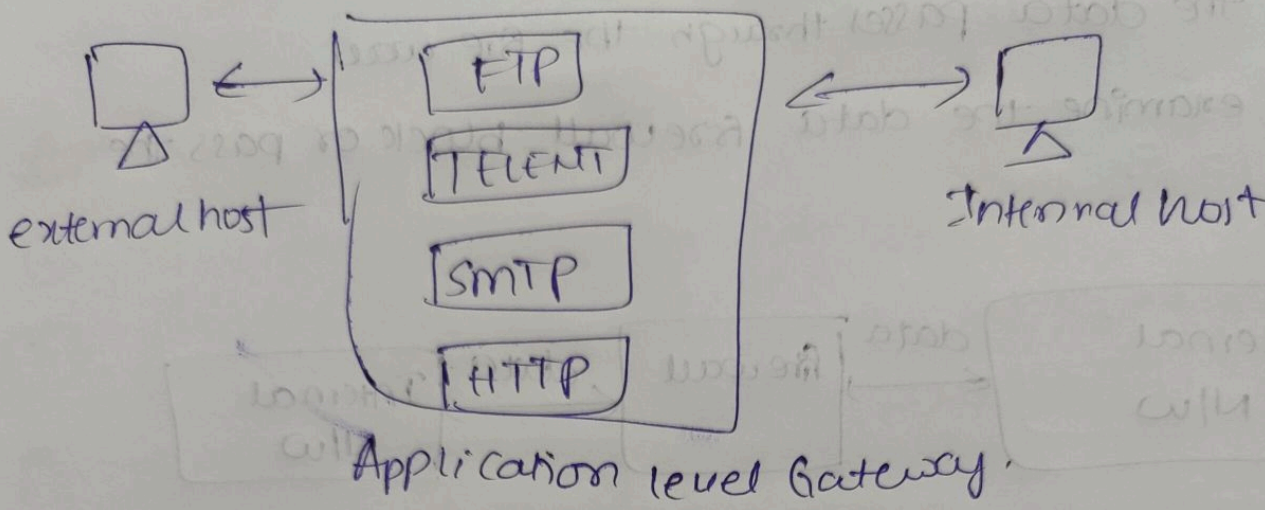
(1) Packet filtering firewalls



⇒ This firewall maintain a filtering table

2) Application level Gateways

⇒ It is also called proxy servers.



⇒ More secure than packet filtering

3) Circuit level Gateways.

⇒ it uses TCP.