3/1/17

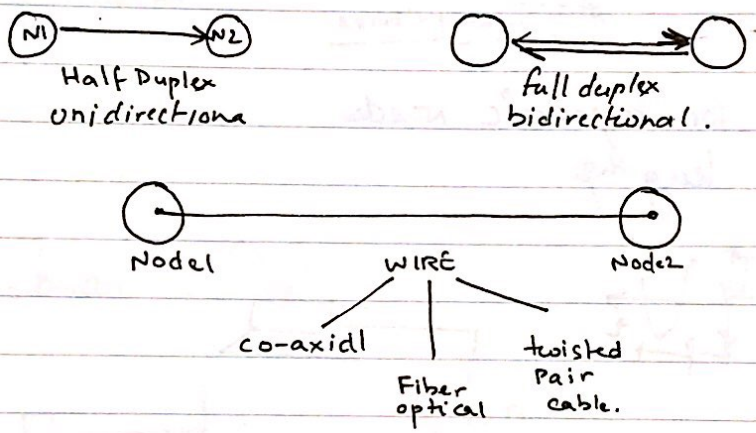
Computer Networks

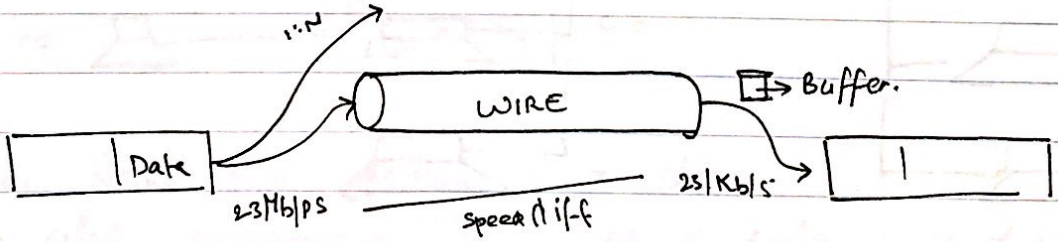
Book : FRosen / Tannenbaum (PPTs)
↳ Theory

Topologies

11/1/17

Mesh , Star, Hybrid, Ring

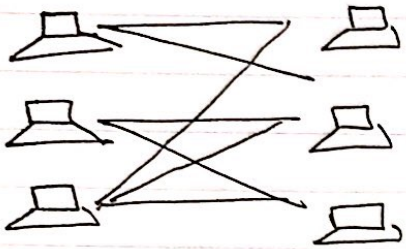




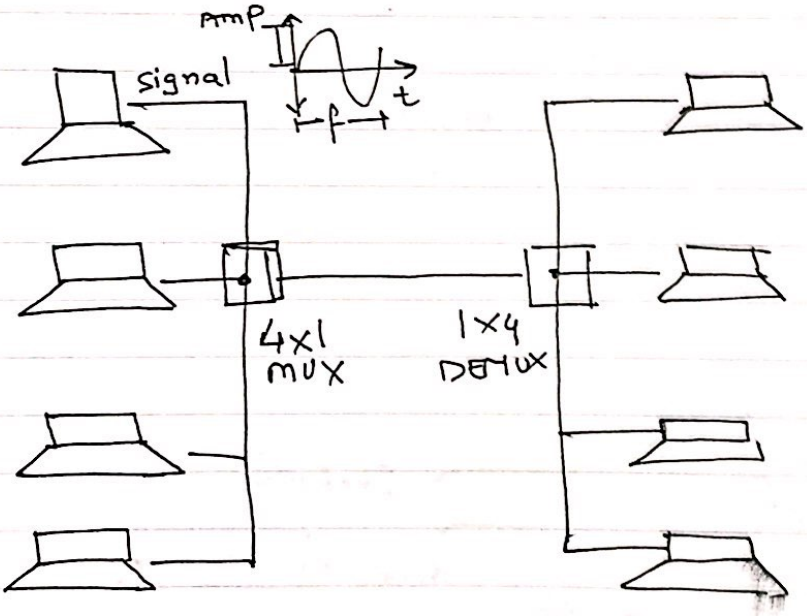
→ Physical layer: data + checksum + error
→ Datalink layer : congestion control
→ Network layer : confirmation of receivers. // port-to port
→ Transport layer: end-to end transfer i/e Appn to Appn.
→ Session layer : Creat a session b/w Appn [ports / sockets]
→ Presentation layer: Ecode/decode ; security
→ Application layer : user level program

16/1/18

1> No-multiplexing



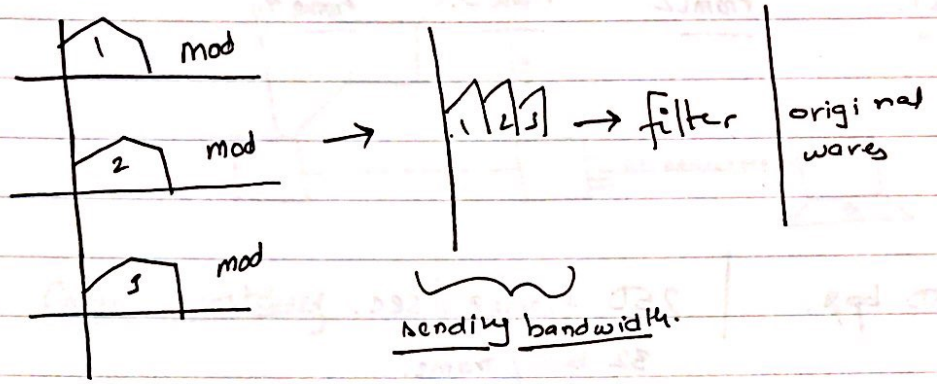
1> No facility for dynamic needs
2> High cable lengths



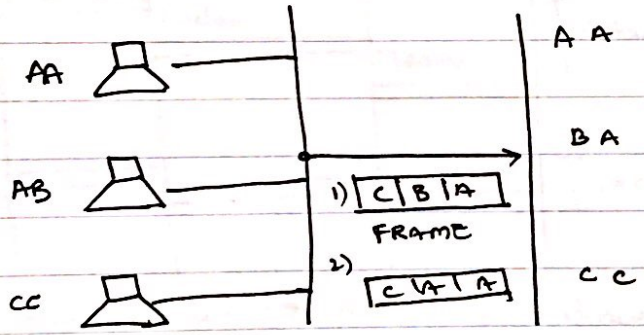
2> Multiplexing-

To avoid collision
→ Keep some traffic control logic
→ change the frequency of each source by fft & add them up.

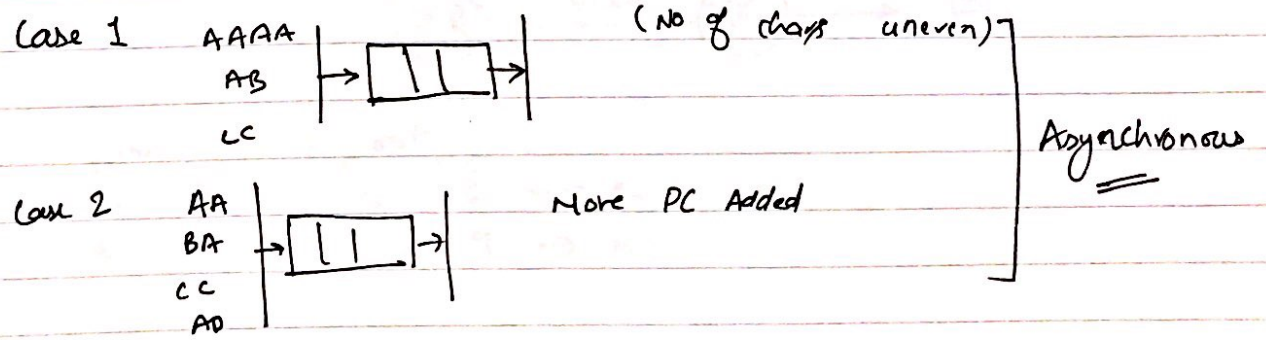
1) Frequency Domain Multiplexing.
2) Time domain Multiplexing.

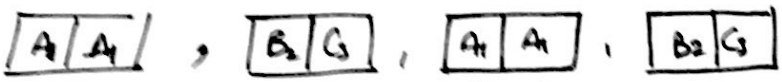


Time Domain Multiplexing



Like Round Robin Scheduling of 1 char
Also called synchronous TDM.
No of devices = No of frame slots.

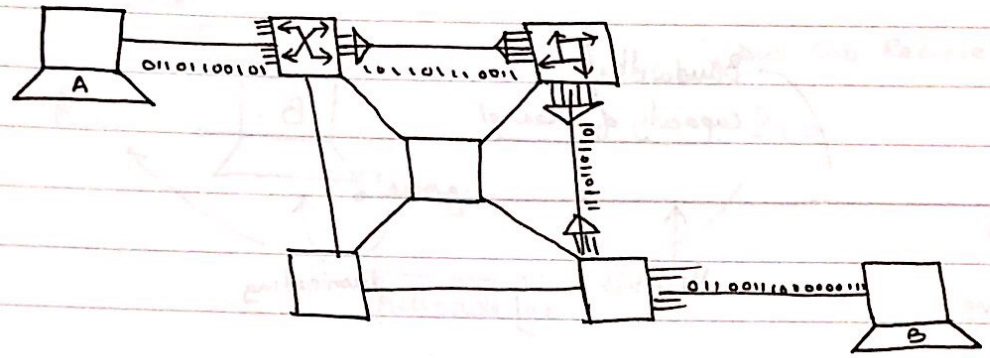


Case 1 → 

from Frame 1. Frame 2. Frame 3. Frame 4.

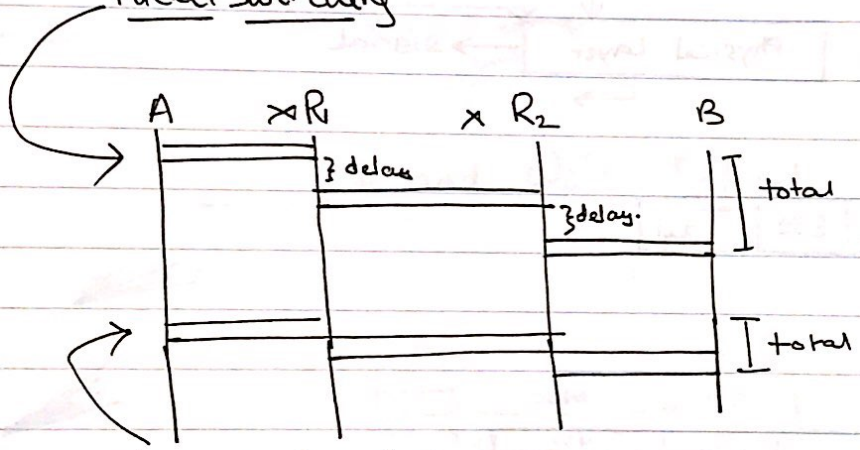
Example

8250 bps. | 250 frames / sec.
52 bits / frame.

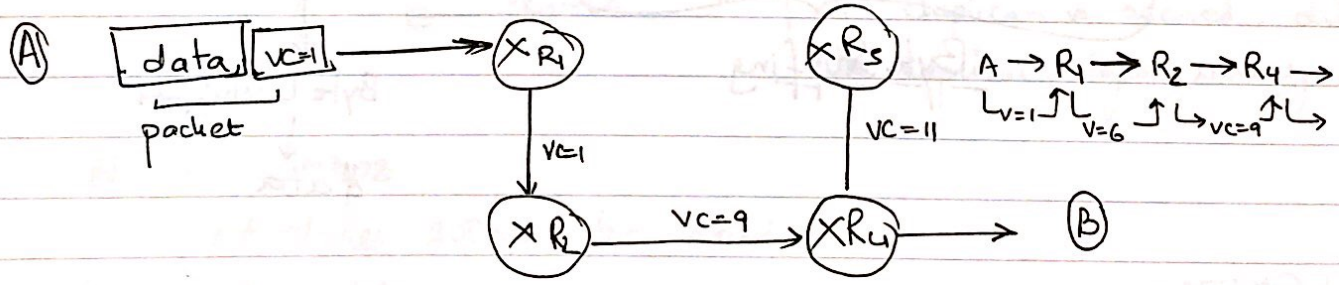


Circuit Switching

Packet Switching

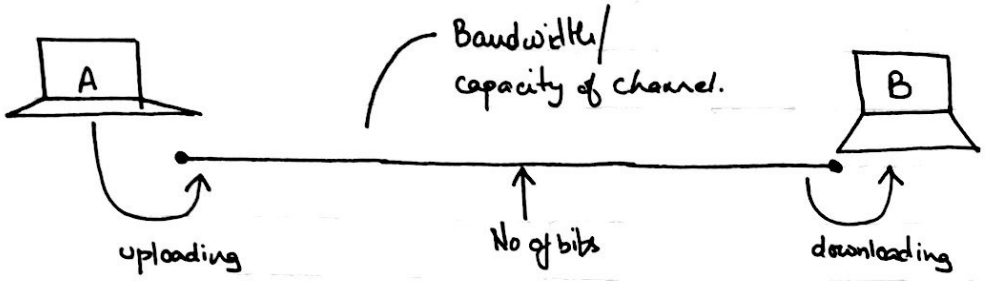


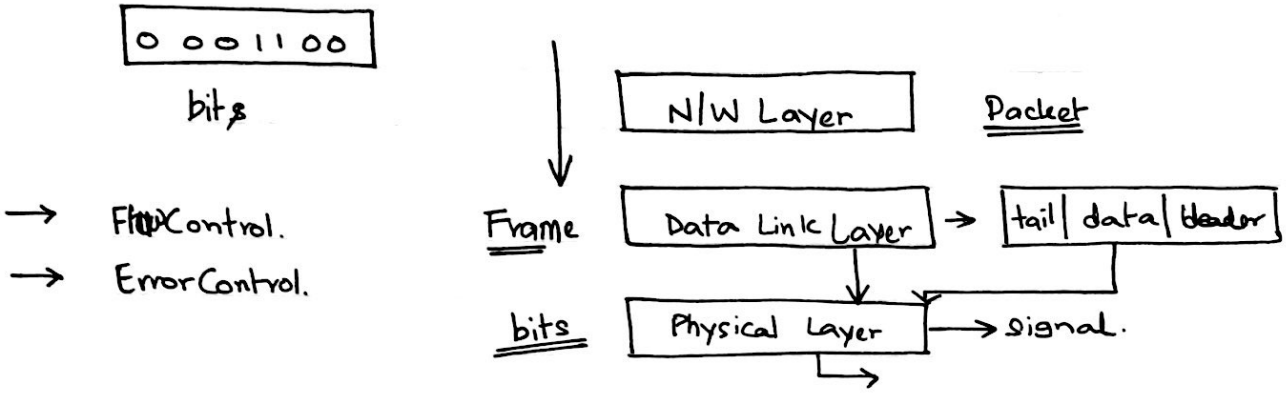
→ Virtual Circuit → mimics circuit switch in packet switching.

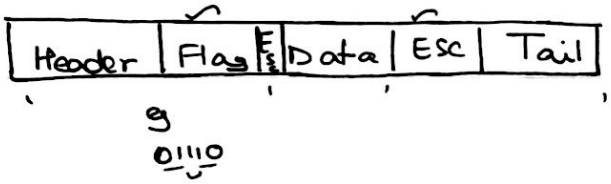


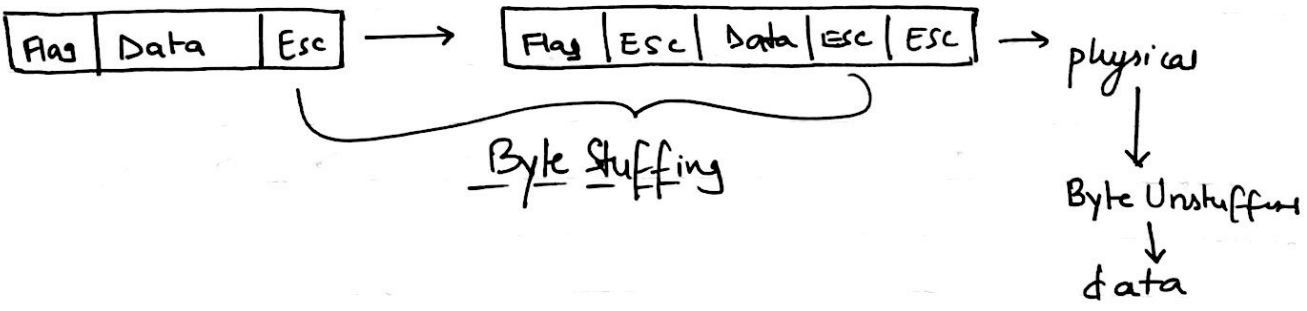
P in	VC	P out	VC	
1	1	5	6	→ R1
5	6	7	9	→ R2

25/1/17







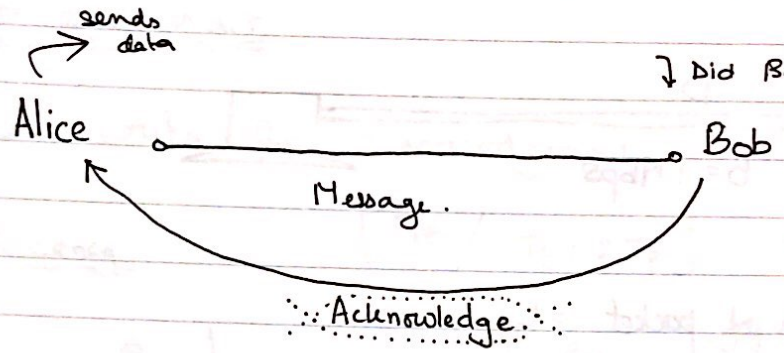


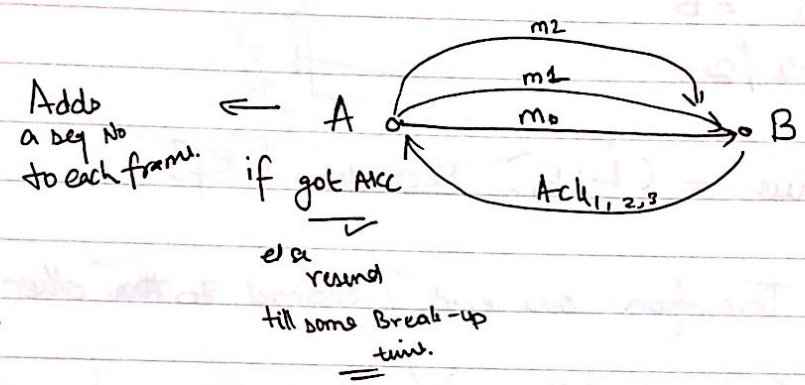
Bit Stuffing

flag : 0 11 11 11 0

data : 011 0 11111/0 1 0 0 0

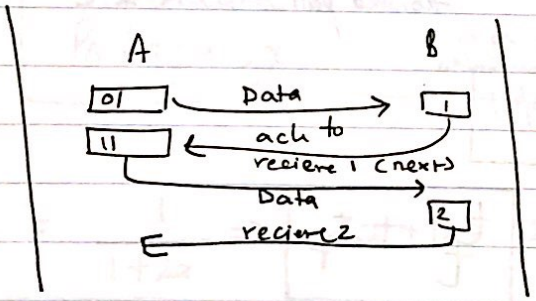
stuffed bit.





"One sided relation don't work".

"Stop and Wait Protocol"



if ack is ~~neg~~ lost then ~~also~~ Alice resends that package. if duplicate is recived, delete the duplicate before sending ack.

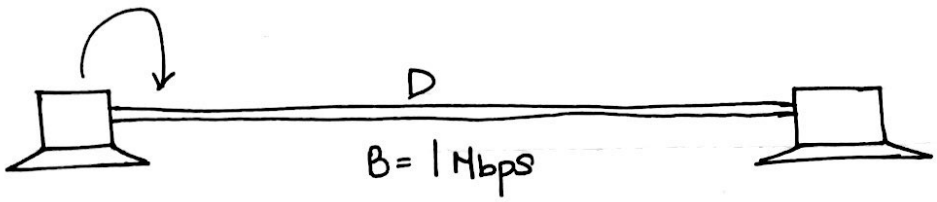
Bw = 1 Mbps

1 bit takes 200 ms for round trip.

Frame = 1000 bits.

Channel Util : $\frac{\text{FrameSize} / 1000}{200000 \text{ (bits)}} \times 100\%$

30/1/18



Simplest Protocol

Length of packet = L
Bandwidth = B
No of Bit's / Sec =

1) Transmision time = (L/B) seconds $[t_f]$

2) Propagation : Time from one end of channel to the other.

t_p = (Length of Channel)/(Speed of prop) //

Speed of prop : ofc = c
twisted pair = 'k' * c $[k \in [0,1]]$

$$t_p = D/V$$

3) Total Time taken : $t_f + t_p$

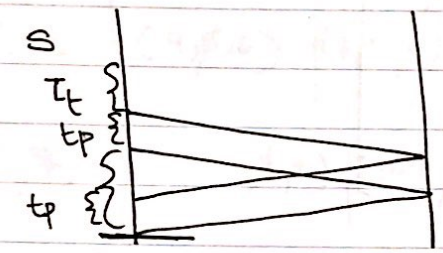
4) Efficiency : useful time / Total time

= $t_t / t_t + t_p$

Stop and Wait.

Sender waits for acknowledgement.

Efficiency : $[T_t / T_t + 2T_p] = \eta = \boxed{\frac{1}{1+2a}}$



$\boxed{a = T_p / T_T}$

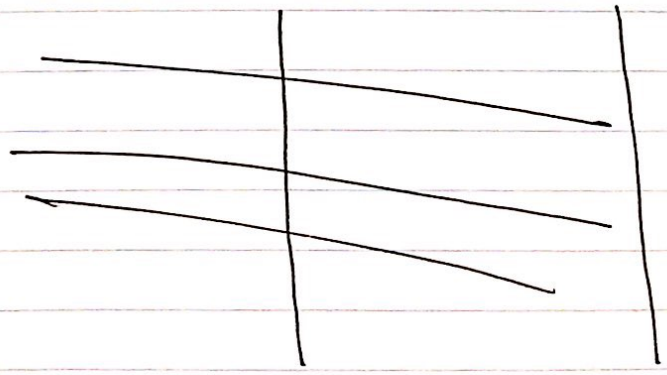
Total = $T_t + 2T_p$

Hw eff (η) is only 6% find best params for 50% ~~A~~

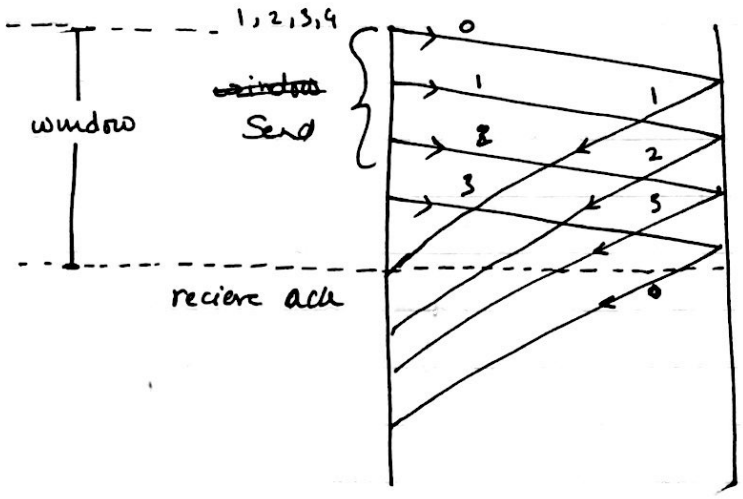
Bandwidth	: B
Package size	: $\frac{2DB}{V}$

$\frac{1}{2} = \frac{1}{1+2a} \Rightarrow 2a+1 = 2 \quad a = 1/2 \Rightarrow T_p / T_t = 1/2$

$\Rightarrow \boxed{L = 2dB/V}$



GoBackN



	m=1	m=2	m=3
⇒	0,1	0,1,2,3	0,1,2,3,4,5,6,7.

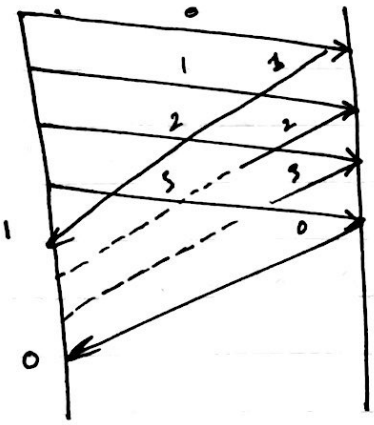
Problem : What if packet is lost?

→ Resend the complete window.

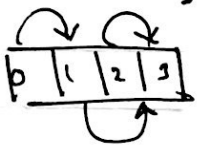
To improve efficiency.

window size = 2^m

0123	0123	0123	...



window size = 1

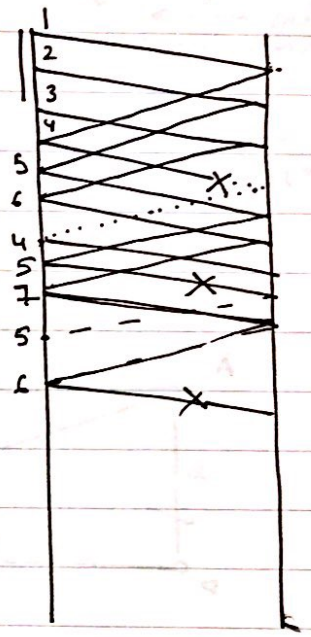


31/1/18

(N) → (N+1)

111 | → 111

Sender is trying to send 10 packets @ window size = 3.
Every 4th Frame is lost.



(1,2,3) | (4,5,6) | (4,5,6) | (7,5,6)

(7,8,6) | (7,8,9) | (7,8,9) | (10,8,9)

(10) | (9,10)

Every 5th Packet is lost

(1,2,3) | (4,5,6) | (7,5,6) | (7,8,9) |

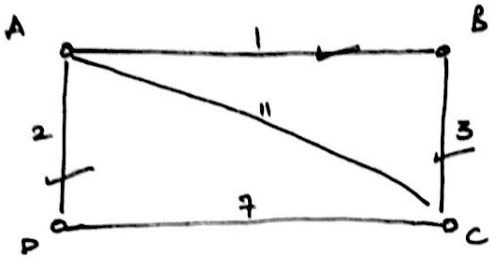
(7,8,9) | (10) | (9,10)

20/2/18

Network Layer

Node 1 (Network Layer) [packets] → data link [congestion / receive check] → bits [phy layer]

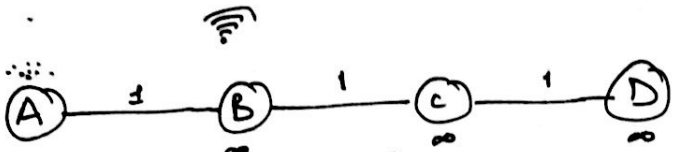
Node 2

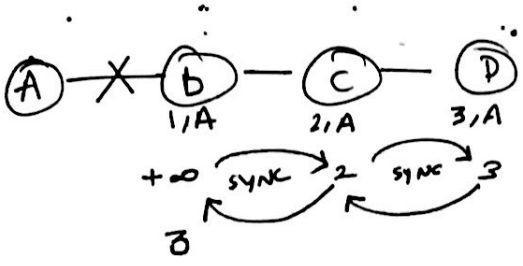


[AC and DC will be used.]

- Distance Vector Routing (DVR) Algorithm

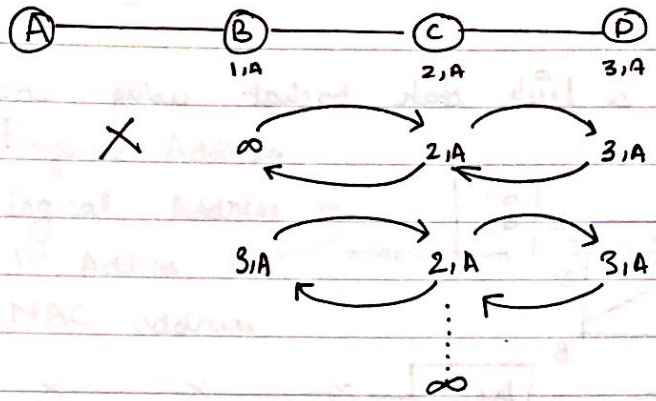
Greedy Approach



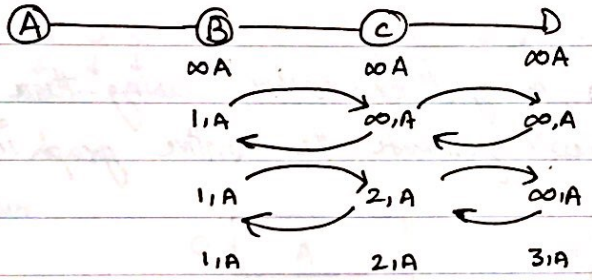


B	
A	X∞

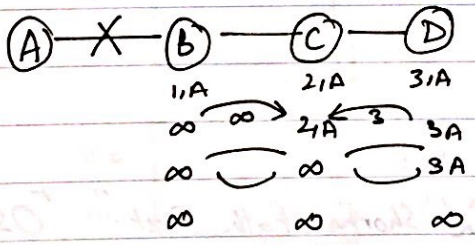
C	
A	2



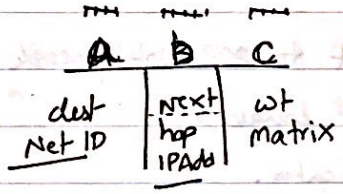
count to infinity problem



Solution to counting to infinity problem



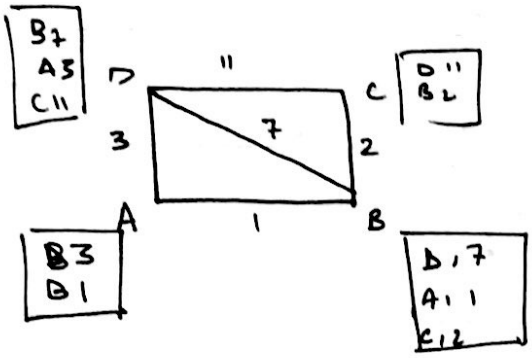
D cannot Reach A



if a node is dependent on some other node then the former node sends the dist vect as ∞ to the later node.

Link State Routing (LSR)

1. Every router will prepare a link state packet using local knowledge



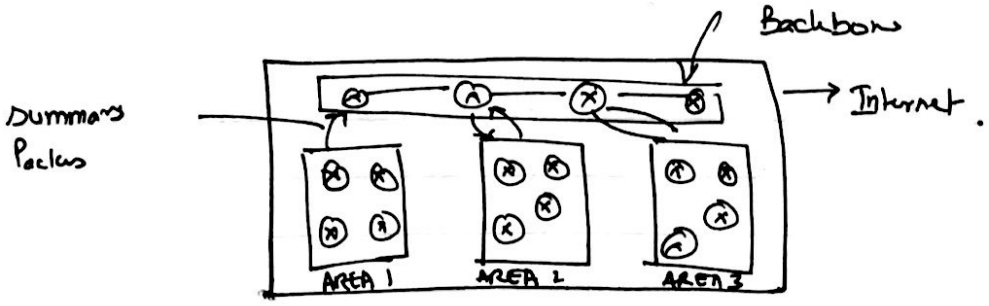
2. All the packets are flooded to all the routers

3. Every router will get LSP from every other router, using these link state packets, every router will generate the entire graph in its local memory

4. Every Router will do single source shortest path algo to find the final routing table.

- # count to ∞ Not possible.
- # high congestion.
- # duplicates.
- # high bit errors.

LSR is implemented using "Open Shortest Path First." "OSPF"



21/2/18

Network Layer

1) Physical Address
2) logical Address → implementation 32 bit.
3) IP Address
4) NAC - address

(implementation)

IP Address

HostID

10.0.0.192 — 0-255. 0-255. 0-255. 0-255

- 8 bit

N/W ID

i.e $2^{24} - 2 \approx 16$ mill.

(0.0.0.0 & 255.255.255.255 are locked)

Classes

fixed @ 0

0	A	0 | 0000000	$2^{24} - 2$ Host, 126 N/W ID
1		0.0.0.0 to 127.0.0.0	
10	B	128.0.0.0 to 191.0.0.0 (N/W ID; N/W 1.a)	$2^{16} - 2$ Host, $2^{14} - 2$ N/W
11			
110	C	192.0.0.0 N/W to 223.0.0.0 (110 [00000.0.0.0] Host)	$2^{8} - 2$ Host, $2^{21} - 2$ N/W
111			
1110	D	224.0.0.0 to 255.0.0.0	
1111			

Choice of class depends on no. of networks & connected computers.

Classless [CIDR]

125.0.0.16 | 26 → total no of network

24 +2

$2^5 - 2$ ⇒ 62 Local IDs

⇒ 125.0.0.00 | 010000

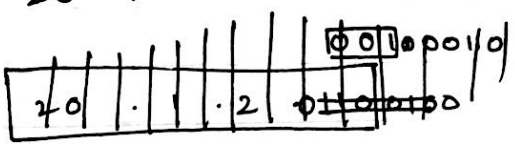
Network | Host

eg 128.6.5.64 | 16

Network 128.6.0.0

Host . . 5.64

eg 20.1.2.100



20.1.2.011 00 100

Network | Host

20.1.2.96 to 20.1.2.127

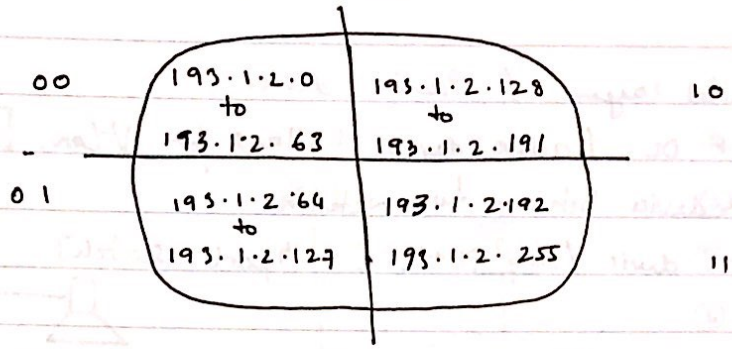
Q Given 192.1.2.0 as the network ID divide into 4 parts

193.1.2.0 | 24

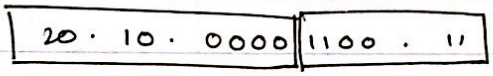
193.1.2.00000000] 127] make 1 bit a part of the network ID

1 0 0 0 0 0 0 0] 128

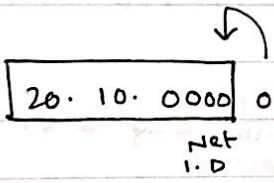
1 1 1 1 1 1 1 1



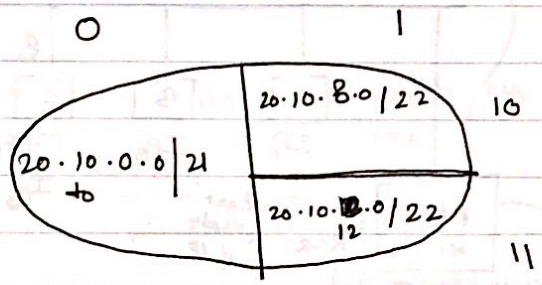
Q. ISP has block of 20.10.12.11 | 20 and wants to give half of its IP to Company 1) quarter to other and keep the rest with itself propose as suitable to ~~the~~



20.10.0.0 to 20.10.15.255

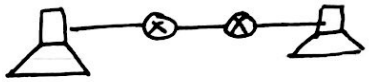


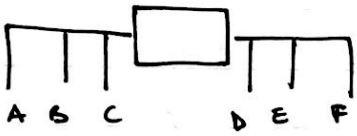
=> 20.10.00000,000.0



22/2/18

1) Repeater
2) Hub → Physical layer / Passive device
3) switch → PL + DL / active device / allows for V-Lan. [within network]
4) Router → Active device between two networks
5) Bridge → Active devic / only PL+DL [Multiport switch]



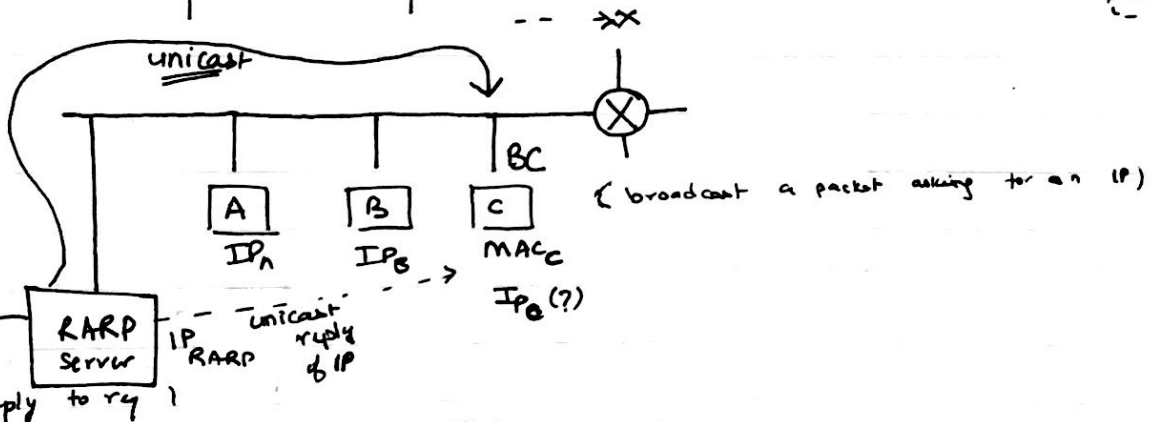


collision domain

3 layer switch ≈ Router.

1 RARP | ARP | BOOTP & DHCP

10.20.0.0 to 10.20.255.255



(broadcast a packet asking for an IP)

// Broad cast - remains within the network.

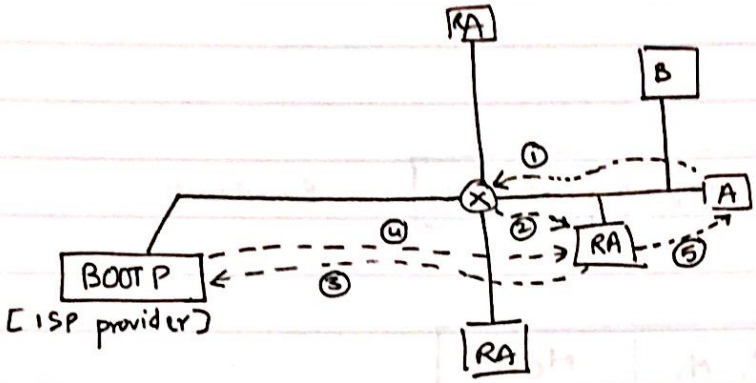
M_A	IP_A
M_B	IP_B
M_C	IP_C

Static static

RARP → wastes IPs

BOOT P

① Send Broadcast for IP
② send to RA
③ send Req for A
④ Reply back to RA.
⑤ Reply to A it's IP



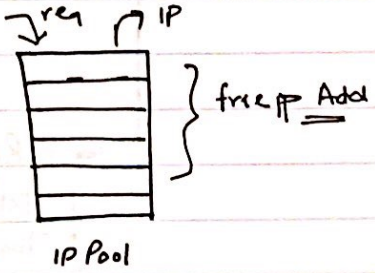
IP are still static

今日
壽終 誕生日
birth life day
訖止

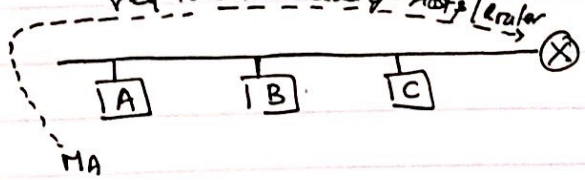
DHCP [Dynamic Host Control Protocol]

MAC	IP	Time
MA	IPA	time 1
MB	IPB	time 2
⋮		

IPA is assigned to MA only for time 1



ARP Address Resolution Protocol



ARP req IPs Ms = ?	Mc All 1's

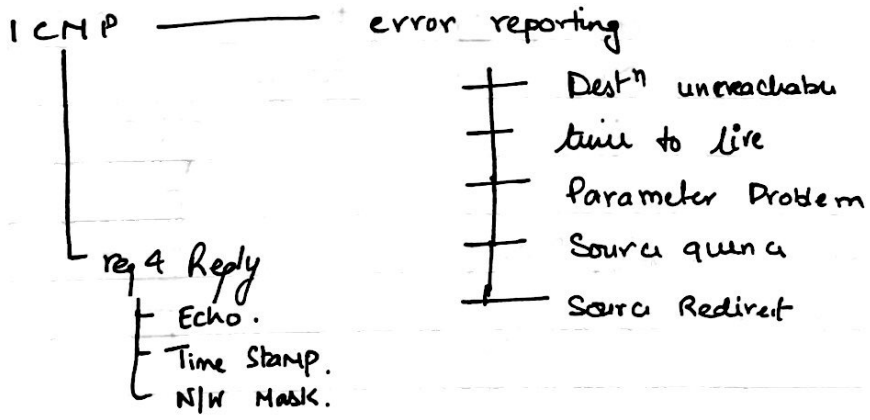
Broadcast

ARP reply IPs Ms	Mc Ms

at data

ICMP

- N/W layer.
- feedback Messages.



21/3/18

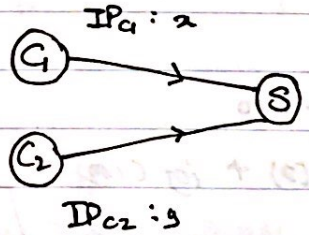
Transport Layer

- End-To-End Connectivity
- Packet Duplicate
-

TCP UDP

Source Port (16)	Destination Port (16)
Sequence No (32)	
ACK. NO. (32)	
TCP header (4) | SYN | URG | ACK | DSH | RST | FIN | Adv Window size (16)	
Checksum (16) ~~window~~	Urgent Pointer 16
Options (32)	
Data (32	

Socket: Combination of IP address + Port i.e 48 bit Random number



Seq No: $(2^{32}+1)$ bytes ~~to~~ whenever this is crossed, repeats

If the sent seq is 4G+1 then a wrap around happens and the time is called a wrap around time after which the seq repeats

B/w = 1b/s what is w.r.t.

$$WAT = 2^{32}\ B/1\ b/s = 2^{32}\ Sec \approx 142\ years.$$

Let BW = 1 Nbs $= \frac{2^{32}}{2^{24}} = 2^{8}$ sec

Life Time Max time the packet can be alive in the network before being absorbed by the reciver. $\simeq$ 3 min.

$$WAT > LT$$

when $B/w = 2^{32}/2^{30} = 2^2 = 4\beta$ I

To increase the WAT we add bits from options and add to the start.

Eg LT = 180 s

B/W 2^{30}

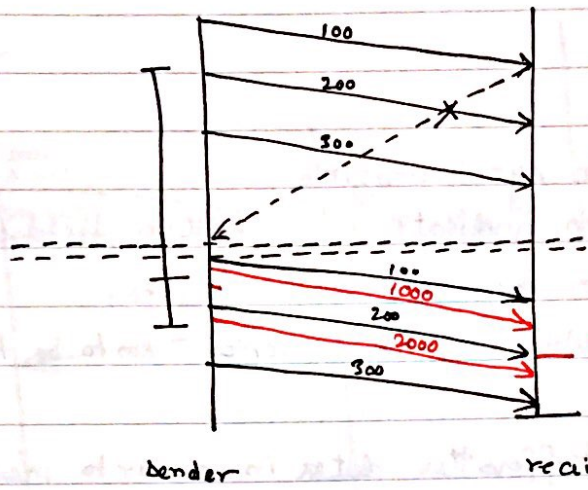
what is min No of bits in seq to prevent wrap around.

$$\frac{2^x}{2^{30}} = 180$$

$$2^x = 2^{30} \cdot 180$$

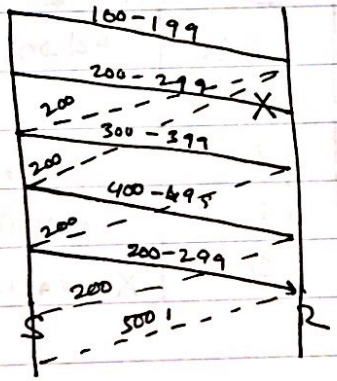
$$x \log(2) = 30 \log(2) + \log(180)$$

$$\Rightarrow x = 38 \quad \Rightarrow \boxed{6 \text{ more bits.}}$$



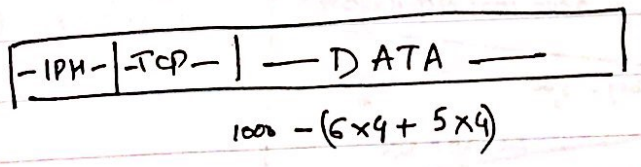
To avoid this the sequence is started with random number.

Acknowledgement Contains the seq no of next expected byte.



Header Length (4 bits)

if the total len field in ~~IP~~ IP datagram is 1000 & header len is 6 also hlen of TCP is 5, find data size in packet.



$1000 - (6\times4 + 5\times4)$

Flags

1. Syn : used to synchronizing
2. Ack : used to indicate the ACK NO field in the header is valid
3. FIN : used to terminate the connection
4. RST : Reestablish ; The connection has to be terminated before eat (reset flag)
5. PSH : TCP buffers the data in order to increase efficiency
   PSH Flag pushes the data directly into the application.
6. URG : (Urgent) : data in segment is urgent & has to be given the highest priority.

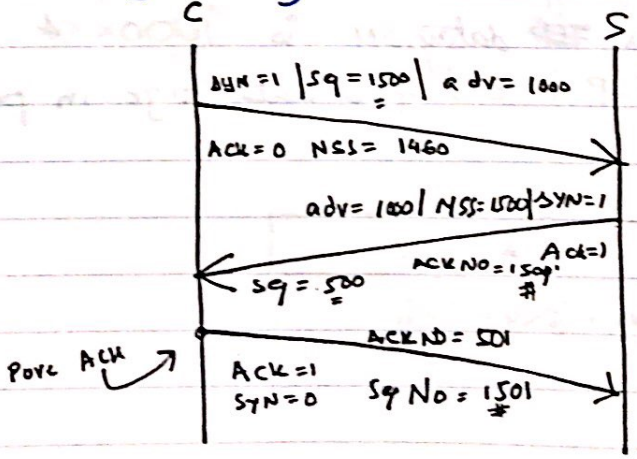
SYN	ACK	Action
1	0	Request for Data
1	1	Reply back
0	1	Only Ack
0	0	X invalid X

Maximum Segment Size

Data → any size

App N

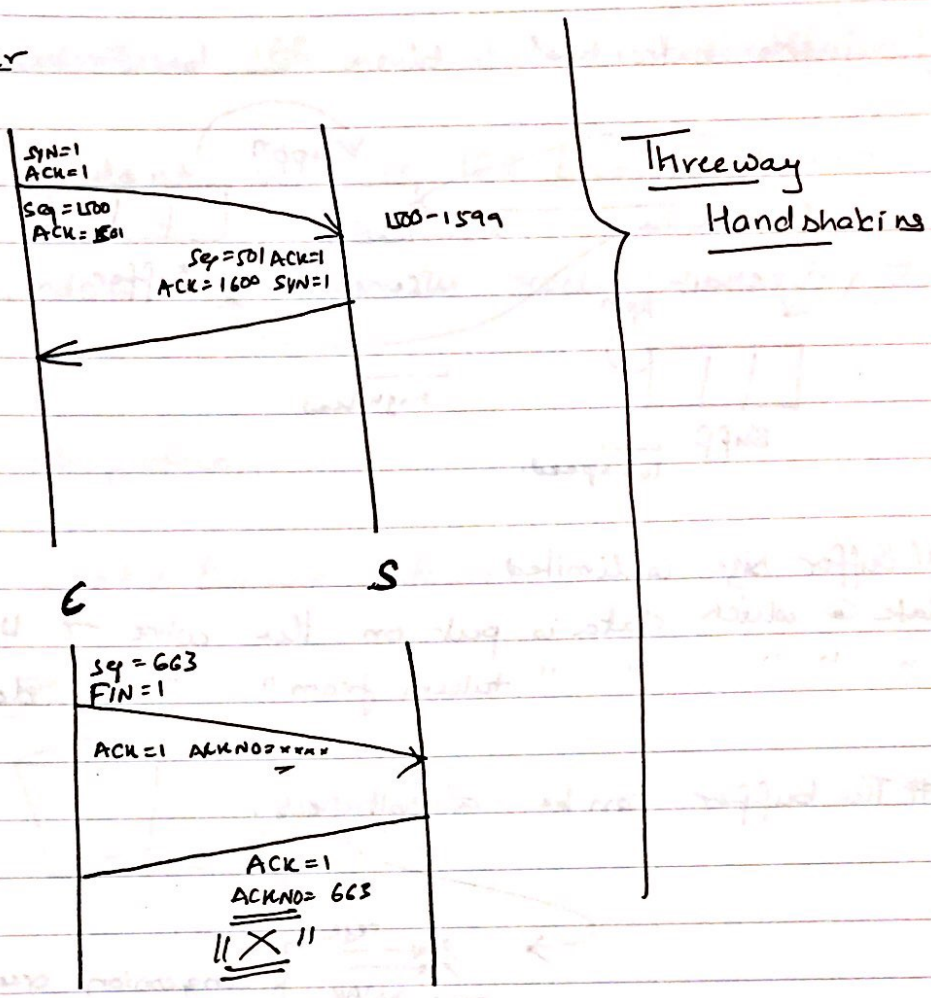
The max Datagram size.



Initial Connection

= =

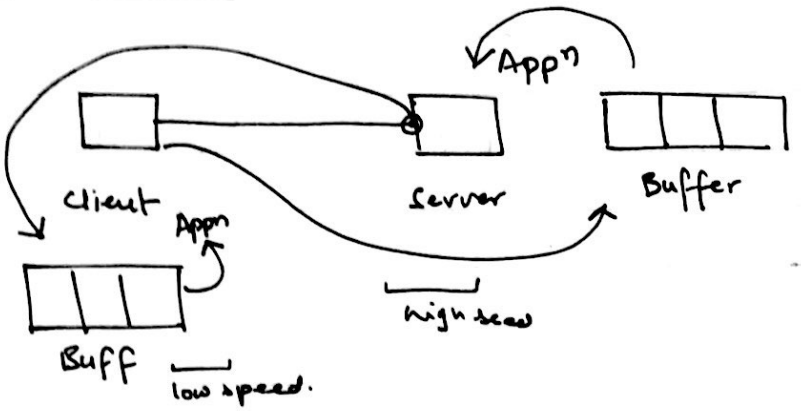
Data Transfer



Termination

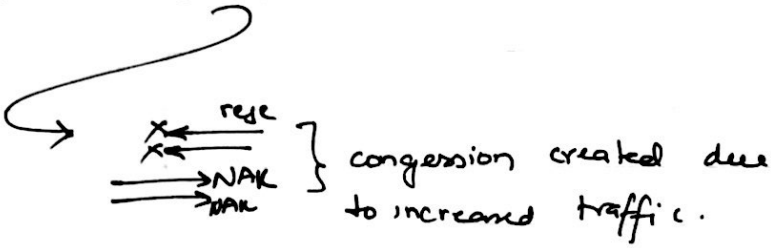
28/3/18

Congestion Control



// Buffer size is limited.
Rate @ which data is put on the wire → Uploading.
" " " " " taken from " " → downloading.

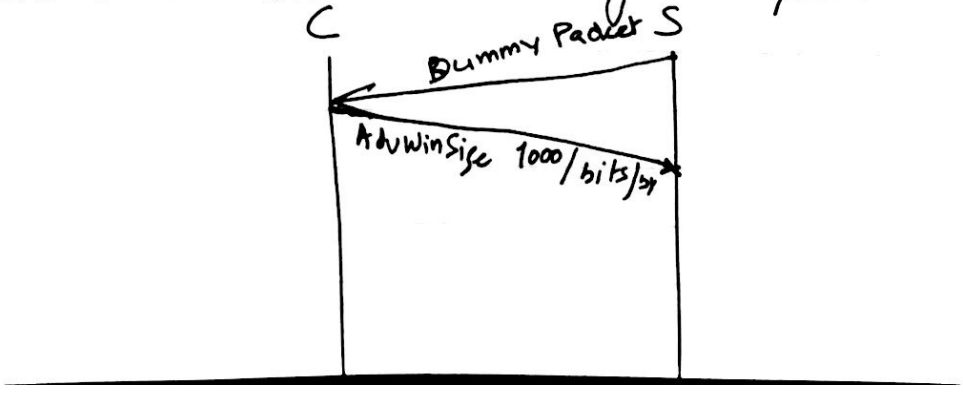
The buffer can be a bottleneck.



To avoid this sync the speed of uploadr and download.

Advanced Window Size This is the window size & then based on this the sender decides upload logic. (16 bits i.e $2^{16} = 64kB$)

To extend it to ~~more~~ e take bits from Option. i.e 32 bits

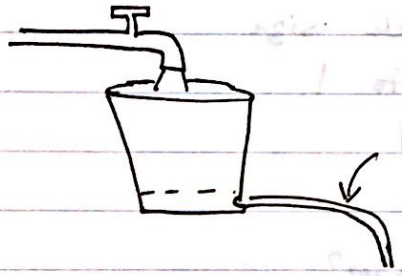


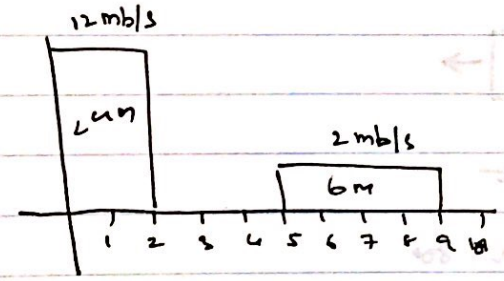
If the X has advertised 1GB should it send it directly?

→ The sender should not send of 1GB because the net may not be able to hold this data ∴ sender will use congestion window to keep the track of capacity of net

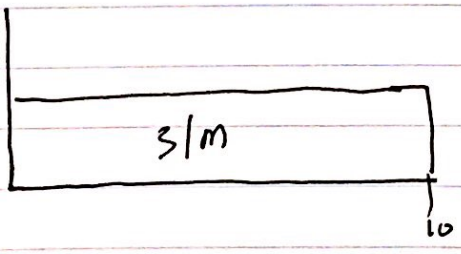
Congersion Control protocol.

@ Reciever Leaky Bucket Protocol.





Bursty Data. receiving data.



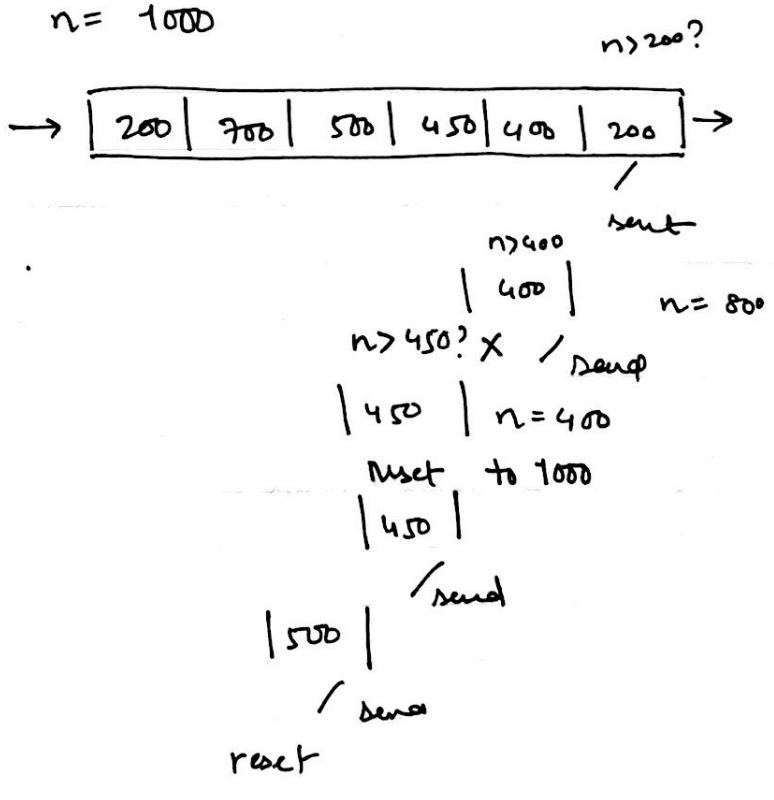
consuming data.

- A leaky bucket can be implemented using FIFO
A FIFO holds the packets if the traffic is of fixed sized packet the process removes a fixed no of packets at each tick of the clock, if the traffic is of variable len, the fixed output break mesh be based on the no of divice/bits

Algo

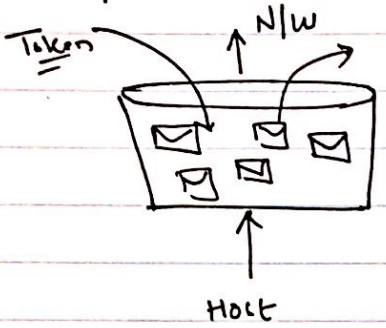
1. init counter = 0 at tick of clock
2. if ~~if~~ n > size of packet :
   send packet & inc the counter by pack size.
   repeat
   repeat till n is < pack size
3. Reset the counter & go to 1.

let n = 1000



Token Bucket Protocol

To remove a packet, add equal value of tokens.



upload rate fixed by the tokens.

10/4/18

Transport Layer

TCP | UDP → High Transmission Speed

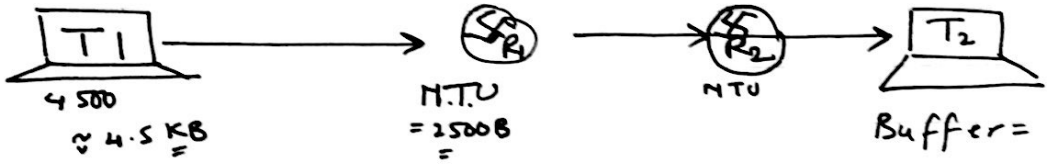
TCP: connectionless; connection based

Youtube but Normal video streaming uses UDP.

→ SMS → UDP

→ Amazon.nk → TCP.

Congestion Control



1) header = 20B Data = 2480

2) header = 20B Data 2020

64 / 4.5

More Frag | off

1 | 0

0 | 370

Case 2

=

4500 B

MTU
2500 k

MTU
1500

64 KB buffer

		F	off
h=20 D=2480 →	h=20 d=1480 →	1	0
	h=20 d=1000 →	1	1480/8
h=20 D=2020 →	h=20 d=1480 →	1	2480/8
h=20	h=20 d=540 →	0	3960/8

11/4/18

Session Layer

Security. | Privacy.

- unauthorized
- No modification
- available
- etc

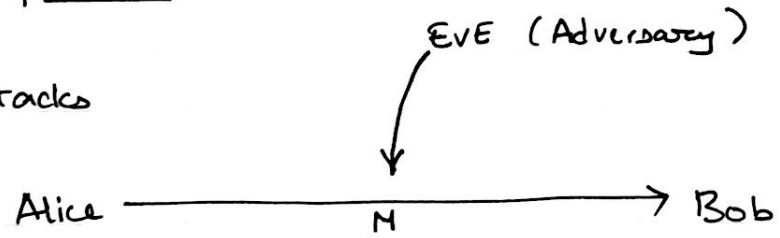
Security

- confidential
- Integrity
- Availability

] authentication

CIA Properties

- Attacks



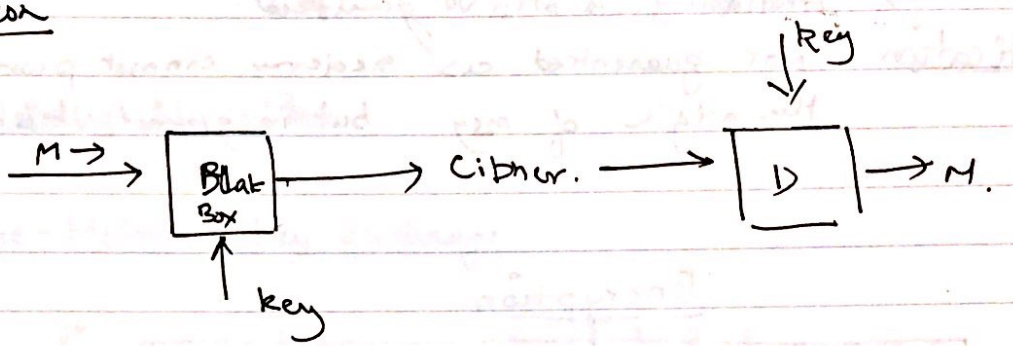
- Message not recieved.
- Message recieved is ~~to~~ cultured.
- M is overhead.
- corrupted.
- delayed.
- fabrication of New Msg.
- Stealing ID of sender
- His broadcasted.
- Replay Message.

あいうえお
かきくけこ
さしすせそ

Attacks

- Passive
- Active

Encryption



1) Cypher Text attack.

'C' → M

m, C ∈ AI

Algo

$C = (M+k) \% 26$

] if k = 3 ceasar cipher =

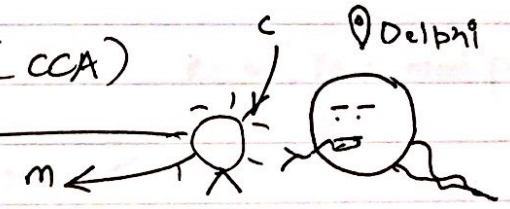
2) Plain Text Attack

$P_1, P_2, \ldots P_n$

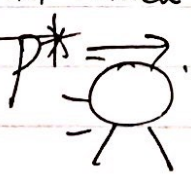
$p^* \longrightarrow c^*$

3) Choosen Cipher Attack (CCA)

Choose from set of ciphers



4) Choosn Plain Text Attack

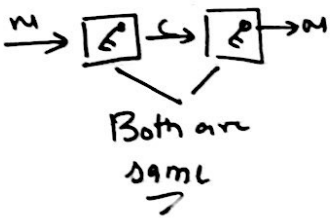


m ⟶ encrypt ⟶ C = E(m, k) → D(C, k)

→ Encryption
  → achieves confidentiality.
(only when safe) → Integrity. ~~[illegible] encryption [illegible]~~ ✓
from attacks
  → Availability. is still NO guaranteed.
→ Authentication : Not guarenteed as reciever cannot prove the origin of msg. but in general it is.

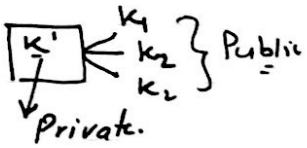
Encryption

Symmetric
- Locks the msg with key



- sharing the keys is hard
- requires alot of keys.

Asymmetric (Public key)



Problem with symetric

- $^nC_2$ pairs
- Sharing the key. (?)

User $\xrightarrow{k}$ gmail / Amazon.

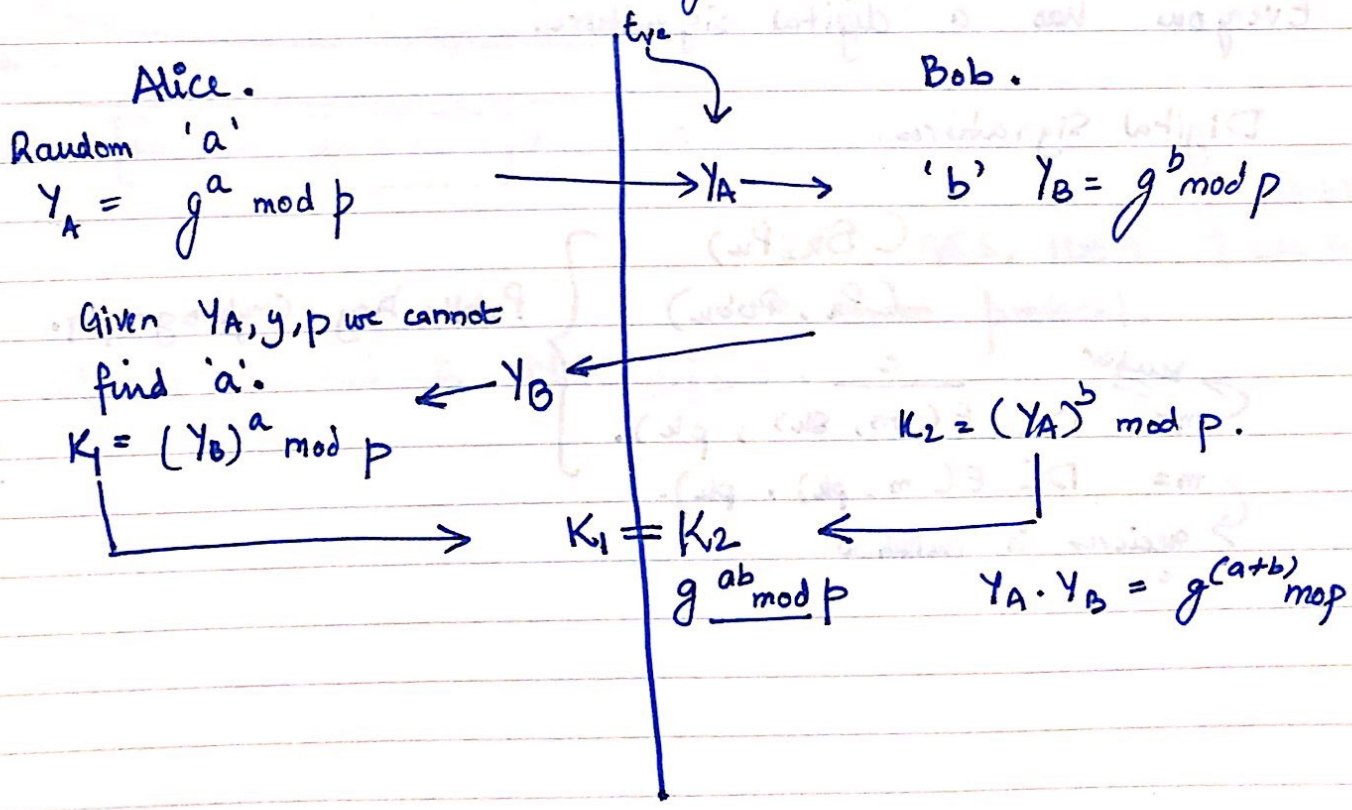
Key Sharing Algorithm

Diffie-Hellman Key Exchange

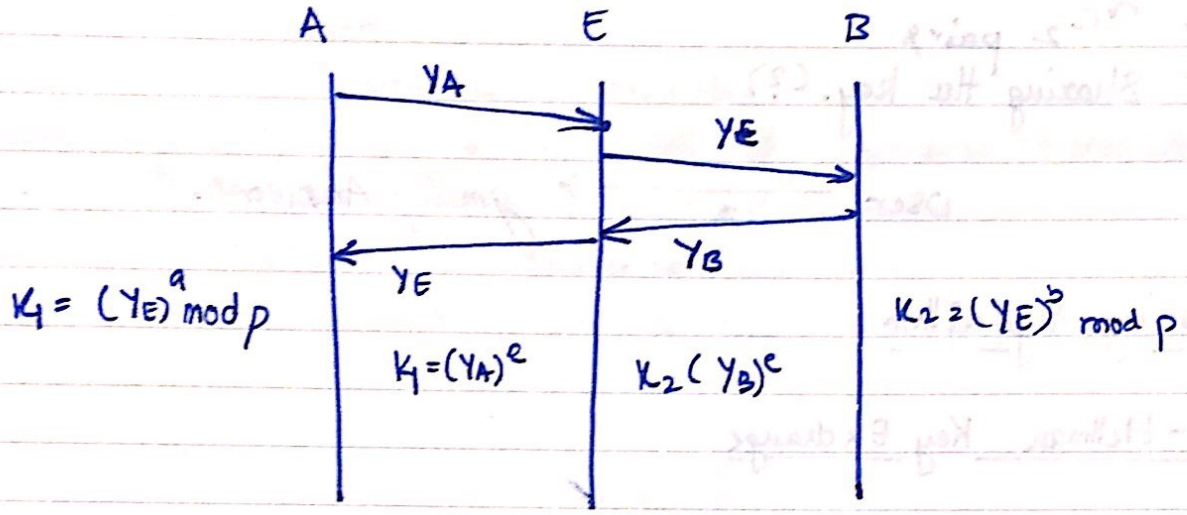
$Z_7 = \{1, 2, \ldots 5, 6\}$ %7 is a group.
↑ prime

extended euclidian algo / FLT - Fermat's little theorem.

Z_p^* is a group G (G, p, g) p = prime no.
g → generator.



Drawback → No authentication



Man in the middle attack / Meet.

Solution: Add authentication.

Everyone has a digital signature.

Digital Signatures.

(S_k, P_u)

(P_u, Pub_k) } Public Key Cryptography.

sender $\xrightarrow{c}$

$m = D(E(m, S_k), p_k)$.

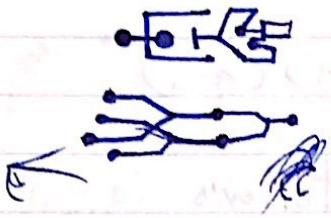
$m = D(E(m, p_k), p_k)$.

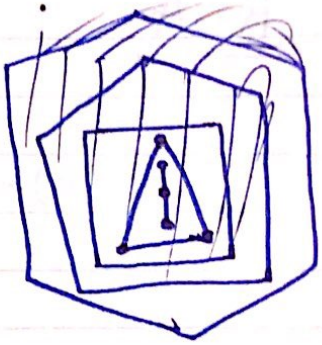
↳ receiver is authenticated

日本

A → Y_A encrypt with S_k.
B → Y_B encrypt with S_k.

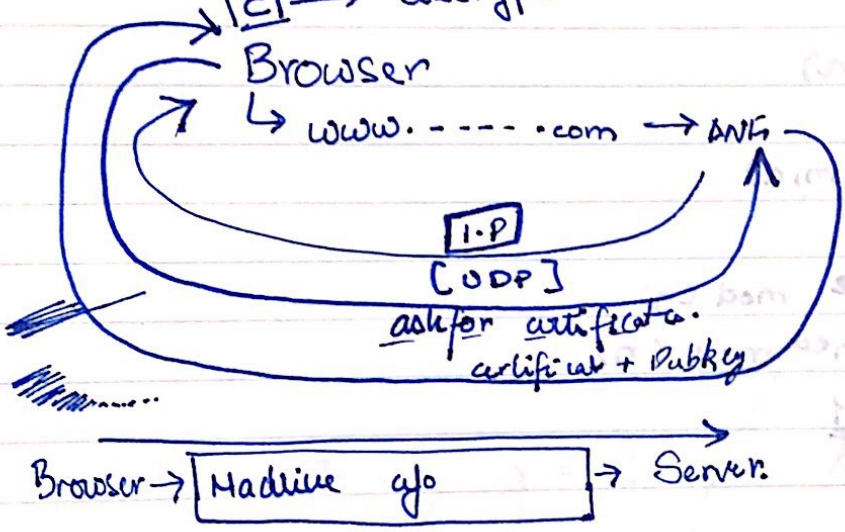
Certificate authority.





SSL

Secure Socket Layer



Browser has the Pubkey built in

No.

DES, AES, IDEA { 128 bit / 256 bit
↳ symm protocol.

alt to DHKS is MAC digest.

RSA [Rivest & Shamir & Adleman]

$$\phi(n) = (p-1)(q-1)$$

Euler's

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

$$e = d^{-1} \bmod \phi(n)$$

$$c = m^d \bmod (n)$$

$$c = E(m, d)$$

$$D(c, e) = c^e \bmod (n)$$
$$= m^{ed} \bmod (n)$$
$$ed = 1$$
$$= m$$

- Fermat's little theorem
- Extended Euclid
- Euler's theorem

19/4/18

27 Elgamal Encryption Key

$G : Z_p^* \cdot g$

Public (G, g, p)

$Z_4^* = \{1, 2, 3, \ldots, 10\}$

↳ generates the group.

$C = (y^r m \bmod p)$

$C = (c, c^x) \bmod (p)$.

$(y^x)^{-1} m (g^r)^x]^{-1} \bmod p$.

$P = 107$ / $g = 2$ / Pvt key Alice. = (67) / $b = 45$

Alice ← Bob "$b = 45$"

"$B = 66$

| Pubkey = 97 $C = 28$ | $P_{key\ bob}$ =

Find vulnerability in Elgamal Enc

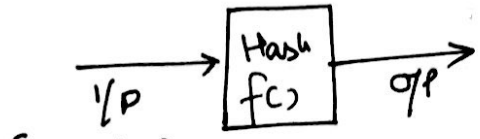
10 marks

25/9/18

Hashing

A B

$C = g^m \cdot (y_a)^b$

1> 

$D(c,a) = c \cdot (y_B^a)^{-1} \bmod p$

$= g^m (y_a^b)(y_B^a)^{p-1} \bmod p$

$= g^m \bmod p$

2> Irreversible function. $f(x)$ exists $f^{-1}(x)$ does not.

3> even if input differs by 1 bit, output differs by many.

4) Least Collisions

Security : C I A

acts like checksum.

Alice ⟶ Bob

(C, H(m))

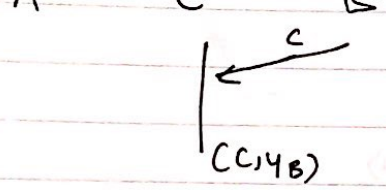
↳ $m' = D(C, k)$

if $H(m') = H(m)$

↙ integrity =

if hash of m is added to the data, then we can overcome the chosen cipher text attack.

A E B



$c' = c \cdot g^{m_2}$

(chosen cipher text attack)

(c', A)

$= c' (y_B)^a \% p$

$= g^m \cdot y_A^b \cdot g^{m_2} \cdot y_B^a r_B$

$= g^{(m+m_2)} \% p$

$= g^{m'} \% p$ // message modified. (Integrity Vollated)

Digital Signature Scheme

Sender

m

$C = E(m, k)$ →

H(m) → Digital Signature (H(m))

Reciever

$D(c, k) = m'$

verify MD

$= H(m)$

if $(H(m) = H(m'))$

→ verified

Egamal DSS

(G, p, g)

A

a is put

$y = g^a \% p$ (pub)

$a = g^k r \cdot p$ for some $k \in (0, p)$

$H(m) = (xr + ks) \bmod (p-1)$

$S = [H(m) - xr] k_1^{-1} \bmod (p-1)$

Send $\longrightarrow$ $(H(m), \underbrace{S, r}_{\text{signature}})$

$g^{H(m)} = y^r r^s$

Pf:

$y^r r^s = (g^x)^r \cdot (g^k)^s \bmod (p-1)$

$= g^{(xr+ks)} \bmod (p-1)$

$= g^{H(m)}$

$p = 23$ $x = 3$ $m = 7$ $H(m) = 7$.

$g = 5$. $G = Z_{23}$.

Let $k = 1$

$r = g^k \bmod p = 5^1 \bmod 23 = 5$

$r = 5$

$H(m) = 3 * 5 + 11 * 1$

$S = [7 - 3 \cdot 5] k_1^{-1} \bmod (p-1)$

$15 = 1$

$[7 - 22] \cdot 8 \cdot (8 \cdot 23)$ (4)

2 $S = K$

$y = 5^3 \cdot 1 \cdot 23 = 70$

$y^r r^s = 10^5 \cdot 5^{14} \cdot 1 \cdot 22 = 2 \; 10 \; \cancel{19} \cdot \cancel{13} \; 9.$ (17)

$g^{H(m)} = 5^7$ (3) (17)

matched

$R = 9$

$S = (7 - 3 \times 5^9 \cdot 1 \cdot 23) - 5 \cdot 1 \cdot 22$

$= 20$

$\Rightarrow (H(m), 20, 11)$.

- Euler's Theorem.

M, N (st both are coprime) (GCD(M, N) = 1)

$N = a^p b^q c^s$

$\phi(N) = [(1 - 1/a)(1 - 1/b)(1 - 1/c)] \times N$

↳ euler's totient $\Rightarrow$ $M^{\phi(N)} \bmod N = 1$

$32^{32^{32}} \bmod 9$ $\quad a = 3^2$

$\phi(N) = (1-1/3) \times 9$

$= 2/3 \times 3 = 6$

$32^6 \bmod 9 = 1$

$32^{32} \% 6$

$=$

$6 = 2^1 3^1$

$= (1-1/2)(1-1/3)\,6$

$= 2$

$32^2 \bmod 6 = 4$

$\Rightarrow 1$

$32^{32^{\cdots}} \Rightarrow$ $\quad 32 \% 9 = 5$