Computer Network

Date:

Protocols

ARP (Address Resolution Protocol) :-

it work on 3rd layer of OSI model

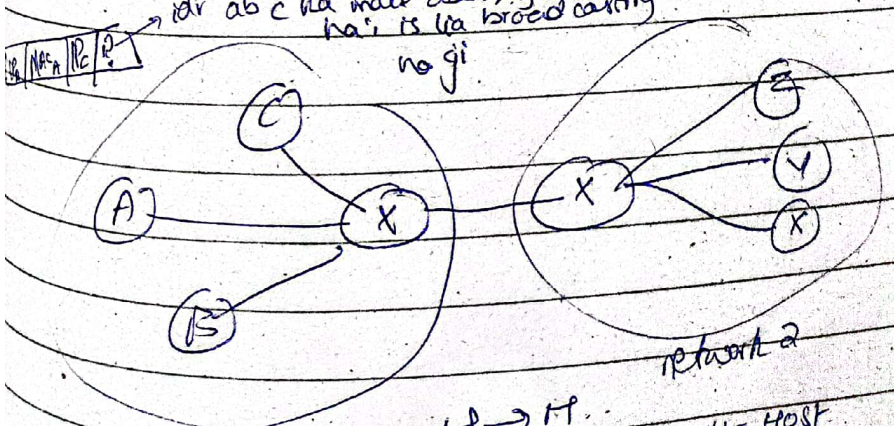
It translate IP address to Mac Address
logical address to physical address

when a new computer join a LAN it is assigned a unique IP address to use for identification and communication

When an incoming packet come the host request for a MAC address from ARP. in order to send packet to another host. so ARP check in its cache that if Mac address corresponding to IP address is there or not. If there is no ~~ifado~~ mac address then ARP broadcasting and packet is send to all machine.

jis machine kā ip address hota hai wo machine wo packet lay lagti hai

idr ab c ka mac address nhi hai is ka broadcasting no gi



H → H
H → R
R → H
R → R

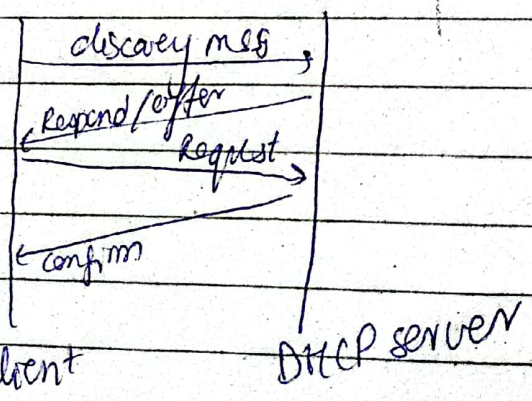
H = Host
R = Router

Date:

DHCP: dynamic host configuration Protocol:

It is a network management protocol used to dynamically assign IP ~~add~~ address to any devices or node on a network so that they can communicate using IP.

Device send request for an IP address that is picked up by a DHCP server. It respond by delivering it an IP address and then monitors the uses of the address and take it back after a specified time or when the device shut down.



NAT Network Address Translation:

it convert

Public IP address → Private IP address

Date:

The idea of nat it to allow multiple devices to access the internet through a single public address.

→ It also does translation of port no.

Generally the bordered ~~network~~ router is configured for NAT ie the router which has one interface in the local (inside) network and other interface global (outside) network. so when a packet ~~to~~ traverse outside the local (inside) network the NAT convert the ~~to~~ local (private) IP address to a global (public) IP address.

Datalink Layer and its Responsibilities:

it work with in a network

It take the data from network layer and give it to physical layer.

It is a link layer

Properties:

→ Hop to Hop delivery of mes

→ Flow control (speed)
- → stop & wait
- → Go back N
- → selective repeat

→ Framing

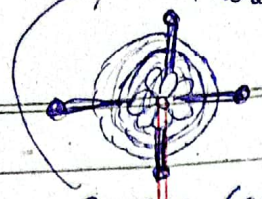
→ MAC

→ Error detection / Recovery
- → check sum
- → parity check

→ Error control (CRC, checksum, Parity)

CRC → Cyclic Redundancy Check

when multiple ... there is a high probability of collision. so CSMA/CD & CSMA/CA is used to avoid collision and loss of frame in the channel.



Date:

→ Access Control:
↳ (CSMA/CD, Aloha, Token)

→ Physical address (MAC) → responsible of addressing frames

→ divide data into frames and add header and tail with it. It also attach special bit (error control and addressing)

→ it's second layer from the bottom of OSI model

→ responsible for encode decode and organize the outgoing and incoming data.

→ it encapsulate the source and destination MAC addr / physical address in the header of each frame to ensure end to end delivery of msg.

Error Detection Techniques:

implemented either at data link layer or Transport layer

Popular techniques

1) Checksum
2) Parity Check → simple parity / → two dimensionality
3) Cyclic Redundancy Check (CRC)

Scanned with CamScanner

Date:

Parity

even parity
means 1's
even hony days

Odd parity
↓
1's should be
odd

→ Simple Parity Check:

- 1 is added to the block if it con
  odd number of 1's.
- 0 is added if contain even no

→ Two dimensional Parity Check.
↳ parity check bits are calculated b
for row and column

e.g

(A)	1 0 0 1 1 0 0 1	0	Row parities
(B)	1 1 1 0 0 0 1 0	0	
(C)	0 0 1 0 0 1 0 0	0	
(D)	1 0 0 0 0 1 0 0	0	
(E)	1 1 0 1 1 0 1 1	0	
column parities			

data send will be

(A)	(B)	(C)	(D)	(E)

↓
all in binary.

Scanned with CamScanner

Date:

⇒ Check sum:

1) The data is divided into k segment each of m bits
2) Sender end segments are added using 1's complement
→ The checksum is sent along with data segment
3) At Reciver end all recieved segments are added using 1's complement.
4) if result = 0
↳ the recieved data accepted
else
discarded.

⇒ Cyclic Redundancy Check CRC:

if there is remainder mean it indicates data is damaged therefore it is rejected
→ it can deted all odd errors, single bit, burst error of length equal to polynomial degree

D = division
R = Redunum bit
m = message into bit

1) R divisor
2) D → original data
3) length(R) − 1 zero's append LSB of D

Scanned with CamScanner

Date:

4) D/R

XOR → same → 0
diff → 1

0	0	0
0	1	1
1	0	1
1	1	0

Given
D = 1010110
R = 1001
4
so we will append 4-1 = 3 → 0

```
        1011
1001 ) 1010110000
       1001
       ----
       00111
        000
       -----
        1111
        1001
       -----
        01100
         1001
        -----
        01010
         1001
        -----
        00110
         000
        -----
         1100
         0001
        -----
         1101
```

→ CRC

all with bit parity
Cayman
1001
111 s
all

so we will add all if
remainder of 000
and then we
send to

Scanned with CamScanner

$R = x^3 + x^2 + 1$

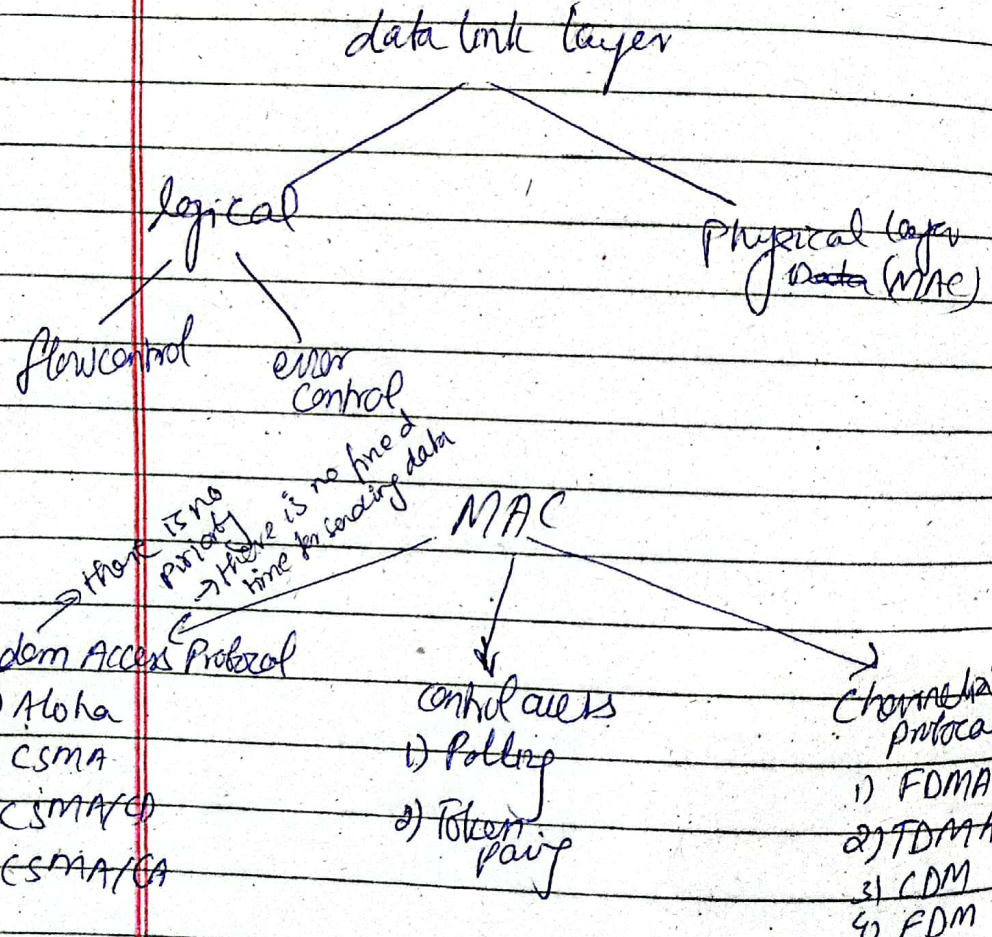
$\Downarrow$

$x^3 \quad x^2 \quad x^1 \quad x^0$

1 1 0 1

we donot have x^1 so we will put 0.

Medium Access Protocol (MAC) :-



MAC mechanism allows several users or transmitter to access a common medium or channel and to prevent data collision.

Date:

The data link layer is responsible for transmission of data b/w two nodes. H main fn are
→ data link control
→ Multiple access control (MAC)

→ responsible for reliable transmission of messages over transmission channel by using techniques like framing, error control & flow control.

Aloha:
It was designed for wireless LAN but is also applicable for shared medium. In this multiple station can transmit data at the same time and can hence lead to collision and data being garbled.

→ Pure Aloha:
When a station send data it wait for an acknowledgment. If ack doesn't come within the alloted time then the station waits for a random amount of time called back off time (Tb) and resend the data. Since different station wait for different amount of time the probability of further collison decreases

Date:

Vulnerable time = 2* Frame transmission time ~~OR~~ ~~Propagation~~ → Propagation time

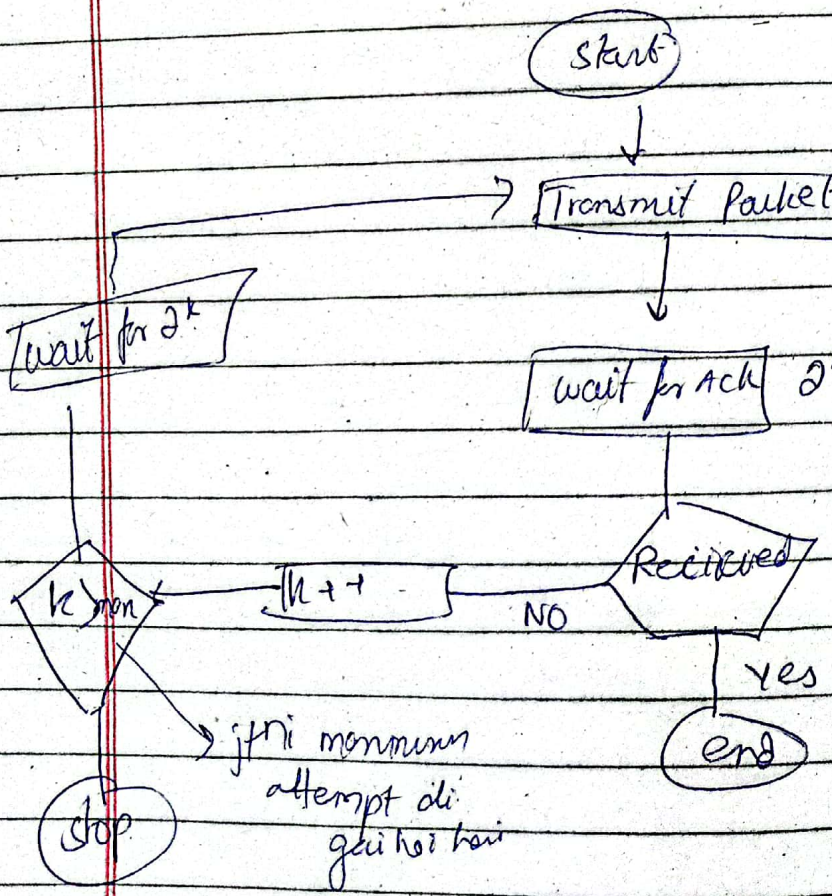
Throughput = G exp{-2*G}

maximum throughput = 0.184 for G = 0.5

~~Slotted Aloha~~

G = no of stations

1) Send frame
2) wait for Ack
   if doesnot recieve
3) Re transmit msg.



Scanned with CamScanner

Date:

→ ~~Slot~~

→ Slotted Aloha:

one slot = T_t

It is similar to pure aloha except th
we divide time into slots and sending of
data is allowed only at the begin
these slots. if a station ~~to~~ misses out
the allowed time it ~~to~~ must wait
the next slot. This reduces the probab
of collision

Vulnerable time = ~~Pkt~~ Frame ~~tt~~

Throughput = $G \exp\{-G\}$.

maximum throughput = 0.368 for G=1

Token passing: → A channel access method where called token is passed btw nodes th that node to communicate. It ensu that not all participants send data to a

A station is authorized to send data
it recieve a special frame called toke
→ when a node recieve a token it holds
the token only if it has some frames t
transmit otherwise it immediately
the token to the next node.

problem:

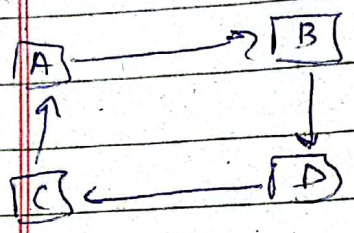
the failure of one node can crash
entire channel

Scanned with CamScanner

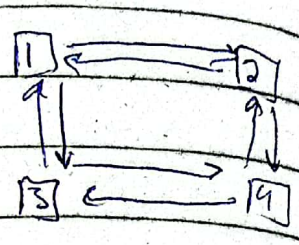
Date:

types of token passing

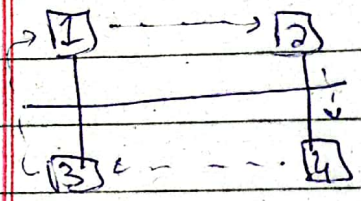
1) Physical ~~Rg~~ Ring



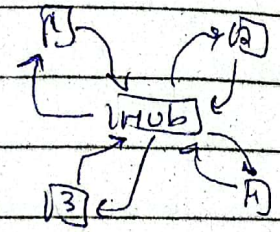
2) Dual Ring



3) Bus Ring



4) Star Ring



Polling:

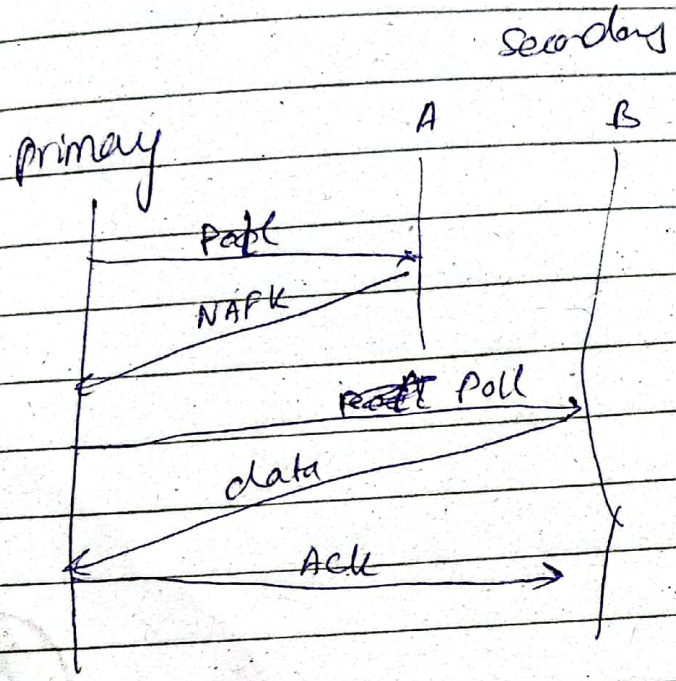
in come in control access protocol.

→ In this one acts as primary station (controller) and the other are secondary stations. All the data exchange must be made through the controller.

→ The msg contain the address of node all nodes receive msgs but only ~~that one respond~~ the addressed one respond if there is no data poll reject (NAK)

Scanned with CamScanner

Date:



$$\text{efficiency} = T_t / (T_t + T_{poll})$$

FDM: frequency division multiplexing:

Multiplexing is a technique used to combine and send the multiple data stream over a single medium. The process of combining the data stream is known as multiplexing and hardware use for multiplexing is multiplexer.

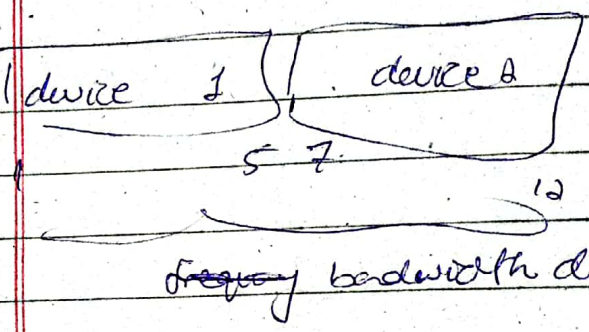
In FDM the available bandwidth of a single transmission medium is subdivided into several channels

The main aim of the FDM is to subdivide the available bandwidth into different frequency channel and allocate them to different devices.

Scanned with CamScanner

Date:

FDM is mainly used in radio broadcast and TV network

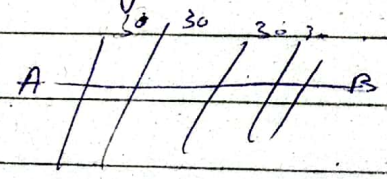


~~frequency~~ bandwidth divided

TDM:

Time division multiplexing

is ma communication medium ko time frame ma divide kia jata hai



In TDM the total time is ~~divided and~~ distributed among different users. therefore each user is allocated with different time interval know as timeslot.

→ the difference is that in synchro many slots are unutilized in Asynchro slots are fully utilized

TDM have two types

1) Synchronous TDM:
↳ in it time slot is preassigned to every device

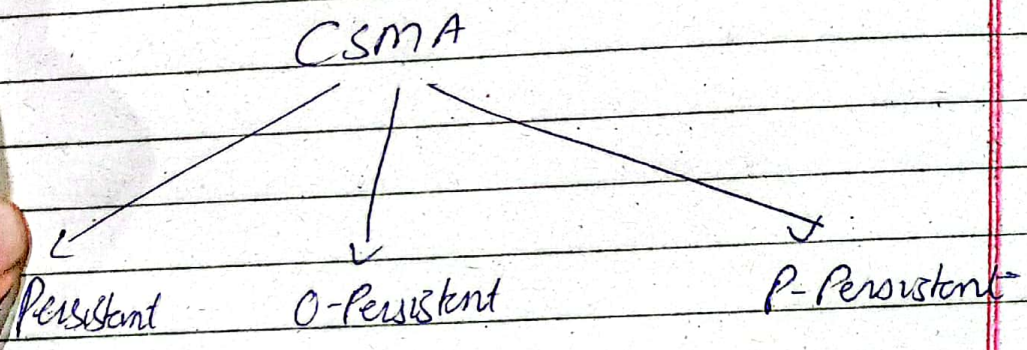
2) Asynchronus TDM:
↳ in it timeslots is are allocated to only those device which have data to sed

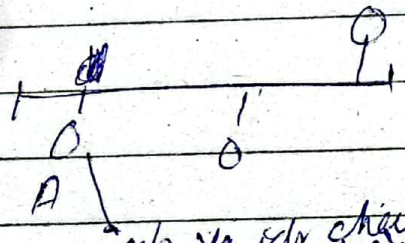
Date:

In FDM all signals operate at the same time with different frequency but in TDM all signals operate at the same frequency with different time

CSMA:

Carrier Sensor Multiple Access





Jab ya idle ~~signal~~ sense karey gya ka is ka ~~agay koi data~~ signal hai ka nhi agar nhi hai to ya data send karey gya CSMA ka kaam hai

~~1-Persistent~~:

CSMA ensure fewer collision as the station is required to first sense the medium if its busy it will wait for idle and then ~~to~~ it will send data.

Date:

1 persistent:

Ya channel ko check karta hai ka wo free ha ka nhi agr free ha to theek ha msg snd kar dayta warna ya lagatar continously check karta rahta hai ka channel free hai ~~tha~~ ha ka nhi

Here there are high level of collision

0-persistent:

if the medium is busy it will wait for a random amount of time and after the time will finish it will snd the data.

P-Persistent:

The node sense the medium if idle it send the data with p probability. if the data is not transmitted ((1-p) probability) then it wait for some time and again check the medium if idle it send data.

→ it is used in wifi & packet radio system

CSMA/CD: → collision detection

→ there is no ack

→ jis time pa transmission kar raha ho aur agr us time hi collide data ay to tab hi pata lag sakta ha ka data collide ho gaya hai

Date:

agar collide data wapis aay aur us time pa-
(A) transmission na kar raha ho
to usay pata nhi lagega ka ya data
kis ka hai

CSMA/CA: → collision Avoidance

it is used in WLAN.

→ it involve sender receiving ack signal.
if there is just one signal (its own) then
the data is successfully sent but if there are
two signal (its own & the one with which
it has collied) then it means collision has
occured

It avoid collision by

i) Interframe space:
Station wait for medium to become
idle when it finds it idle is doesnot directly
send data it wait for period of time called
interframe space IFS. after this time it again
check medium for being idle. IFS depend
on priority of station.

2) Contention Window:
It is ~~amount~~ amount of time divided
into slots. if the sender is ready to send data it choose
a random no of slots as wait time which

double every time medium is not found idle. if the medium is found busy it does not restart the entire process rather it restart the time when the channel is found idle again

3) Ack:

The sender retransmit the data if ack is not recieved before time-out

CDMA:

Code division multiple access.
is a sort of multiplexing that facilitates various signal to occupy a single transmission channel
It optimize use of available bandwidth.
It is different from time and frequency ~~multi~~ multiplexing. In it the user has the access to the whole bandwidth for the entire duration
→ one channel carries all transmission simultaneously

Date:

Network layer ⇒ forwarding the packet

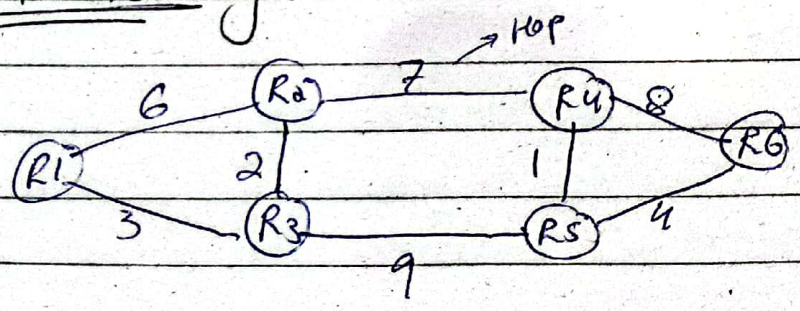
Routing Protocol

- intra domain
  - Distance Vector (RIP)
  - Linkstate (OSPF)
- Interdomain
  - path vector (BGP)

These all protocol work in unicasting

Link State Routing:

R = Router



we use it so that router can make its Routing table

It is an interior protocol used by every router to share the information or knowledge about the rest of routers on network.

→ router share knowledge of every ~~router~~ router to

K → Router is mai aik hello msg and doosray ko hello msg bhej kar unka dhaakhy lain kar kis ka sath connect hai aur distance kia hai

Step 1: making link state table

seq no

TTL

R1	
R2	6
R3	3

R3	
R1	3
R2	2
R5	9

R5	
R3	9
R4	1
R6	4

R1	
R5	4
R4	8

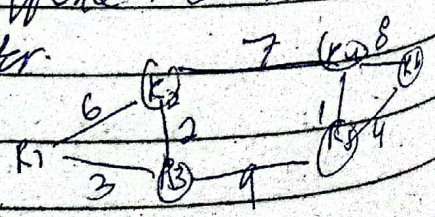
R2	
R1	6
R3	2
R4	7

R4	
R2	7
R5	1
R6	8

Step 2: ab in ko aik doosray ka sath share kary gain

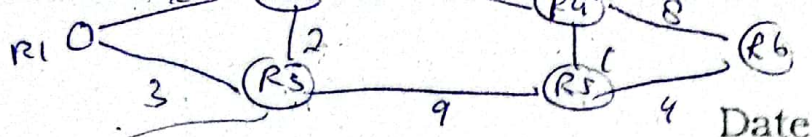
→ In link state routing we do flooding
→ bandwidth aur congestion zyada istemal ho gi idhr

Global knowledge → Har router sari information aa gai ka kun kis ka sath connect hai aur sequence ma ha
↳ it is not in distance vector



~~Step~~

flooding → Hrs R3 flooding



Date:

Step:

Now we will apply dijkstra Algorithm

$R_3 \to R_2 + 2 = 2+3=5$

	R_2	R_3	R_4	R_5	R_6
R_1	6	3	∞	∞	∞
R_1R_3	5	3	∞	9+3 12	∞
$R_1R_3R_2$	5	3	7+5 12	12	∞
$R_1R_3R_2R_4$	5	3	12	12	~~20~~ 21
$R_1R_3R_2R_4R_5$	5	3	12	12	16 → 12+4

Now Routing table of R_1

		via → kis ka through jaa rha hai
R_1	0	R_1
R_2	5	R_1
R_3	3	R_1
R_4	12	R_3 R_2
R_5	12	R_3
R_6	16	R_3 R_5

jis ki help ka kar hum ~~do~~ main router pa pooncha rahe ~~hai~~ hain

⇓

This is routing table of R_1. Now like this we have to make for all those router which are ask in question.

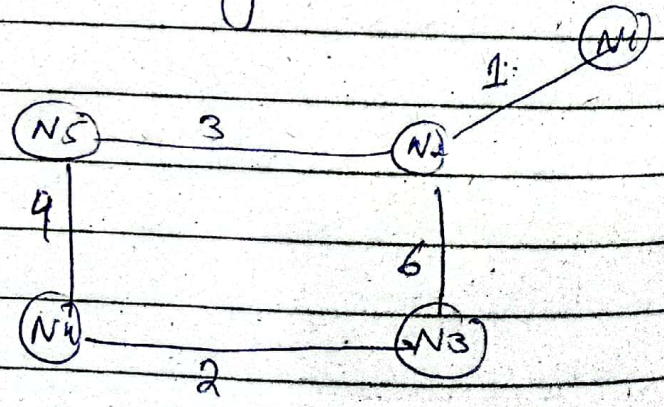
Date:

Distance Vector Routing : (DVR)

It work by having each router maintain a routing table giving the ~~best~~ best ~~kno~~ known distance from source to destination and which route is used to get there.

It is an asynchronous algorithm in which nodes x send the copy of its distance vector to all its neighbor. When ~~nes~~ node x receive the new distance vector from one of its neighboring vector v, it saves the distance vector of v and uses the Bellmanford equation to update its own distance vector.

→ every Router will know that is network me total kitna router hai



Step 1: making local routing table

Date:

Table. → jidhar direct link hai wo likhy gaye

$N_1 \Rightarrow$

Dest	Dist	Next
N_1	0	N_1
N_2	1	N_2
N_3	∞	—
N_4	∞	—
N_5	∞	—

$N_2 \Rightarrow$

Dest	Dis	Next
N_1	1	N_1
N_2	0	N_2
N_3	6	N_3
N_4	∞	—
N_5	3	N_5

$N_3 \Rightarrow$

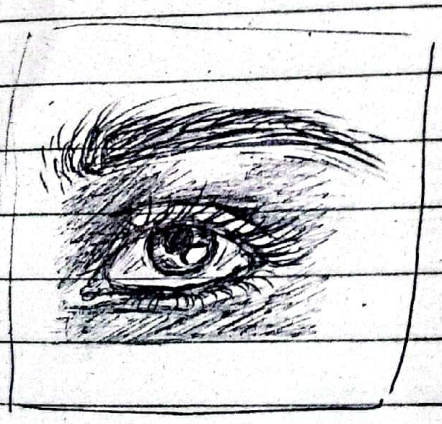
Des	Dis	Next
N_1	∞	—
N_2	6	N_2
N_3	0	N_3
N_4	2	N_4
N_5	∞	—

$N_4 \Rightarrow$

Des	Dis	Next
N_1	∞	—
N_2	∞	—
N_3	2	N_3
N_4	0	N_4
N_5	4	N_5

$N_5 \Rightarrow$

Des	Dis	Next
N_1	∞	—
N_2	3	N_2
N_3	∞	~~N3~~
N_4	4	N_4
N_5	0	N_5



PTO

Scanned with CamScanner

Date:

Step2:

→ we will share only ~~neighby~~ neighbours

→ and only its distance vector. not whole table

At N_1 — N_2

At N_3 — N_2, N_4

At N_5 — N_2, N_4

At N_2 — N_1, N_3, N_5

At N_4 — N_5, N_3

Step3: we will ~~do~~ update.

that from diagram.

At N_1

N_2

N_1	1
N_2	0
N_3	6
N_4	∞
N_5	3

N_1 New Routing table

Dest	Dist	Next
N_1	0	N_1
N_2	1	N_2
N_3	7	N_2, N_3
N_4	∞	–
N_5	4	N_5

$N_1 \to N_2$ & $N_2 \to N_1$

$1 + 0 = 1$

$N_1 \to N_2$ & $N_2 \to N_3$

$1 + 6 \Rightarrow 7$

$N_1 \to N_2$ & $N_2 \to N_4$

$1 + \infty = \infty$

Scanned with CamScanner

Date:

parallely baki sarro ka bhi
bun gay kain

Direct is that
for e.g N4 to all Routes

Dest	Dis	Nexto
N1	8	N1
N2	7	N2
N3	2	N3
N4	0	N4
N5	4	N5

bus direct likno jo bhi shortest path ha wo likho

Principle of Data Security:

TCP

OSI
↳ Application
Presentation → Encryption, compress code
Session

Security:

In computer science security is to secure the integrity, availability and ~~confederiality~~ ~~confid~~ confidentiality

Scanned with CamScanner

Date:

of information system resources (include hardware, software, data, firmware etc.

yamss pass jay which device ka to authorized device hai.

(Authorized access optional.

Security →

C — Confidentiality

I — Integrity

A — Availability

Confidentiality:

The principle of keeping sensitive information private unless the owner give access to share it with other party.

e.g account information

Integrity:

Data or information in your system is maintained so that it isnot modified or deleted by unauthorized parties.

for e.g sender send msg so it should be recieve only by reciver not any one else

Date:

Availability:

It is that the data should be available to users when they need.

e.g. authentication service

Encryption

Symmetric key Encryption

→ ~~private key en~~ key

→ private key encryption

→ Ceaser Cypher

→ Mono Alphabetic

→ Poly "

→ Des

→ 2DES + 3DES

Assymeric key encryption

→ public key encr (RSA)

PTO

Scanned with CamScanner

Date:

Cryptography:

to convert
plain text ⟶ Cypher text
⟵
↓
secret msg

we use to achieve confidentiality

[M]
Plaintext ⟶ [Encryption] ⟶ cipher text ⟶ [Decryption] ⟶ Pl
↓key
M'
cipher text
↓
M' → M

Symmetric , Asymmetric
↓
same key
means jis key
sa encrypt hua
usi sa decrypt hoe

Symmetric key Cryptography:

DES ⇒ data encryption standard
AES ⇒ advance " "

DES ⇒ 56 bit
3DES = 192 bit
AES ⇒ (128 bit , 192, 256 bit)

Scanned with CamScanner

Date:

Substitution ~~Cypher~~ Cipher technique:
to convert plain text → Cipher
Techniques

1) Ceaser Cipher:

It is an encryption technique.

	A	B	C	...
	0	1	2	...

eg plain text

[Hello] if key = 3

H	E	L	L	O
↓	↓	↓	↓	↓
ijk	fgh	mno	mno	pqr

[k h o o r]

Cipher text

→ mean H ka agay jo 3 alphabet aya hai (abc) ma wo likho
↓
alphabets.

A L i = plain text
bcd mno jkl

[d o l] ~~eg~~ cipher text.

→ It is ~~eg~~ easily decrypted

Date:

2) a) Mono alphabetic Cipher:

permutation:

→ technique that determine the possible arrangment of set

e.g $S = \{a, b\}$

ab

ba

→ is ma aik letter ka bhi random alphabet lay gai lekin that ga

for e.g

A → X

L → Y

L → Y

plain text → cipher text

ith if we will do random mapping

for e.g

A → X

L → C

I → D

plain text → cipher text

} kisi bhi random no sa replace kar do

for cracking of this we use brute force technique

Poly Alphabetic Cipher: (Vigenre Cipher)

kisi bhi random ~~Ab~~ number sa ~~replace~~ replace karo ga ~~aur~~ agr same letter ~~ka~~ rahta hai for e.g Hello, to m dono ~~ka~~ ka kia different ~~aq~~ alphabet use karo ga jis ka mano waly mer same use karta than

25 mod 26

25 26 Date:

A	B	C	D	- - -	Z
0	1	2	3		25

0	A
1	B
2	C
3	D
4	E
5	F
6	G
7	H
8	I
9	J
10	K
11	L
12	M
13	N
14	O
15	P
16	Q
17	R
18	S
19	T
20	U
21	V
22	W
23	X
24	Y
25	Z

Encryption:

$$C = (P + k) \bmod 26$$

decryption:

$$P = (C - k) \bmod 26$$

for Eg

Key : Hello Hellos

Plaintext : muhammadali

Ciphertext : TYSLATEOLZA.

	H	E	L	L	O	H	E	L	L	O	S
key:	7	4	11	11	14	7	4	11	11	14	18
PT :	12	20	7	0	12	12	0	3	0	11	8
CT :	19	24	18	11	0	19	4	14	11	25	0

$= (7 + 12) \bmod 26$

$= 19 \bmod 26$ $\quad 26 \sqrt{19}$

Scanned with CamScanner

PC = Permutated choice

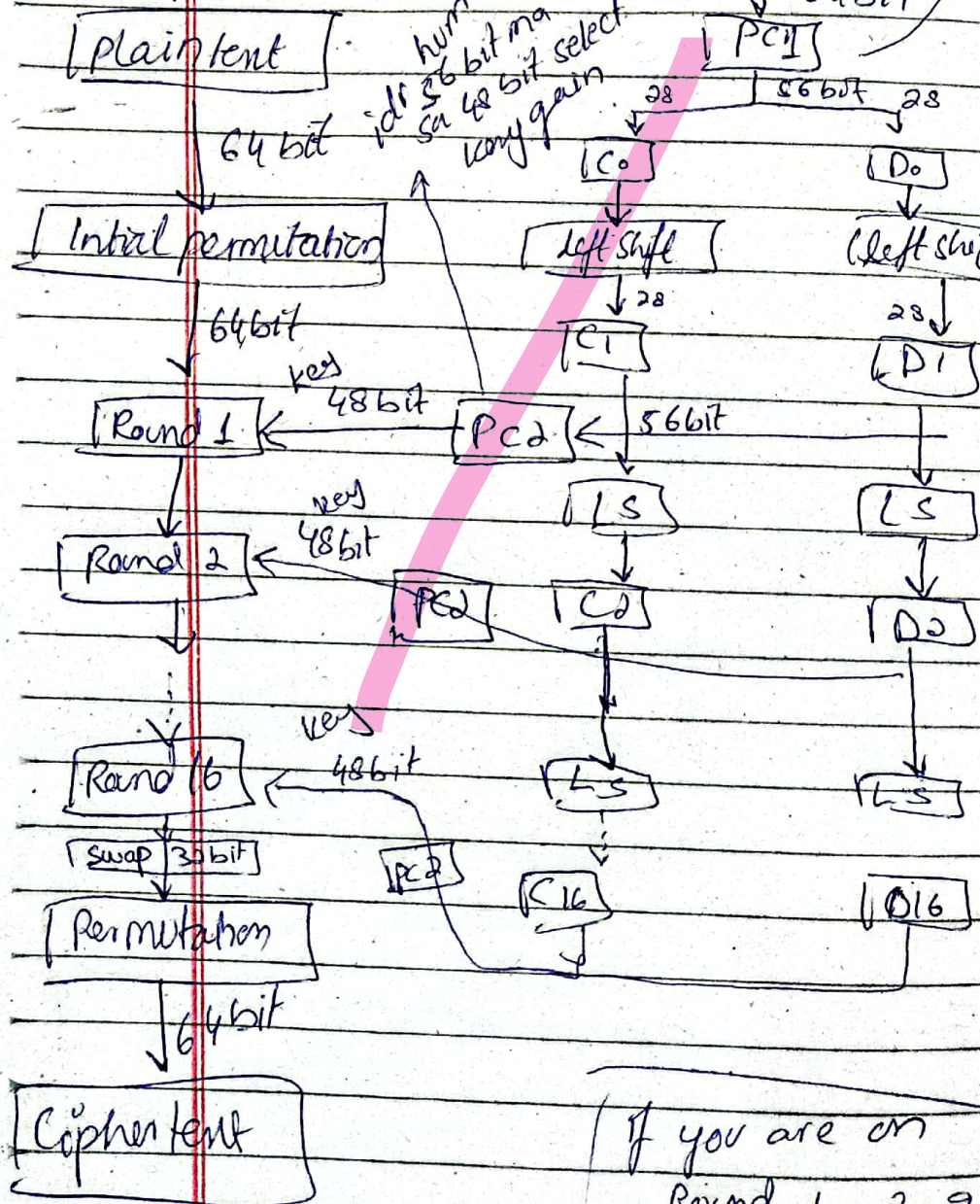
LS = Left Shift

Date:

DES:

It is a block cipher
intial key = 64 bit
plain text = 64 bit

Data encryption Standard algorithm



hum jdi 56 bit ma sa 48 bit select karny gain

If you are on Round 1, 2, 9, 16 will shift one bit in left shift

other than these round we will shift

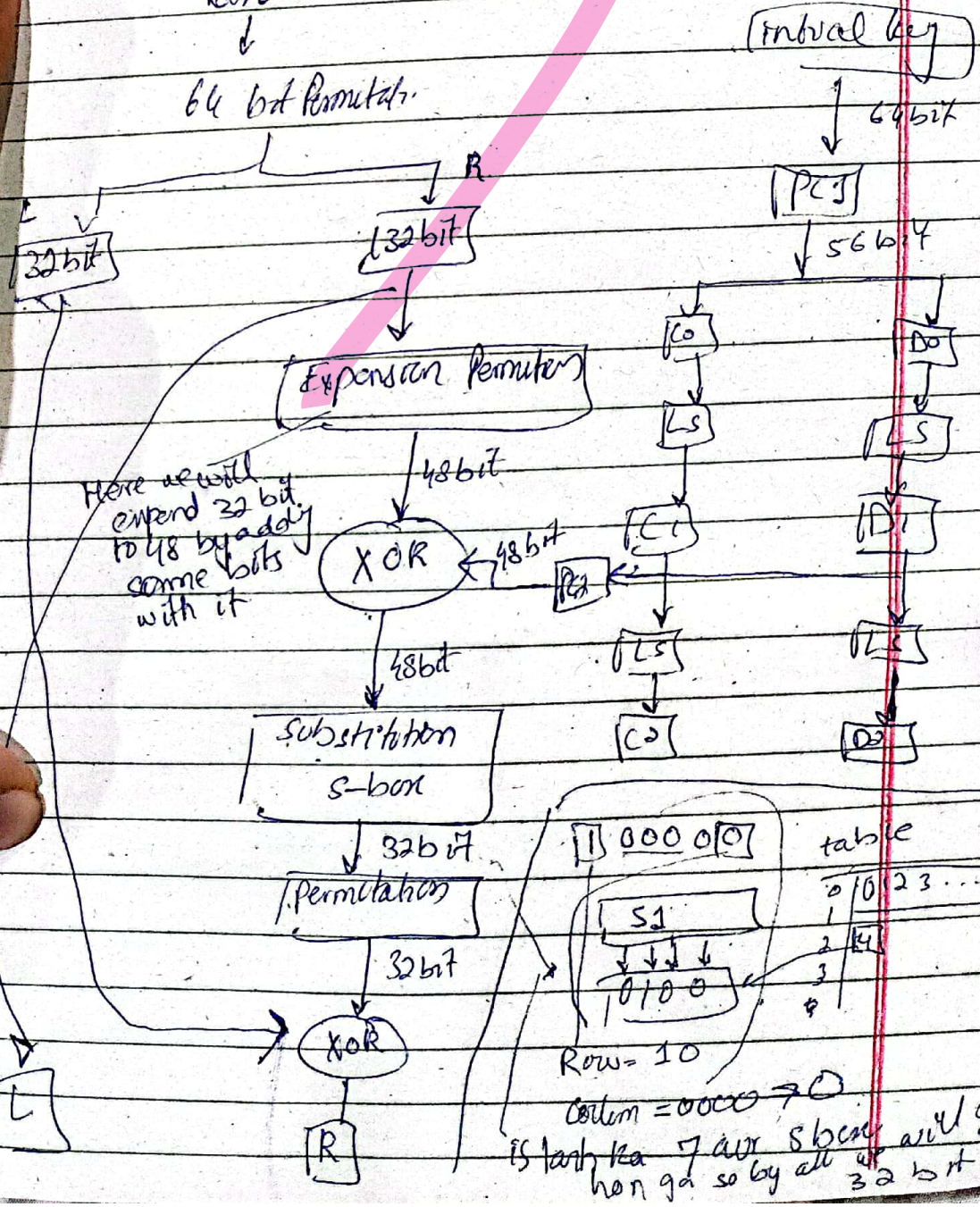
Date:

This 48 bit key will be different for every round

Now understanding Round function

~~Round~~

Round 1



is tarah ka 7 aur sbox and get hon ga so by all of 32 bit

Scanned with CamScanner

Date:

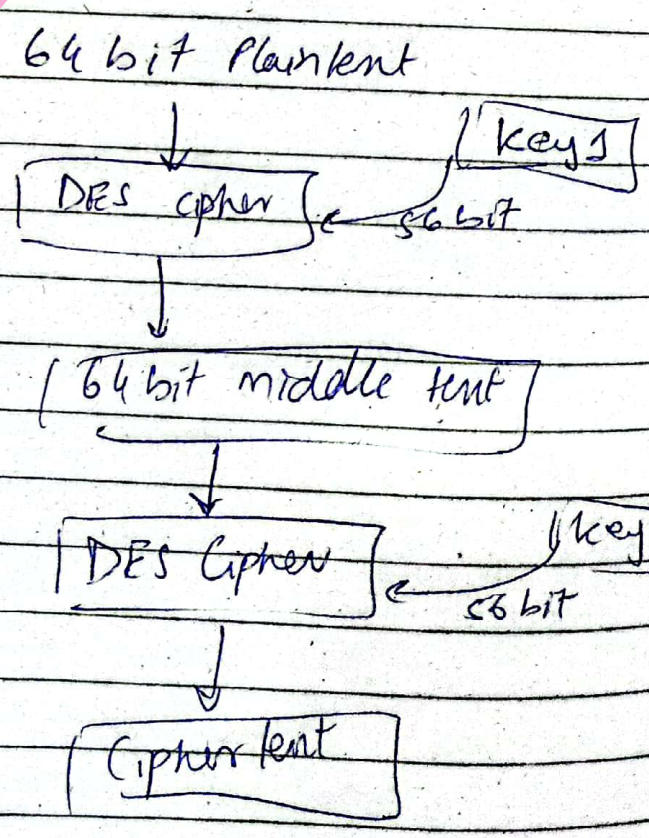
2DES:

Since DES attack was easily cracked by very brute force attack that's why ~~the~~ new variation of DES were introduced.

double des.

→ use 2 different keys
(56 + 56) = 112 bit key

→ double encryption occur here

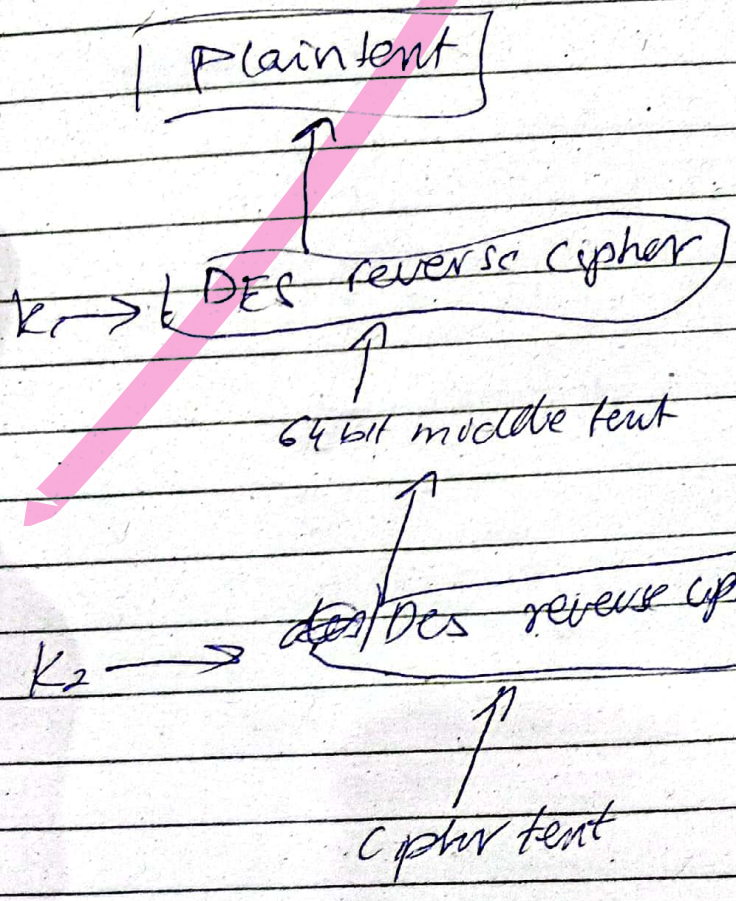


Scanned with CamScanner

Date:

⇒ for decryption
1st decrypted using (key 2) and then key 1.

for decryption



Scanned with CamScanner

K = key

Date:

3 DES:

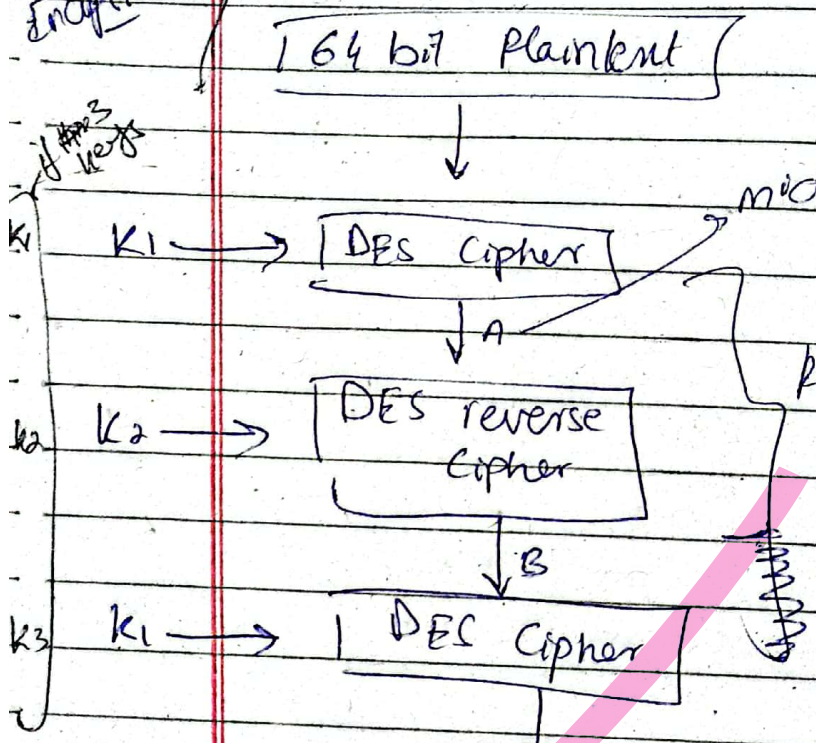
if two keys now if 3 keys we use K_1, K_2, K_3

→ 2 or 3 keys are used

→ much stronger than double DES

Encryption

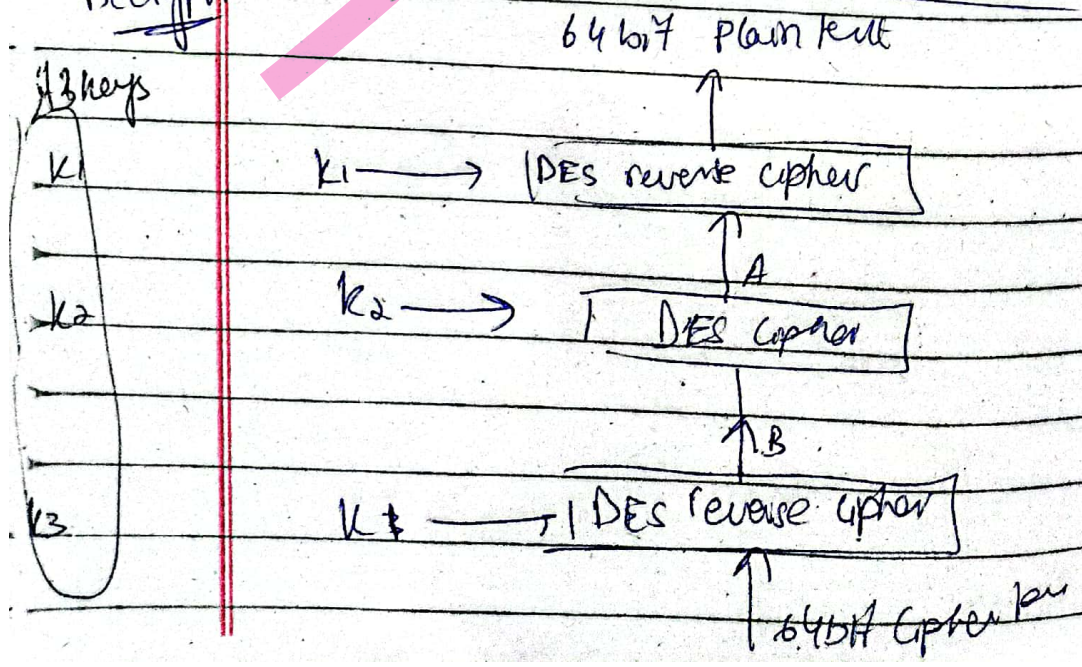
if 3 keys



keys should be different else result will be same.

Decryption

if 3 keys



Scanned with CamScanner

Date:

AES: Advanced Encryption Standard

→ symmetric key block cipher
(ie same key used for encryption and decryption)
→ more secure than DES
→ fixed block size = 128 i-e 16 bytes = 4 words

1 word = 32 bit

Round	no of bits in key	
10	128	AES 128 version
12	192	" 192 "
14	256	" 256 "

→ no of keys generated by key expansion algorithm = (no of rounds + 1)

bit → 0 or 1

1 byte → group of 8 bits
1 word → 4 byte ⇒ 32 bit
Block size → 128 bit data

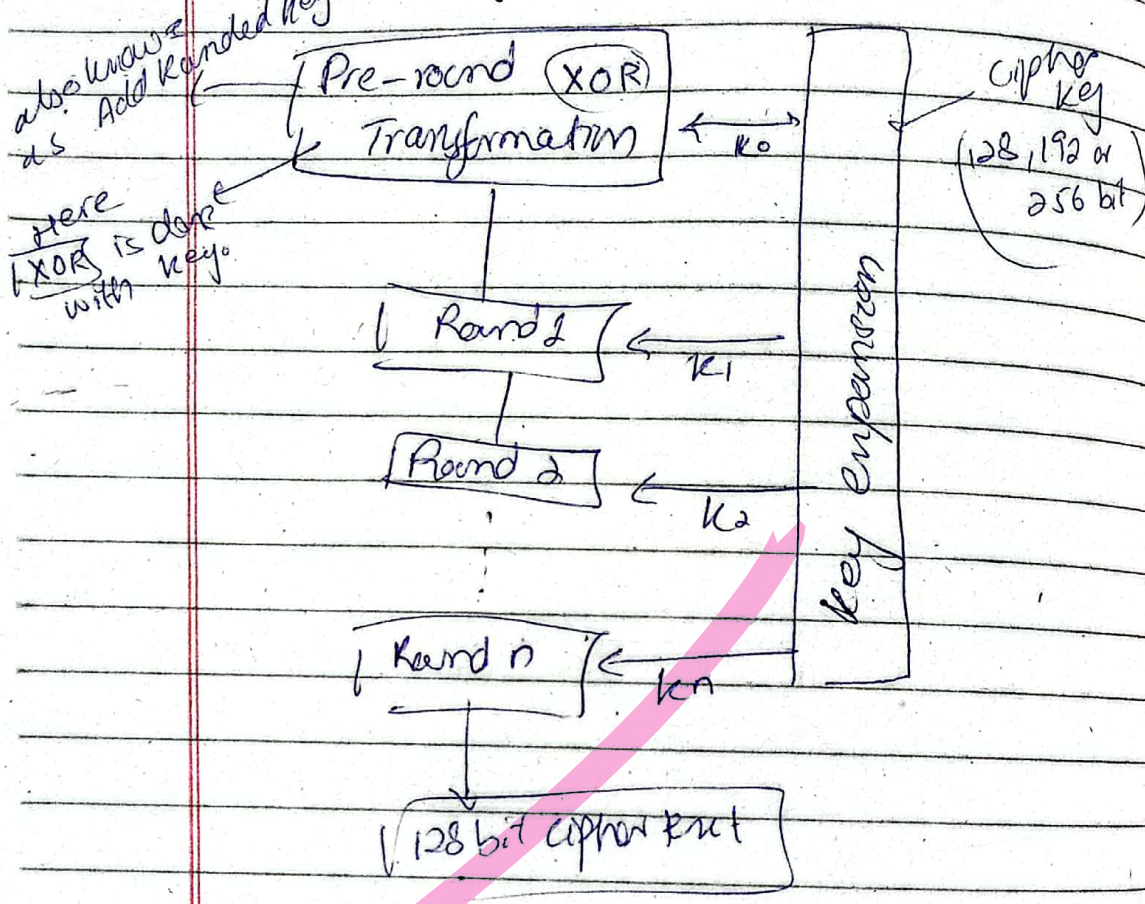
State: → matrix
16 bytes (4x4)
stories intermediate results

Scanned with CamScanner

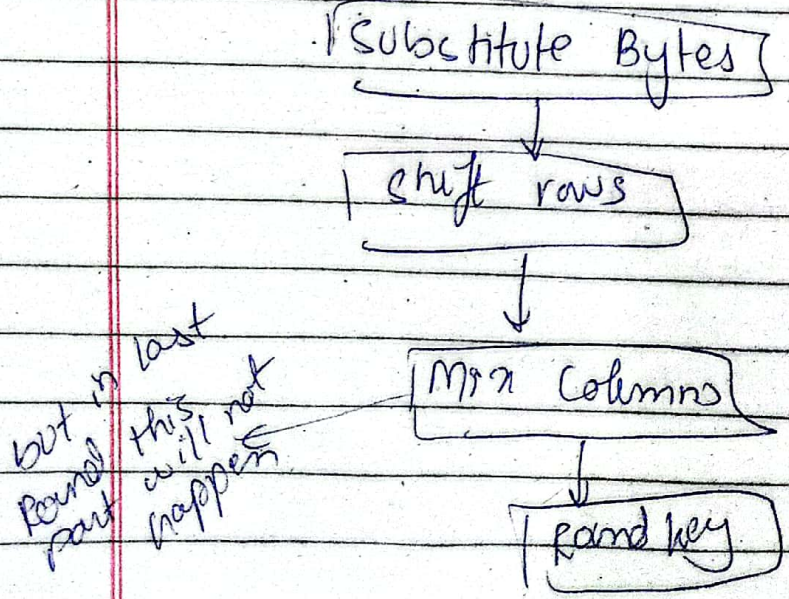
1 word = 32 bit

Date:

General Design of 128 bit plain text AES encryption

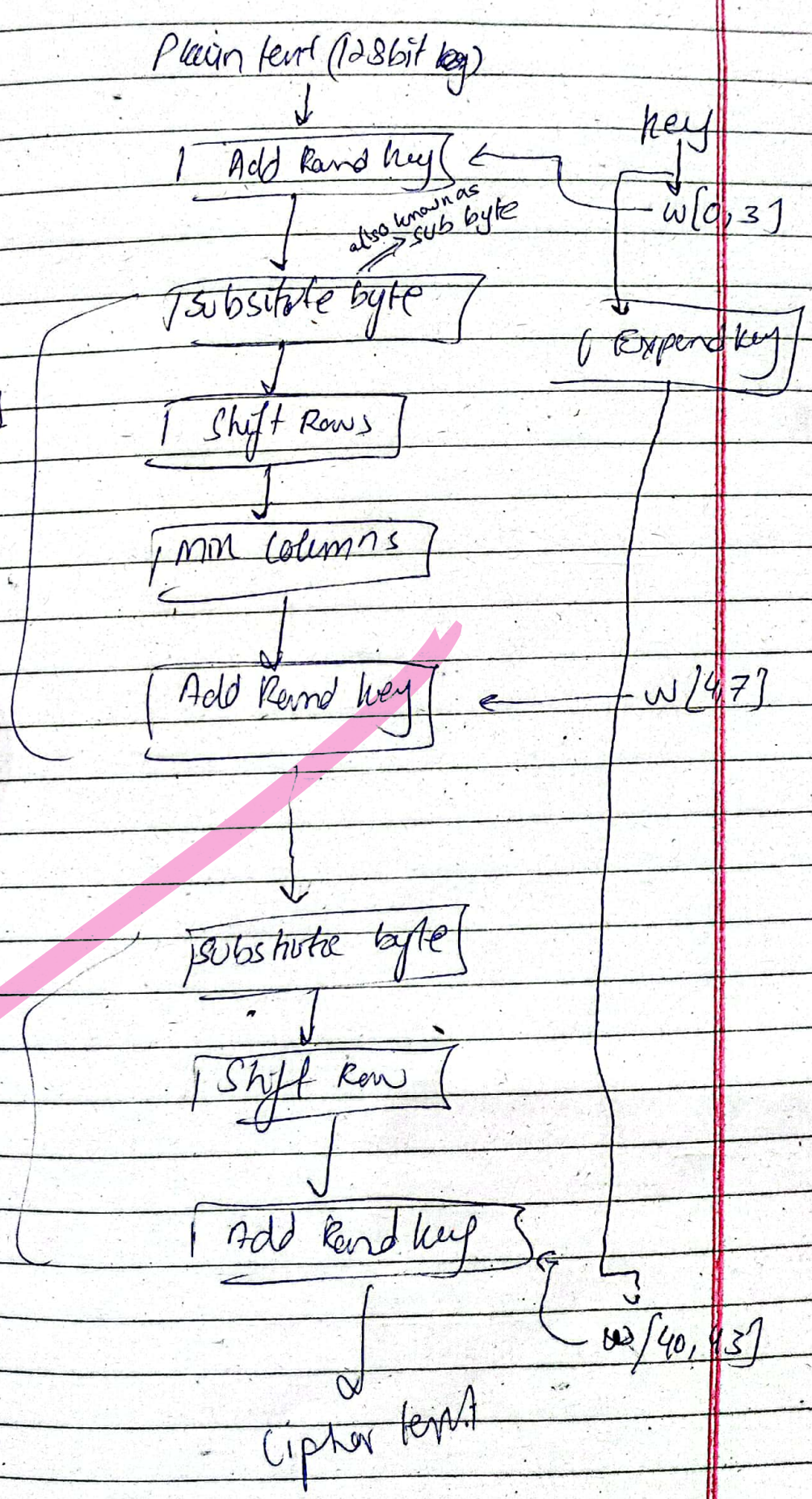


now in each Round.



Scanned with CamScanner

Date:



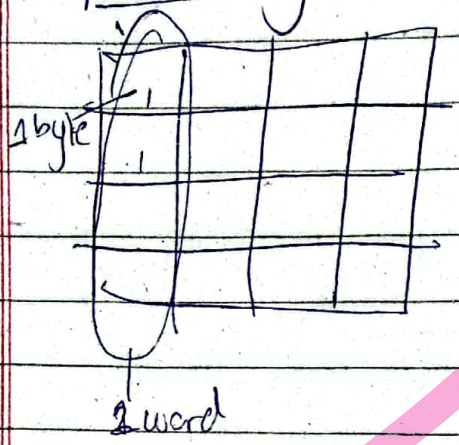
Scanned with CamScanner

128 bit Semarwe.

Date:

⇒ Input Array 4x4 i.e 16 byte i.e 128 bit or 4 words

1 word = 4 bytes



⇒ State Array (4x4) 16 byte ⇒ 4 word

Stores the intermediate result

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$
w_0	w_1	w_2	w_3

1st bytes of 0 word.

2nd bytes of 3rd word.

⇓

$[w_0 \; w_1 \; w_2 \; w_3]$

⇒ Key

w_0	w_1	w_2	w_3
k_0	k_4	k_8	k_{12}
k_1	k_5	k_9	k_{13}
k_2	k_6	k_{10}	k_{14}
k_3	k_7	k_{11}	k_{15}

expand key algorithm →

w_0	w_1	.....	w_{43}

44 words

Scanned with CamScanner

Date:

Transformations

4 types

substitution, permutation, mixing, keyadding

Substitution:

AES use same mechanism like DES but here substitution is done for each byte

Subbyte.

we interpret the byte as 2 hexadecimal digit

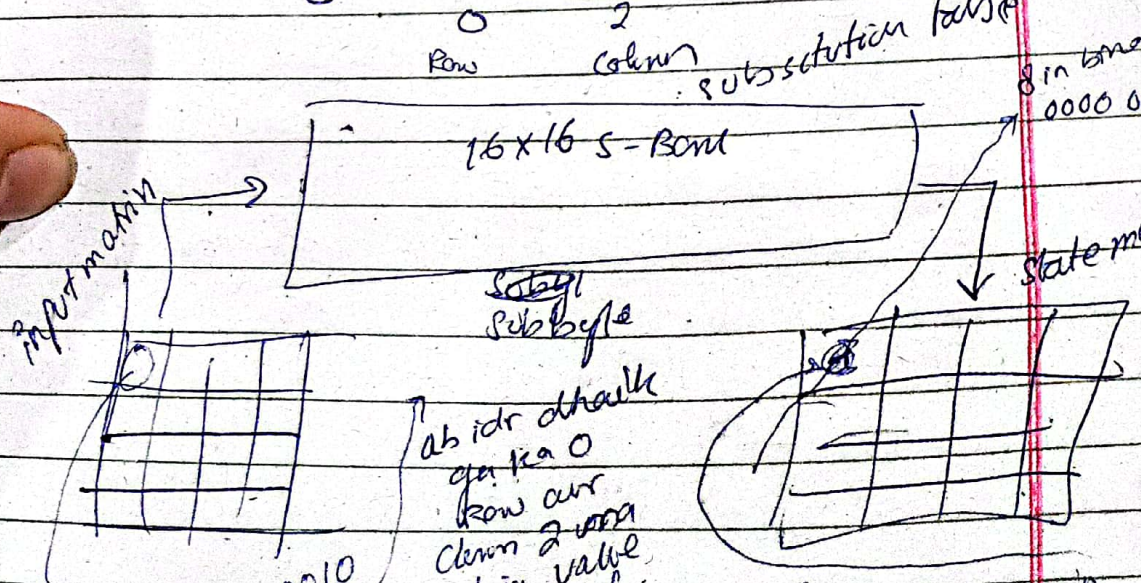
1st hexadigit → row

2nd hexa digit → column

transformation is done one byte at a time

eg 00000010

0 (Row) 2 (column)



Date:

Permutations

2) Here permutation will be done in byte level in DES we have done at bit level.

Shift Rows :

→ Shifting is done to the left

→ no of shift depend on the row of the state matrix.

⇒ for Row 0 there will be no shift

⇒ for Row 1 ⇒ Shift 1 byte

Row 2 ⇒ Shift 2 byte

⋮

like this it will go.

for eg

b0	b1	b2	b3
b4	b5	b6	b7
b8	b9	b10	b11
b12	b13	b14	b15

shift row shift left ⇒

b0	b1	b2	b3
b5	b6	b7	b4
b10	b11	b8	b9
b15	b12	b13	b14

1 byte shift

2 byte shift

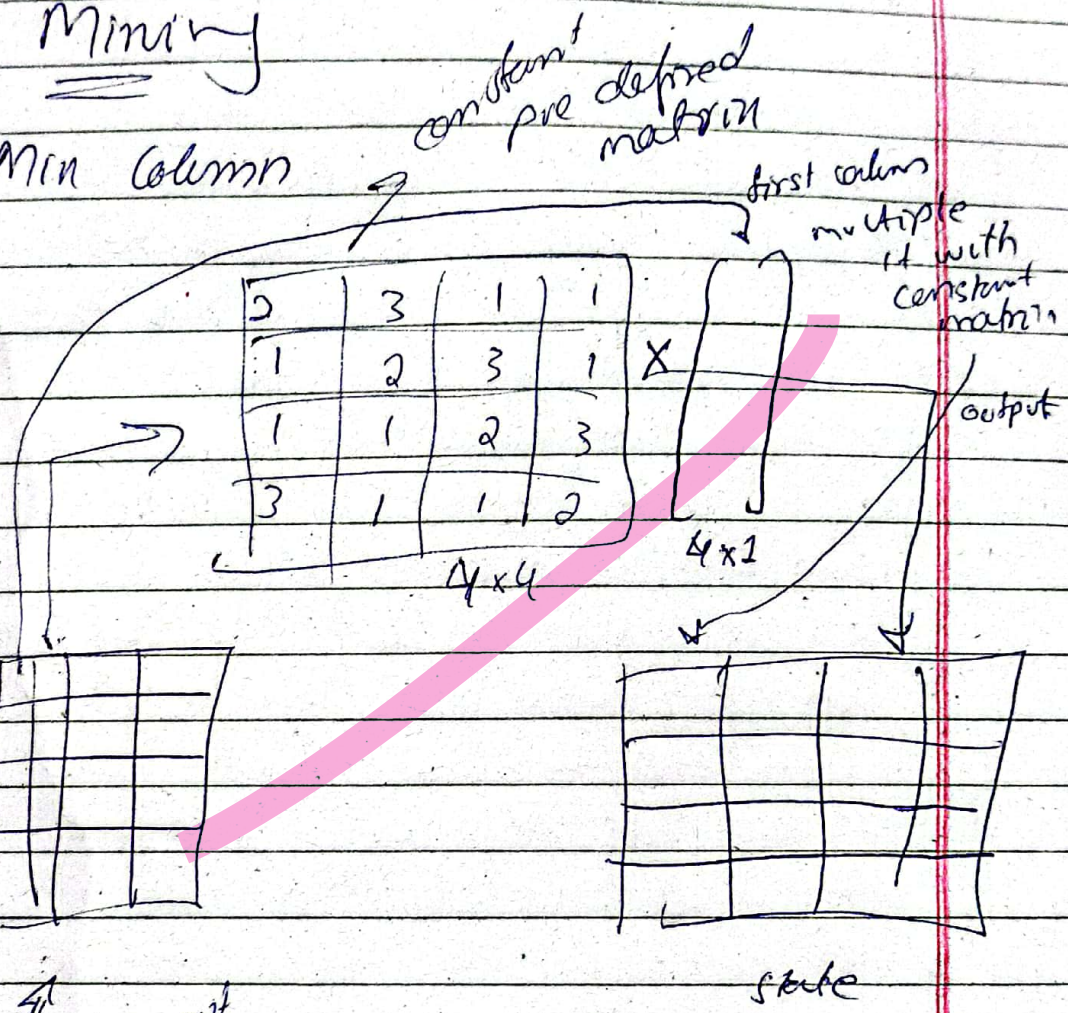
3 byte shift

Scanned with CamScanner

Date:

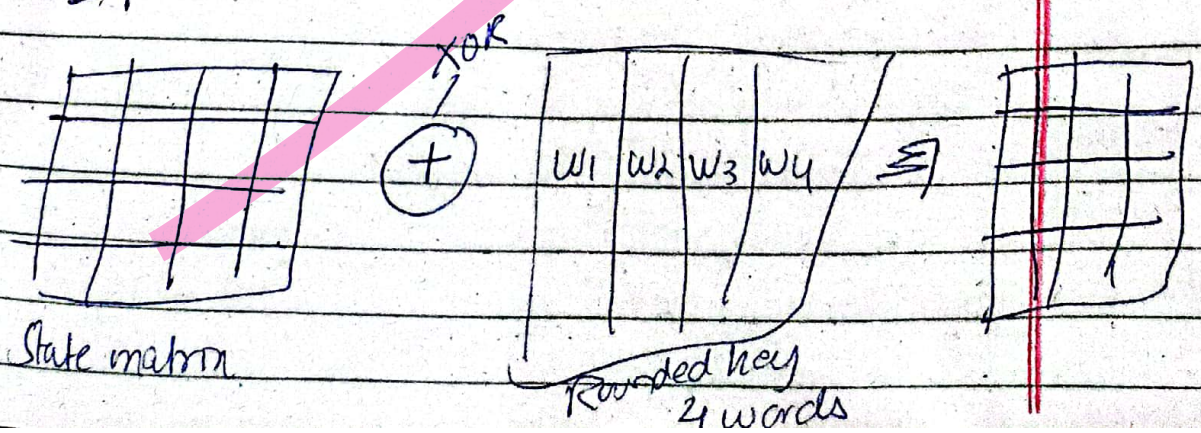
3) Mixing

Mix Column



4) Key Adding / add rounded key

→ proceed 1 column at a time



Scanned with CamScanner

Date:

so first we get plain text it is xor with key0 now the key is 128 bits key is passed through key expansion algorithm. over there key is passed to state array there 4 words are made from that key and these 4 words are expanded to 44 words in 128 bit senarue. each round is passed with 4 words in each round we substitute bytes then shift rows and then mix colums in the end we xor it with rand key. In the last round we donot do mix column.

→ now is substitution the input matrix is passed from ~~there~~ that matrix we take each byte ~~fe byte~~ ~~data~~ data from 1 byte is broken into two parts from that we know the row and column and then from Sbox we take the data of that row and column and then pass is to state matrix like this we do for all byte.

⇒ now state matrix is passed to shift row here rows are shifted first row is not shifted we shift row to left Row 1 = Shift 1 byte

Row 2 = " 2 byte

Date:

like ~~thi~~ this and then we pass it to ~~Ate~~ State matrix.

→ Now this state matrix is pass to mixing column here it is ~~meat~~ each column is multiple with a predefined matrix and output is store in state matrix

→ Now this state matrix is XOR with rounded table ~~they~~ this process is known as key adding.

like this ~~if~~ this whole process take place in each round.

SSL : Secure socket layer

→ it is between application layer and transport layer.
application layer sa cheez SSL ma aati hai

→ use for data security
it provides
→ integrity → data tampered na ho
→ Authentication
→ Confidentiality → no one else should approach data

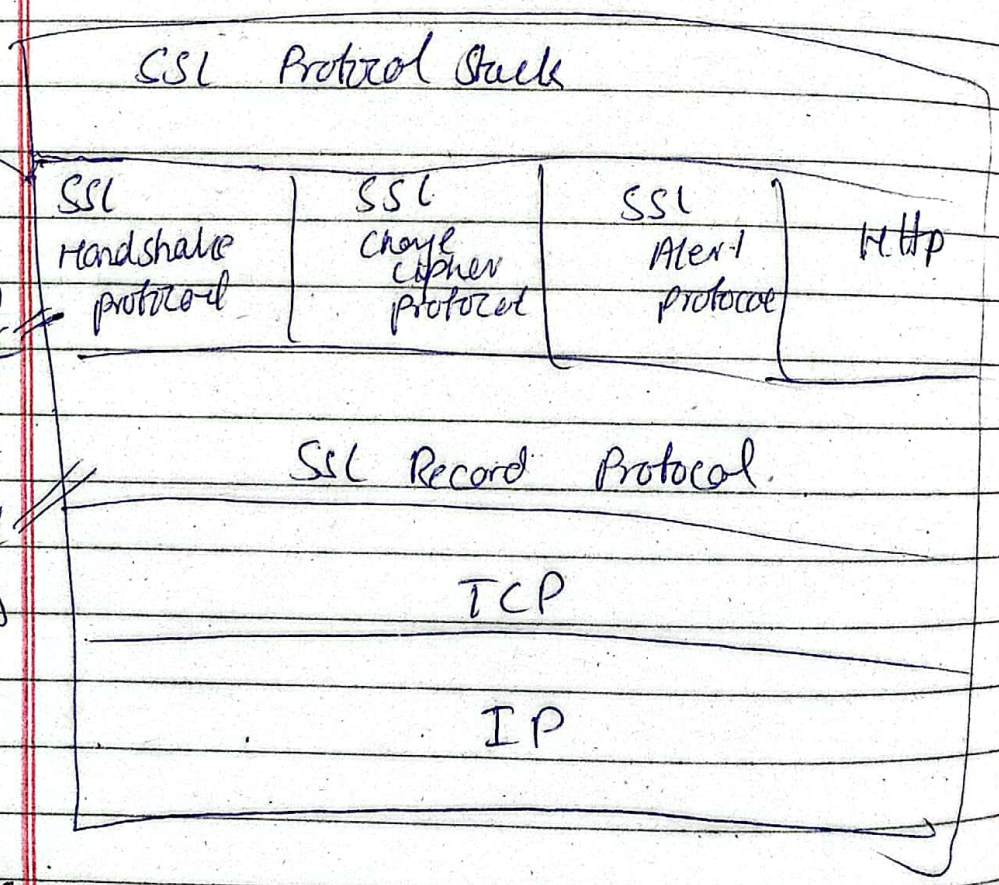
When the data is recieved ~~from~~ to

Date:

SSL from application layer
it encrypt the data and ~~and~~
add SSL Header with it

⇒ ~~TLS~~ TLS do the same work but
it perform this process in Transport
layer.

SSL Header



TLS : Transport layer Security.
Same as SSL but it
is done in Transport
layer

Date:

Digital Signature:

The proof in the hand of the reciever that the data is recieved from the authentic resource.

How it work

Consider a senario

A want to send data to B

A B

⇒ A will use it private key to generate a digital signature through some digital signature generation algorithm

⇒ Then A will append that digital signature with message and send it to B.

⇒ Now B will decript the message/signature with A public key if it decript successful then B will know that the msg is recieve from B other wise he will know that msg is not from an authentic source.

Scanned with CamScanner

Date

Fire wall:

It prevent an unauthorized data to come from external network to internal network.

→ It can be hardware ; or software.

Types of Firewall

1) Packet filtering
2) Application level gateway
3) Circuit filtering firewall

1) Packet filtering:

→ Check destination address & port number & source address & port number

→ There are certain set of rules (Check DA ; DPN ...)

→ If it will meet these those rules then it will be allow it else it will be discarded

Scanned with CamScanner

Date:

→ if such packet come that has no rules defined then the fire wall will discard it too.

disadvantage
it doesnot check the data and data might be malicious.

2) Application level gateway (Proxy-Server) :-

→ it is more secure
→ it check data whether it is malicous
→ in it if a host want to sent data outside the interal network
- the request will go ~~to pro~~ through proxy server and proxy server will check it and when someone from the external network want to send data it will go through proxy server for checking

disadvantage:
It take long processing

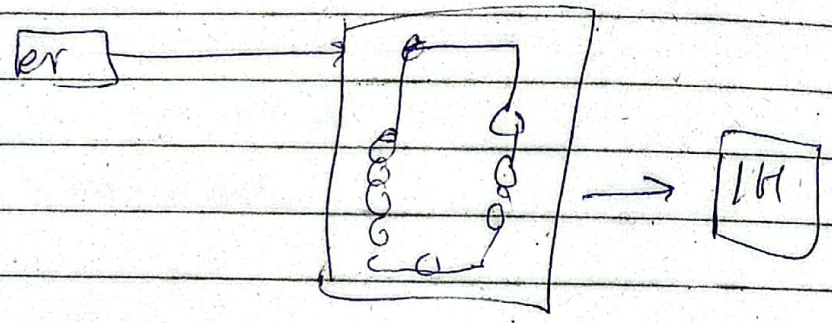
PTO

Scanned with CamScanner

Date:

3) Circuit Filtering Firewall:

⇒ 2 TCP connection are made
→ b/w internal ~~bes~~ host & circuit level gateway
→ b/w external host & circuit level gateway.



⇒ Authentication is done before setting up connection

→ once the connection is established data will pass ~~tbk~~

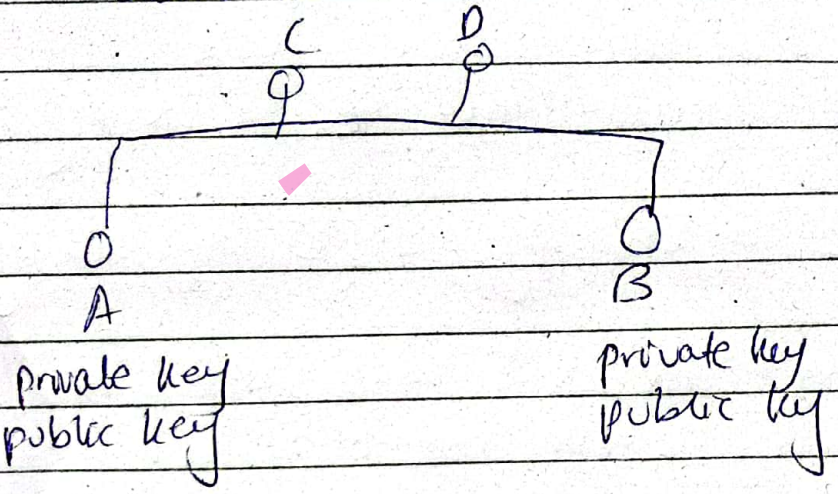
RSA:

it is an asymmetric cryptography algorithm. Assymetric means it work on two different key ie private & public

Scanned with CamScanner

Date:

Consider A want to send data to B



Now if A want to send data to B and encrypt data with its (A) private key it can only be decrypted with its own public key and vice versa.

Now there are 4 cases.

E = encrypt
D = decrypt

1) E (A public key) = D (A private key)

this wont work bcz B did not have A private key to decrypt.

2) E (A private key) = D (A public key)

this can be decrypte by anyone because A public key is publish key

Date:

3) E (B private key) = D (B public key)

This also not possible bcz
A doesnot have B private key.

4) E (B public key) = D (B private key)

Now this will work bcz A
encrypt data with B public key
and B decrypt data with
its own (B) private key
So it is secure.

What if key gets ~~kidno~~ hacked?

Ans) It is impossible bcz the key
is generated with a large
prime number which need
high computation to crack &
will take decades to take.