Principal of Data security

Following are the principal of security :-

1) Confidentiality :-

It determines the secrecy of the information. The Principle specifies that only the sender and receiver will be able to access the information shared between them. Confidentiality compromises if an unauthorized person is able to access a message.

2) Authentication :-

Authentication is the way to identify the user of the system. It ensures the identity of the person trying to access the information. The Authentication is most secured by using Username and password.

3) Integrity :-

It gives the assurance that the information is exact and accurate. If the content of the message is changed after the sender send it but before reaching the receiver, then it is said that integrity of the message is lost.

4) Non-Repudiation :-

It is the mechansim that prevents the denial of the message content sent through a network. In some case the sender send the message and later denies it then the merge will be sent to recived so it can not refuse late.

5) Access control :-

The principal of Access control is determined by role management and rule management. Role management determine who should access the data while rule management determine up to what extent one can access the date.

6) Availability :-

The principal of availability stetes that the resources will be available to authorize party all the time. Information will not be useful if it is not available to be accessed.

7) Issues of ethics & law :-

1) Individuals right to access personal information is refered to as privacy.

2) Property :- It is concerned with the information's owner.

3) Accessibility is concerned with an organization right to collect information.

4) Accuracy also matter.

Symmetric Key Cryptography

Symmentric key Cryptograph also known as Symmetric Encryption is when a secret key is genrated for both encryption and decryption functions. This method is opposite to Asymmetic Encryption where one key is used to encrypt and another is used to decrypt. During this process, data is converted to a format that can not be read or inspected by anyone who does not have the secret key that was for encryption & descryption.

Some common encryption are :-

1) Advanced Encryption standard (AES)
2) Data Encryption standard (DES)

DES (Data Encryption Standard)

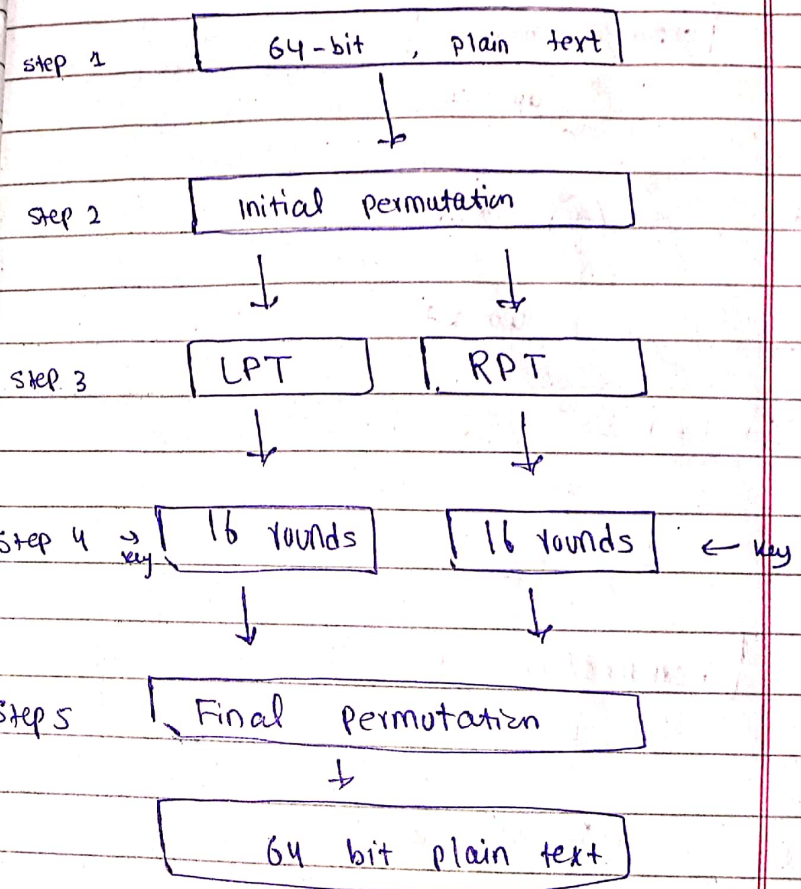
1) Block cipher
2) Symmetric cipher. (same key for enc & dec)
3) 64 bits plain text block.
   (It encrypt the data in block of size 64 bit each).
4) 16 rounds ← Total hotin hain.
   ↘ each round is a Tiested round,

★ steps :-

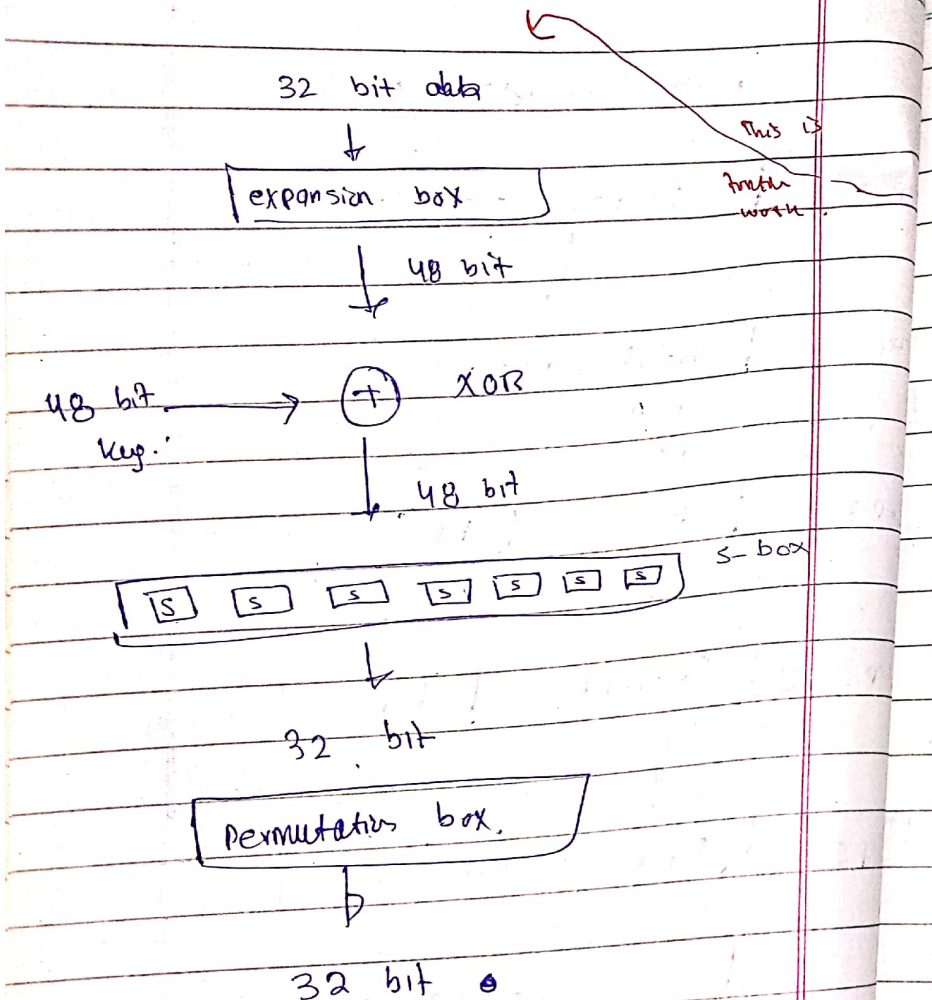
1) Initial permutation
2) 16 Tiested round
3) swapping / left right swap
4) Final permutation / inverse initial permutation.

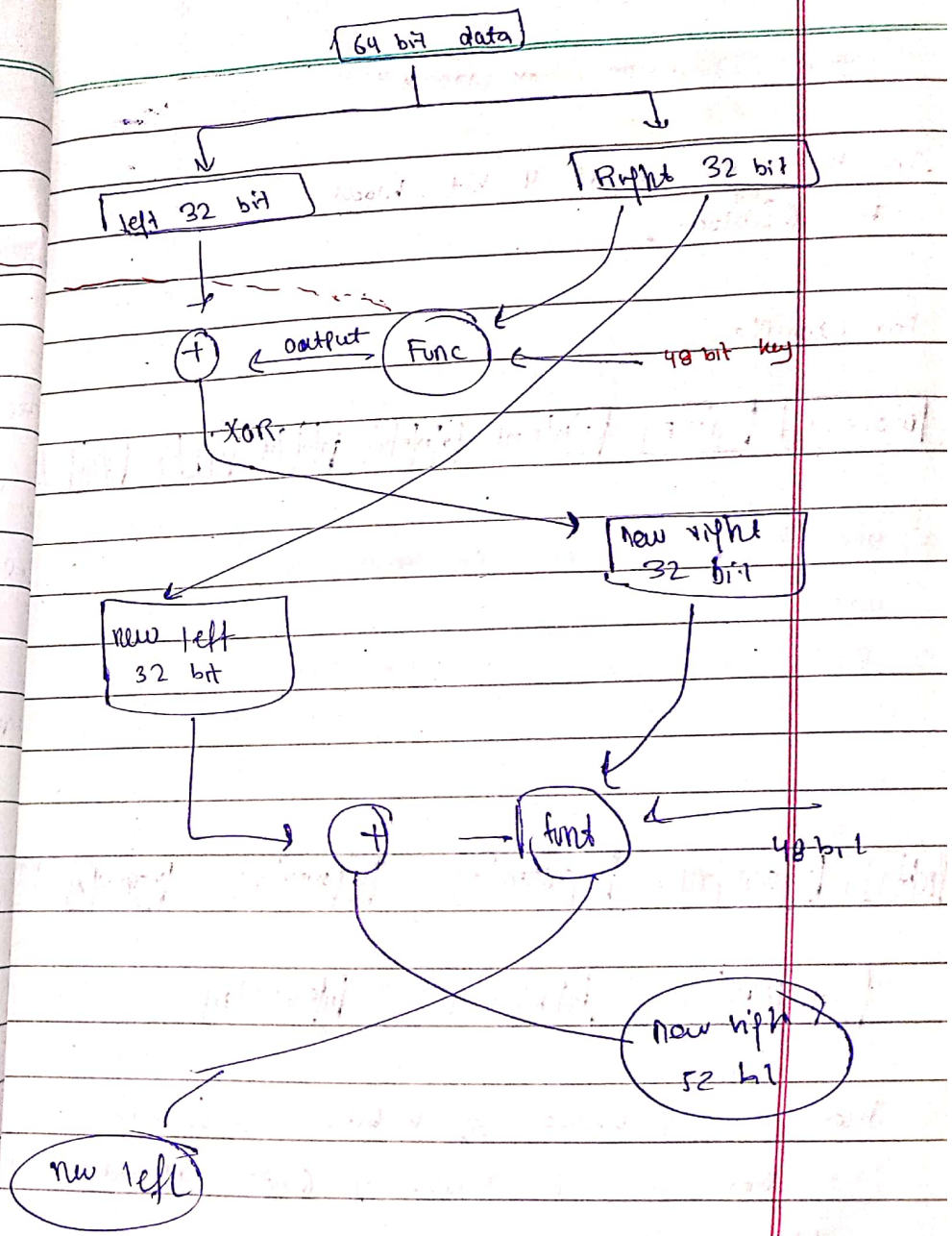
structure

★ DES encryption ★



Function definition





How Expansion box work?

In this we convert 4 bit block to 6 bit block.

For example

D	O	N	T	G	I	V	E	T	H	E	M	O	N	E	Y	T	O	T	H	A	T	P	E	P	E	R	S	O	N	E	V	E	R	D

a) New box banao or uss main six bit lelo.

b) Pehly ka last aple ka first.

T	G	I	V	E	T	E	T	H	E	M	O	M	O	N	E	Y	T	Y	T	O	T	H	A	H	A	T	P	E	R	E	P	E	R	S	O	N	E	N	E	V	E	R	D

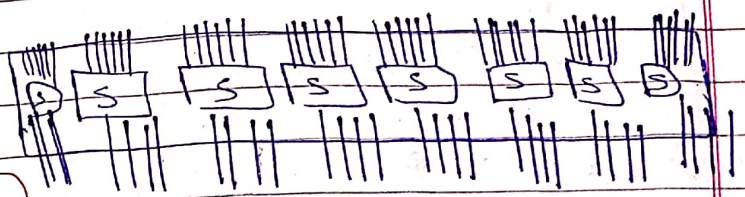
There were 8 blocks of 4 bits = 32 bit

Now There are 8 blocks of 6 bits = 48 bit

After this

48 bit will XOR with 48 key.

Q:- What happens in S-boxes? How this S-box convert 48 bit to 32 bits.



How 6 bits convert to 4 bits?

0 0 1 0 1 1

Row — Columns — Row.

01 = 1

0101 = 5

How 16 Sub keys are generated?

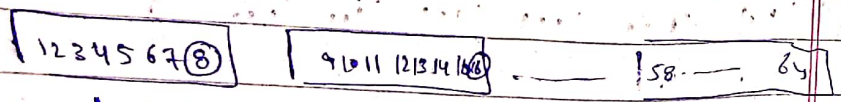
→ we have 64 bit key.

First it goes to PC1 permuted choice and we get output as 56 bits key.

Inside PC-1 (Permuted Choice)

64 bit key divide into 8 parts each of 8 bits.

$8 \times 8 = 64$ bit.

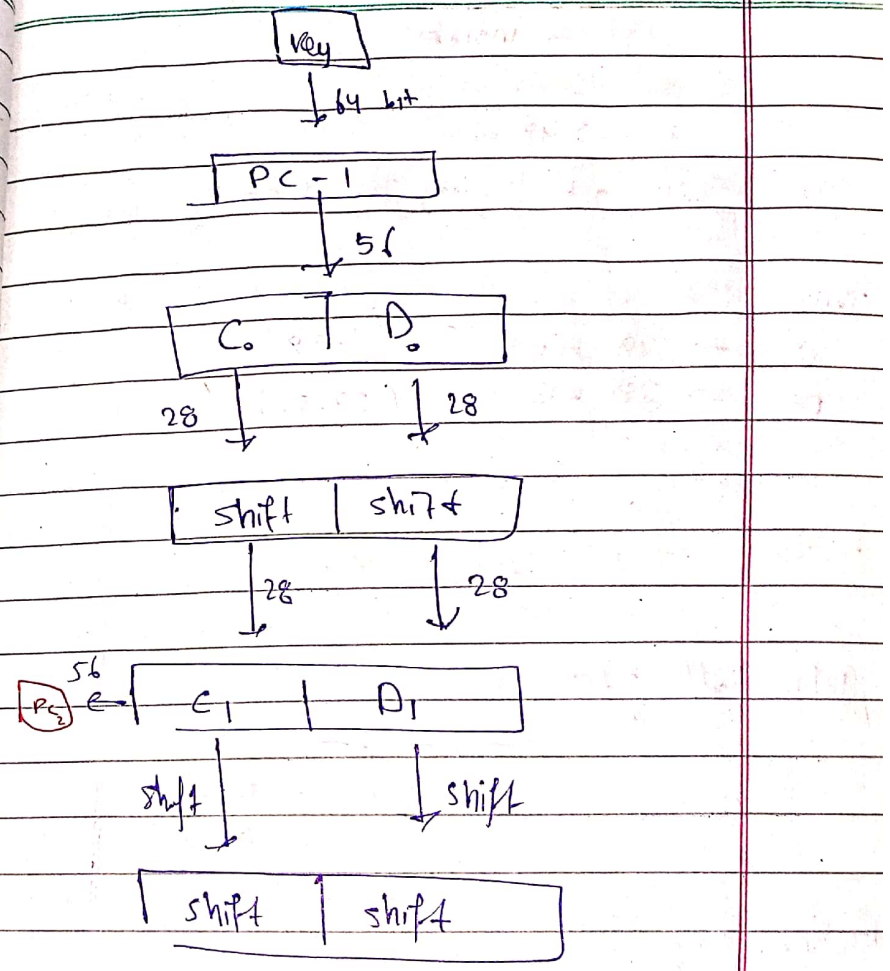


From each part, last bit → discard.

i.e. bit, 8, 16, 24, 32 —— 64 discarded

Hence we have 8 parts of 7 bit

$= 8 \times 7 = 56$ bits.



Round 1, 2, 9, 16 → iss main 1 bit shift hoys

bari

3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15 → 2 bit shift

P2 – inside

56 bit ⟶ 48 bits

Then we will get 1 key for round 1

Then

C_1 ⟶ 28 bits – (1-28)

D_1 ⟶ 28 bits – (29-56)

• How 56 bit convert into 48 bit ?

left half side

(–, –, –, –)

4 – bit · position bit ren

Right half side

(–, –, –, –)

4– Position bit ren

24+24 = 48

2DES (Double DES)

1) Double DES

→ use 2 differed keys

(56 + 56) = 112 bit key

→ Double encryption occurs :-

as

$P \rightarrow E(K_1, P)$

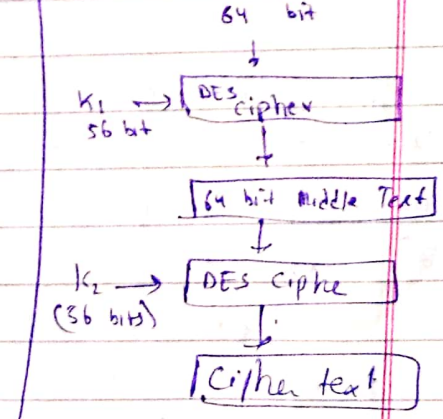
$E(K_2, E(K_1, P))$ = Cipher

↑ Encryption

For decryption

we will use K_2 to encrypt single Cipher the K_1

Block Diagram of 2DES



Q:- Draw back of Double DES ?

Meet - in - the - Middle attack. (MIM attack)

This attack involves encryption from 1 end and decryption from the other end and then matching the results in the middle and hence the name.

Answer

This attack require some plaintext/ ciphertext pair.

The attack processed follows:

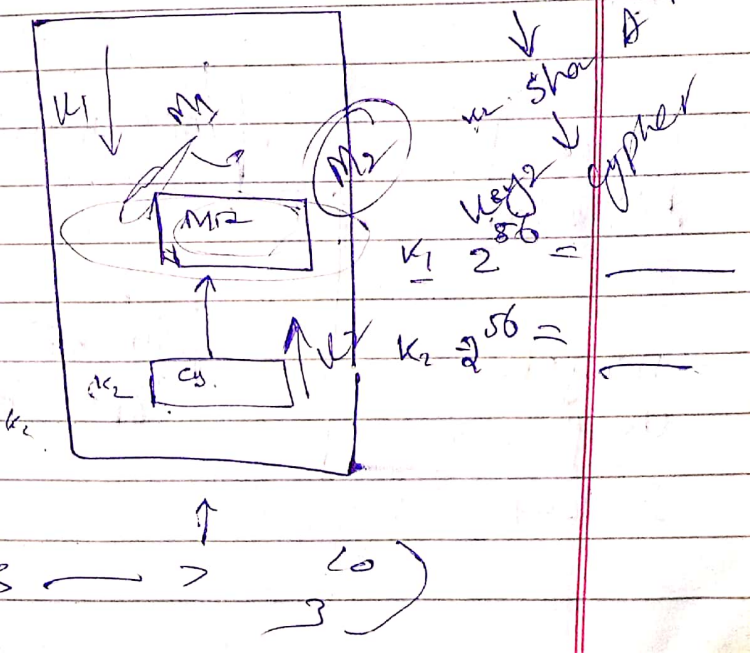
1) encrypt up to all 2^{56} possible value of K1 and then store the result in table and sort it.

2) Now decrypt "c" of all 2^{56} possible value of K_2. As each result is produce, check again the table for a match.

iii) when there is match we have located a possible correct pair of key.

iv) Attacker will know the plain text

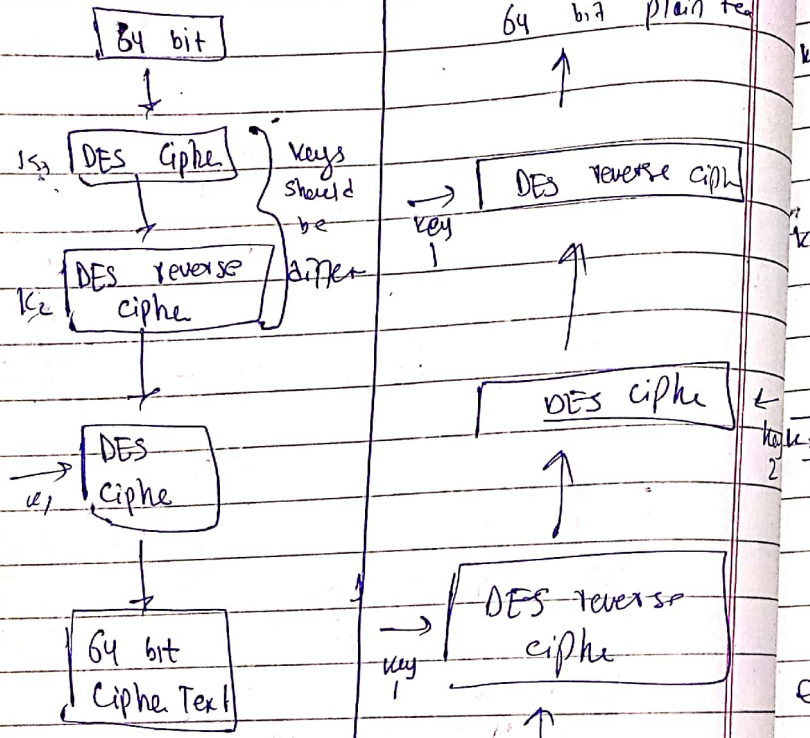
Rough



3 (DES)

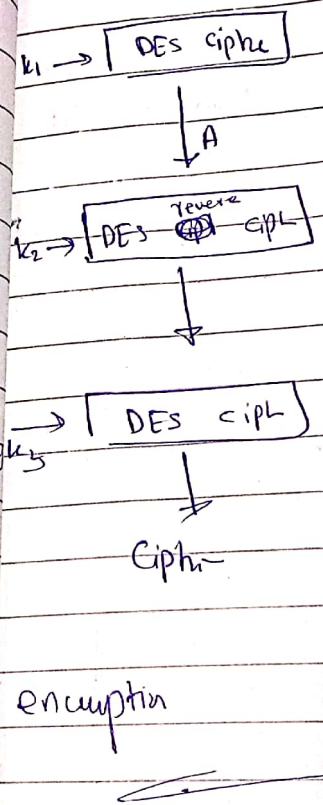
→ It can use 2 or 3 key.

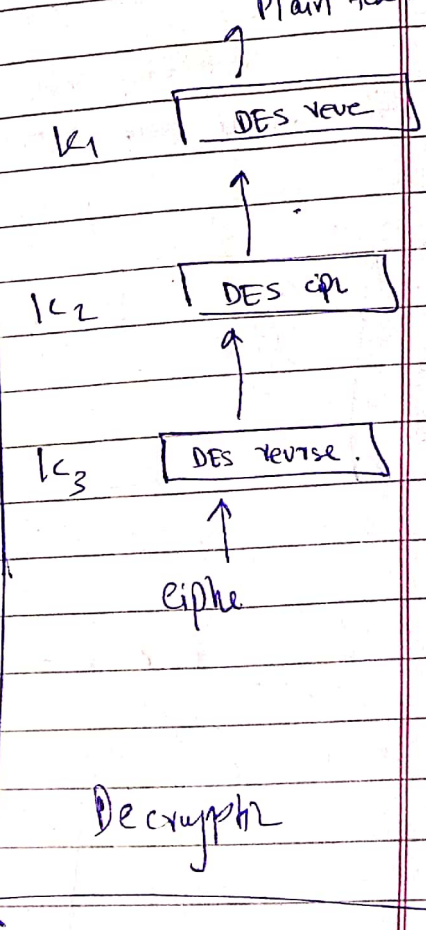
→ much stronger than double DES



encryption using 2 key

using 3 -keys





3d

key

$1^{56} + 2^{56} + 2^{56}$ ←

AES (Advanced Encryption standard) in Cryptography

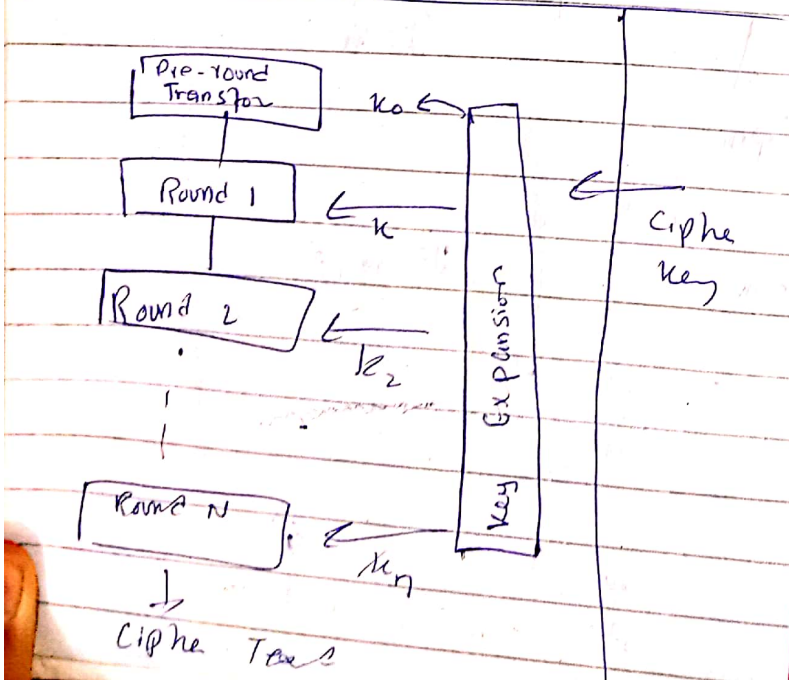
AES :-

→ It is symmatric key block cipher

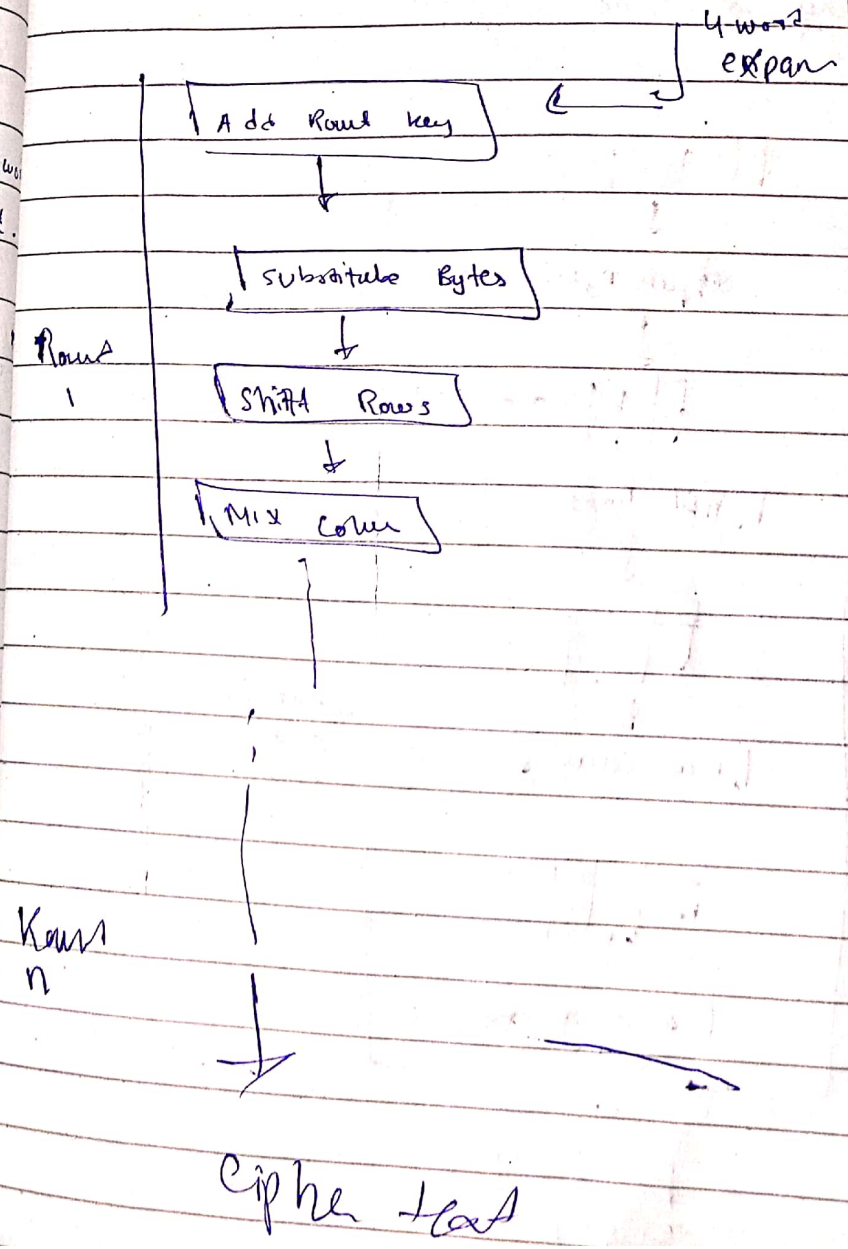
→ fixed block size - 128 bit. ∴ 16 byte = 4 word

1 word = 32 bit.

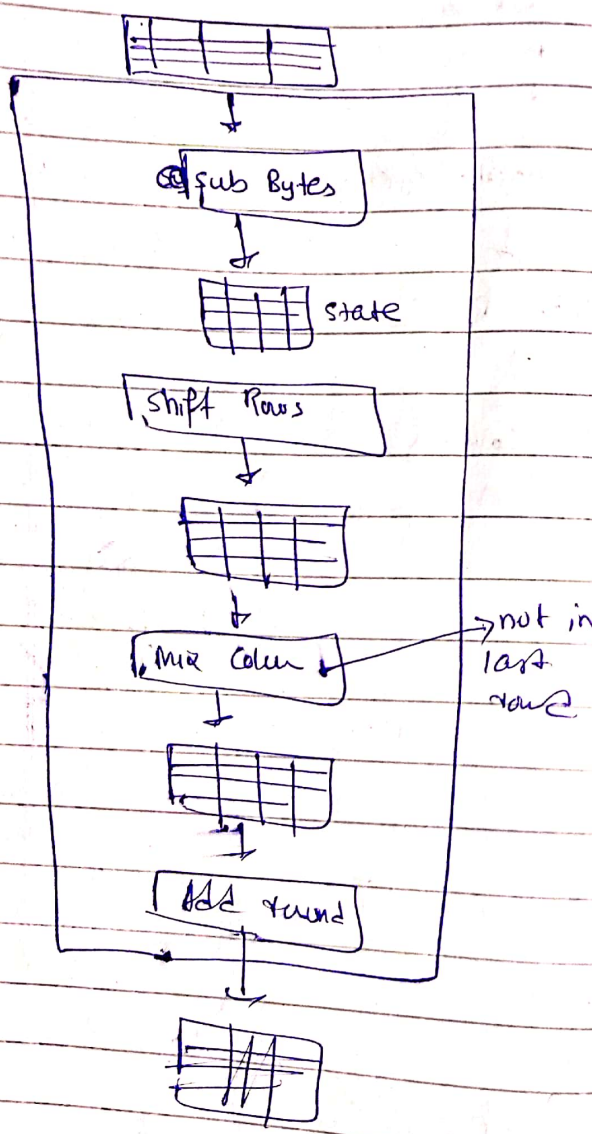
Rounds	no of bits in key
10	128
12	192
14	256



no of key generate = No of rounds + 1



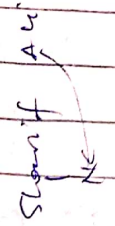
* Structure of each round at the encryption side



Transformation

↳ Four types

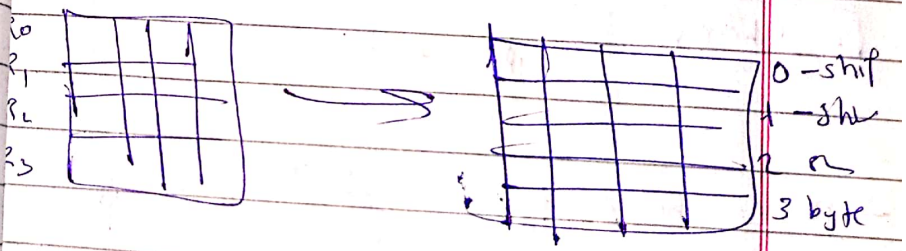
1) Substitution



2) Shift Row

→ it is done to the left.

⇒ no of shift depend on row no.



3) Mixing

Multiple Matrix by colour 1 the 2, then 3, then 4 or new matrix bane gg.

1) Ceaser Cipher :-

It is an encryption technique

For - Exam

↓ Plain text

Hello if key = 3

H	E	l	l	o
↓	↓	↓	↓	↓
ijk	fgh	mno	mno	pqr

= khoor → Cipher text

→ It can be easily decipher.

Mono - Alphabetic Cipher :-

In the type of cipher in which we shuffle the Alphabetic by any random mapping.

A	B	C	———	L, M, - —	Z
↓	↓	↓		↓ ↓	↓
e	z	o	- ———	a	t	x

iss main hum abcd — z ko apne sy koi alphabet ayn kartin hn. or phir cipher text banatin hn.

BCZQ → ZOXE

plaintext → cipher text

Poly Alphabetic Cipher (Vigenre Ciphr)

Kesi bhi random ~~ka~~ numbe
sy ~~characters~~ characters ka
replace karo.

Encryptio

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

decryptio

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

Key = Hello Hellos
Plaintat = Muhammad ali

	H	E	L	L	O	H	E	L	L	OS
Key:	7	4	11	11	14	7	4	11	11	14 18
Plain:	12	20	7	0	12	12	0	)	o	11 8
CT:	19	24	18	11	0	19	4	14	11	28 0

= (7 + 12) mod 26
= 19 mode 2 = 26 | 19

RSA Algorithm

→ It is an asymmetric cryptographic algorith.
→ (2 key) → public key & private key will used.

Public key = known to all users in N/W
Private key = kept secret not shareable to all.

If Public key of user 1 is used for encryption we have to use the private key of same user for decryption.

How to generate key?

next page

1) Select two large prime no "p" & "q".

2) Calculate $n = p * q$.

3) Calculate

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

4) Choose vale of e

$$1 < e < \phi(n)$$

v) Calule

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

i.e

vi) public key = $\{e, n\}$

vii) private key = $\{d, n\}$

Encryption = $M^e \bmod n$

decryption = $M = c^d \bmod n$

For example (For generating key).

Let $p = 3$ $q = 11$

$n = p \times q$

$n = 3 \times 11 = 33$

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

$\phi(n) = 2 * 10 = 20$

so let $e = 7$ as $1 < 7 < 20$

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

$de = 1 \bmod \phi(n)$

$7 \times d = 1 \bmod \phi(n)$

$7 * d \bmod \phi(n) = 1$ ← (1)

$\therefore d = 3$

7 √21

wo value aye gi jo remende hogi.

Public key = $\{e, n\} = \{7, 33\}$

Private key = $\{d, n\} = \{3, 33\}$

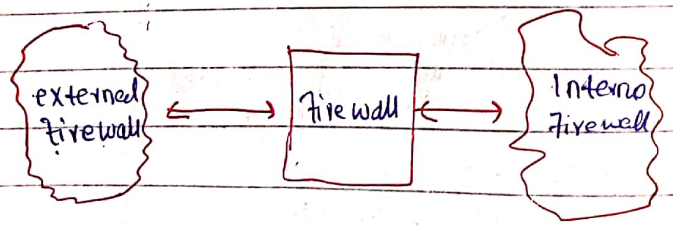
★ Fire Wall ★

Firewall :-

A firewall is a n/w security systems that monitors and control incoming and out going network traffic based on set of rule.

It is the barier between external & internal network.

→ All data most be passed through this fire wall.



★ Types of fire wall :-

1) Packet filtering firewall
2) Application level Gateway
3) Circuit level Gateway.

i) Packet filtering firewall

It is the type of firewall in which it has set of rule to each incoming IP packet.

Rules are based on source IP, destination IP, Port number.

If it match the rule then it will be accepted other wise it will be discarded

If packet come to the firewall without rule then it will be discarded.

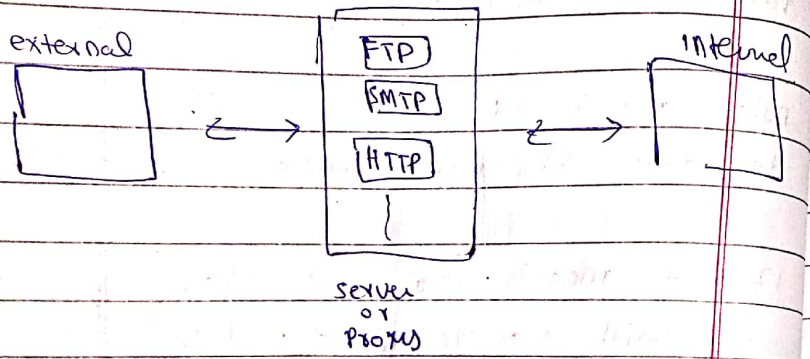
Disadvantage :-

It does not check the data it may contain virus.

→ It is less secure

2) Application Level Gateway

→ It is more secure.



→ It check data whether it is malicious

→ in this if a host want to sent data outside the internal network the request will go through proxy server and proxy server will check it and when someone from external network want to send data it will go to proxy server for check.

Disadvantage:

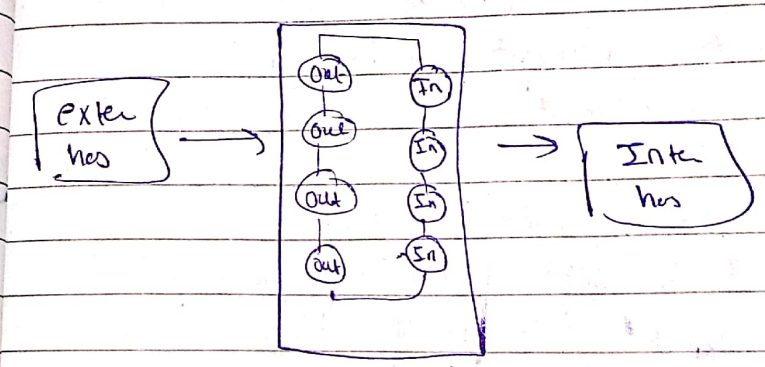
It take large process.

3. Circuit Level Gateways.

→ It uses TCP connection.

a) b/w Internal host and Gateway

b) b/w external host of Gateway



→ Authentication is done before setting up connection

→ once the connection is established data will be passed

SSL

What is SSL Protocol?

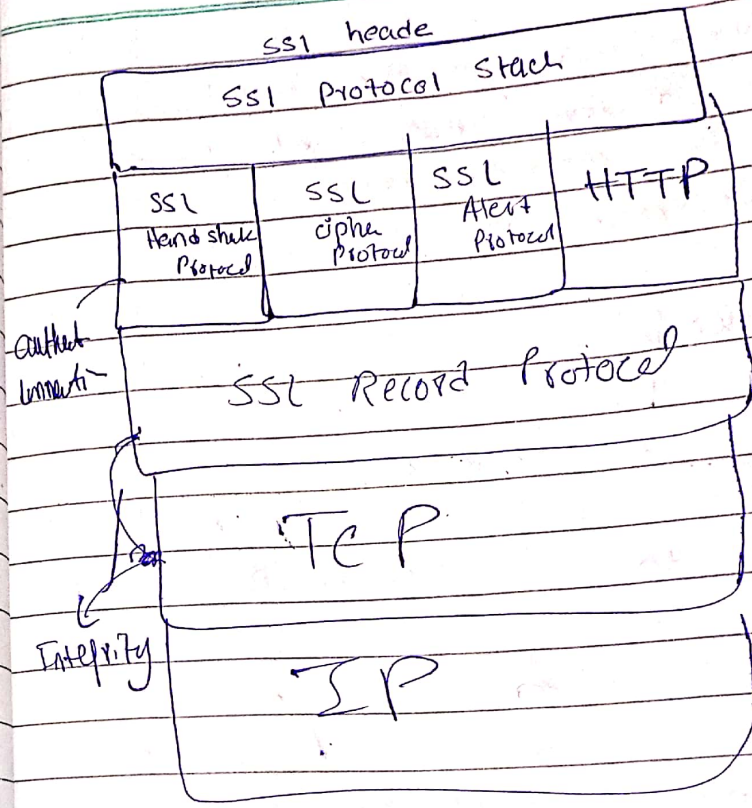
→ Secure Socket layer
→ Security protocol to privide Security and privacy.
→ Used to encrypt information between client & serve.

→ SSL layer work between Application layer & Transport layer when encrypting the information between client & serve.

Application

SSL layer

Transport layer



TLS: Transport layer Security

Same as SSL but it is done in Transport layer.

Digital Signature :-

- It is the proof in the hand of the recieven that data is recived from the authentic resorce.

→ Working

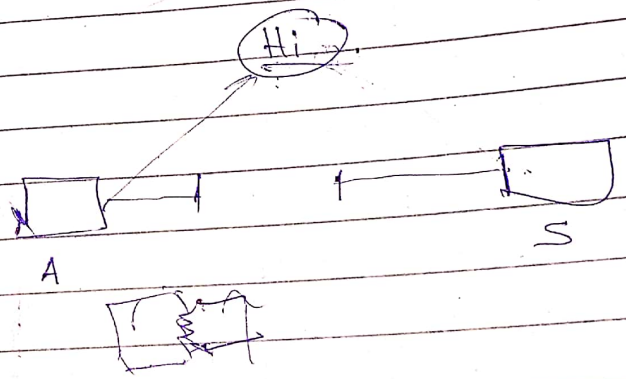
Consider a senario

- A want to send data to B

→ A will use it private key to generate a digital signature through same digital signature operation 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 is descrypted successfully then B will known that the msg is recive from B other — wise he will know that the msg is not from an authentic source.



* Link state Routing *

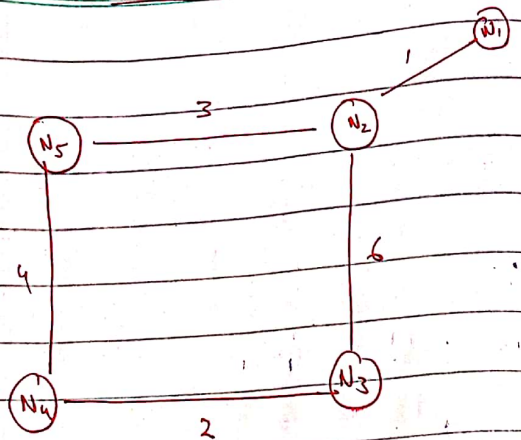
-> to find table

→ Routing table

→ Dijstra algorith to find shortest path

→ Begi notes sy dekho.

* Distance Vector Routing *



N1

Dest	Dis	Next
N_1	0	N_1
N_2	1	N_2
N_3	∞	–
N_4	∞	–
N_5	∞	–

N2

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

N3

Dest	Dis	Next
N_1	∞	–
N_2	6	N_2
N_3	0	N_3
N_4	2	N_4
N_5	∞	–

N4

Dest	Dis	Next
N_1	∞	–
N_2	∞	–
N_3	2	N_3
N_4	0	N_4
N_5	5	N_3

N5

N_1	∞	–
N_2	3	N_2
N_3	∞	–
N_4	4	N_4
N_5	0	N_5

* Now sharing distance

Apne-wala Column

Step 1 :-

1) Only 1 neighbour
2) only Distance Vector

At N_1
= N_2

At N_2
= N_1, N_3, N_5

At N_3
= N_4, N_2

At N_4
= N_3, N_5

At N_5
= N_2, N_4

Step # Now update...

At N_1

N_1 new RT

	1
	0
	6
N_2	∞
	3
	.

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

= $N_1 \rightarrow N_2$ and $N_2 \rightarrow N_2$

$1 + 0 = 1$

= $N_1 \rightarrow N_2$ and $N_2 \rightarrow N_3$

$1 + 6 = 7$

= $N_1 \rightarrow N_2$, and $N_2 \rightarrow 4$

$1 + \infty$

= $N_1 \rightarrow N_2$, $N_2 \rightarrow 5$

$1 + 3 = 4$

Go - Back - N Repeat

$$\eta = \frac{T \times |W_s|}{T_t + 2 * T_p}$$

$$\eta = \frac{|W_s|}{1 + 2 * a}$$

$|W_s| = 1 + 2a$ ← efficiency

Numbe of bits required for sequens numbe

= ceil $(\log_2(1 + 2a))$.