Cryptography → The art of protecting data by transforming it into unreadable form.

i) method of protecting Data.
ii) it all about analysing.

Key :- Key is a string of data which is used lock and unlock cryptographic function.

Key → Public key
Private key.

Public Key :- Known to everyone

Private Key :- Known only to that particular person.

Types of cryptography :-

cryptography → Symmetric key C
Asymmetric key C
Hash function C

① Symmetric key cryptography :- Whenever encryption & decryption done by common key is called symmetric key
② It is also called secret key C

Plain text → Key K1 → cipher text → Key K1 → Plain text

③ Asymmetric key cryptography → Whenever encryption & decryption done by diff keys is called Asymmetric key C

Plain text → K2 → cipher text → K1 → Plain text.

Hash function cryptography → A cryptographic hash function is an algo that takes an arbitrary amount of data input & produce a fixed size output of enciphered text called a hash function value.

Symmetric Key C v/s Asymmetric Key C

i) Symencryption & decryption done by common key	i) diff key
ii) Private key	ii) Public key
iii) faster	iii) slower
iv) less complex	iv) more complex
v) less time taking	v) more time taking
vi) Key sharing is done	vi) not allow
vii) DES, AES	viii) RSA, DA

Security Goals → C → Confidentiality
I → integrity
A → Availability.
CIA

i) Confidentiality → it's only allows authorized users to access sensitive & protected. in simple words the data sent over the network should not be access by unauthorized person.

Encryption
↓
Access control
↓
Authentication
↓
Authorization
↓
Physical Security

ii) Integrity :- Integrity refers to the methods for ensuring that data is real accurate & safeguard from unauthorized user modification.

Back-ups
↓
check sums
↓
Data correcting codes
↓
Availability

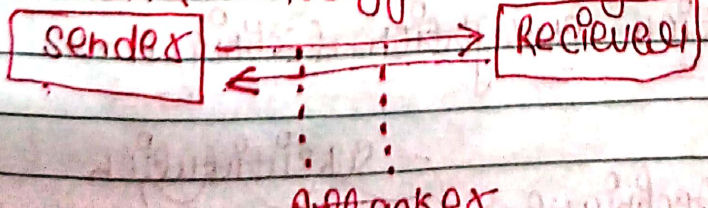
iii) Availability → Availability is the property in which info is accessible by authorized person anytime & anywhere.

Physical Path
↓
Computational Redundancies.

Security Attacks :-

Security Attacks — Active attack
— Passive attack

Passive attack → The main goal of passive attacks is obtain unauthorized access to the information
In this attack attackers only read the information attackers can't modify the info.



Active attack :- In this attack attacker obtain unauthorized Access & modify your information also.

Security mechanisms :- (How to secure data)

(i) encipherment → The use of mathematical algo to transform data into a form that is not in cipher form.

(ii) Digital signature :-

(iii) Data integrity :- check value.

(iv) Authentication exchange. — two entity exchange some message to prove their identity to each other.

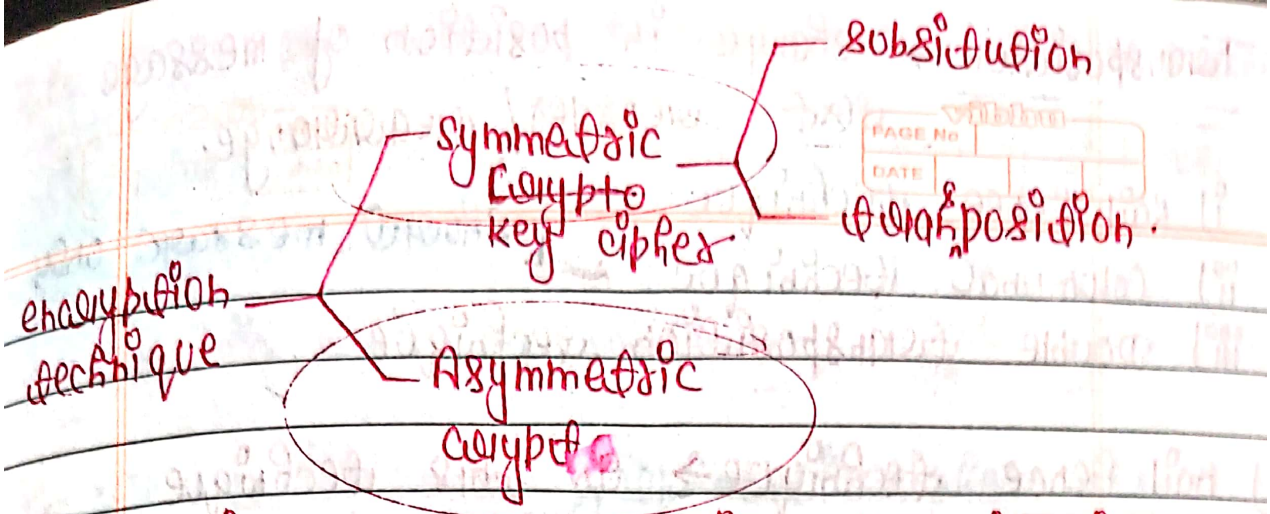
(v) Traffic padding :- In this technique we add some extra bits with the data while before encryption.

(vi) Routing control → selecting & continously changing diff available route for sending data.

(vii) Access control → Authorized person or unauthorized person checking

Classification encryption technique →

encryption technique → Substitution
Transposition



① substitution ~~cryptog~~ encryption → substituting something in plain text & ~~ton~~ transform it into cipher text

i) ceasar cypher
ii) mono-alphabatic cipher
iii) poly " "
iv) play-fair cipher
v) Hill cipher
vi) one time pad technique

i) ceasar cipher → it is also called swift cipher & additive cipher

each ~~letter~~ in the plain text is replaced by a ~~letter~~ corresponding to no of swifts in the alphabet.

Example → key = 3

meet me zebra
↓↓↓↓ ↓↓ ↓↓ ↓↓↓↓ (P+K) mod26
PHHW PH CHEUD

→ phwphceud

C = E(key, plain) = (P+K) mod26

Ex:- HELLO

C(H) = (P+K) mod26
(7+4) mod26 = 11 L
C(E) = (4+4) mod26 = 8 I
L (11+4) mod26 = 15 P
C = (14+4) mod26 18 S

LIPPS

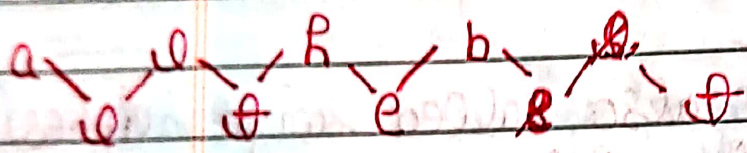
Transposition → change in position of message text - reorder / rearrange.

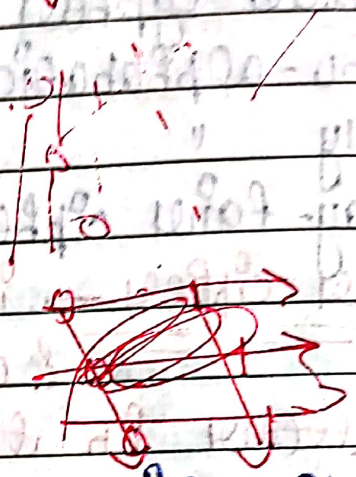
i) Rail fence technique
ii) Columnar technique
iii) Double transposition technique.

} short message only

i) Rail fence technique → In this technique the plain-text is written as a sequence of diagonals & then read off as a sequence of names.

Example → "add the best"





ii) Columnar (columnar)

ii) Row Transposition cipher - we write the message in a rectangle, row by row.

Ex.

attack postpone until 2am

4	3	1	2	5	6	7 ← Key
a	t	t	a	c	k	p
o	s	t	p	o	n	e
u	n	t	i	l	t	w
o	a	m	x	y	z	

extra dummy bits

tntlf
tta apimtsnoaovwcoolpetz

iii) double transposition technique → double encrypt
in both encryption key will be same/ diff also.

play-fair ciphers algorithm → Hello
xy oogc
11

Hill cy ciphers → (Polyalphabetic ciphers also called.

(i) Encryption a pair of letters which was called polygraph: (pair, trice of letters).

[A / +] Polygraphy C = KP mod 26
Plain-text
Key

S1→ choose a key (key matrix must be a square matrix)

view ⇒ $\begin{bmatrix} V & I \\ E & W \end{bmatrix} \Rightarrow \begin{bmatrix} 21 & 8 \\ 4 & 22 \end{bmatrix}$

Example → Attack

key $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$

$\begin{bmatrix} A & T \\ T & A \end{bmatrix} \begin{bmatrix} T \\ A \end{bmatrix} \begin{bmatrix} C \\ K \end{bmatrix}$

$\begin{bmatrix} A & T & T \\ A & C & K \end{bmatrix}$

[A / +] → Polygraph

$\begin{bmatrix} A \\ T \end{bmatrix} \times \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \Rightarrow \begin{bmatrix} 0 \\ 19 \end{bmatrix} \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} = \begin{bmatrix} 57 \\ 114 \end{bmatrix} \bmod 26$

$\begin{bmatrix} 0+57 \\ 0+114 \end{bmatrix}$

$\begin{bmatrix} 1 & 5 \\ 10 & \end{bmatrix} = \begin{bmatrix} F \\ K \end{bmatrix}$

EKLSAB FK

Decryption

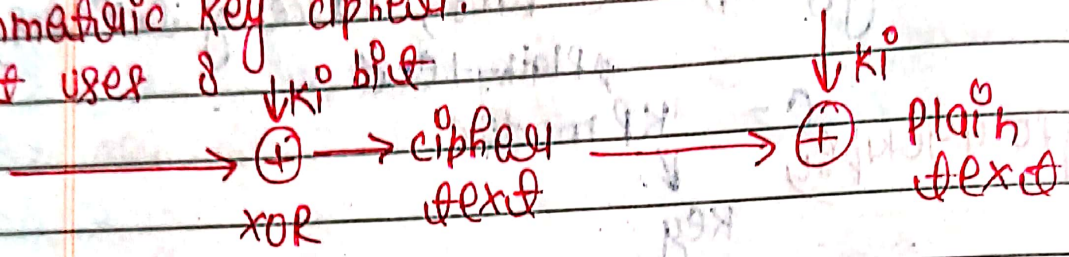
Hill cipher →

12

Stream cipher & block cipher

Stream cipher → that encrypts a digital data stream one bit or 1 byte at a time.

i) Symmetric key cipher.
ii) It uses 8 bit



Block cipher → a block of plain text is treated as a whole, & used to produce the cipher text of equal length

ii) Typically a block size of 64 & 128 bit is used
iii) Symmetric key cipher.

Block cipher v/s stream cipher.

plain text to cipher text by taking plain text's block at a time	1 bit or 1 byte of plain text to cipher text
It uses 64 bit or more	It uses 8 bit
complexity is simple	more complex
use confusion & defusion both concept	only confusion concept used.
reverse encrypted	reverse encrypted easy.
word	

Modern block ciphers / components

C+P

Deffusion :→ The idea of deffusion is to hide the relationship b/w the ciphertext & plaintext.

In simple words, if a symbol in the plaintext is change, several or all symbols in the ciphertext will also change.

C+K e

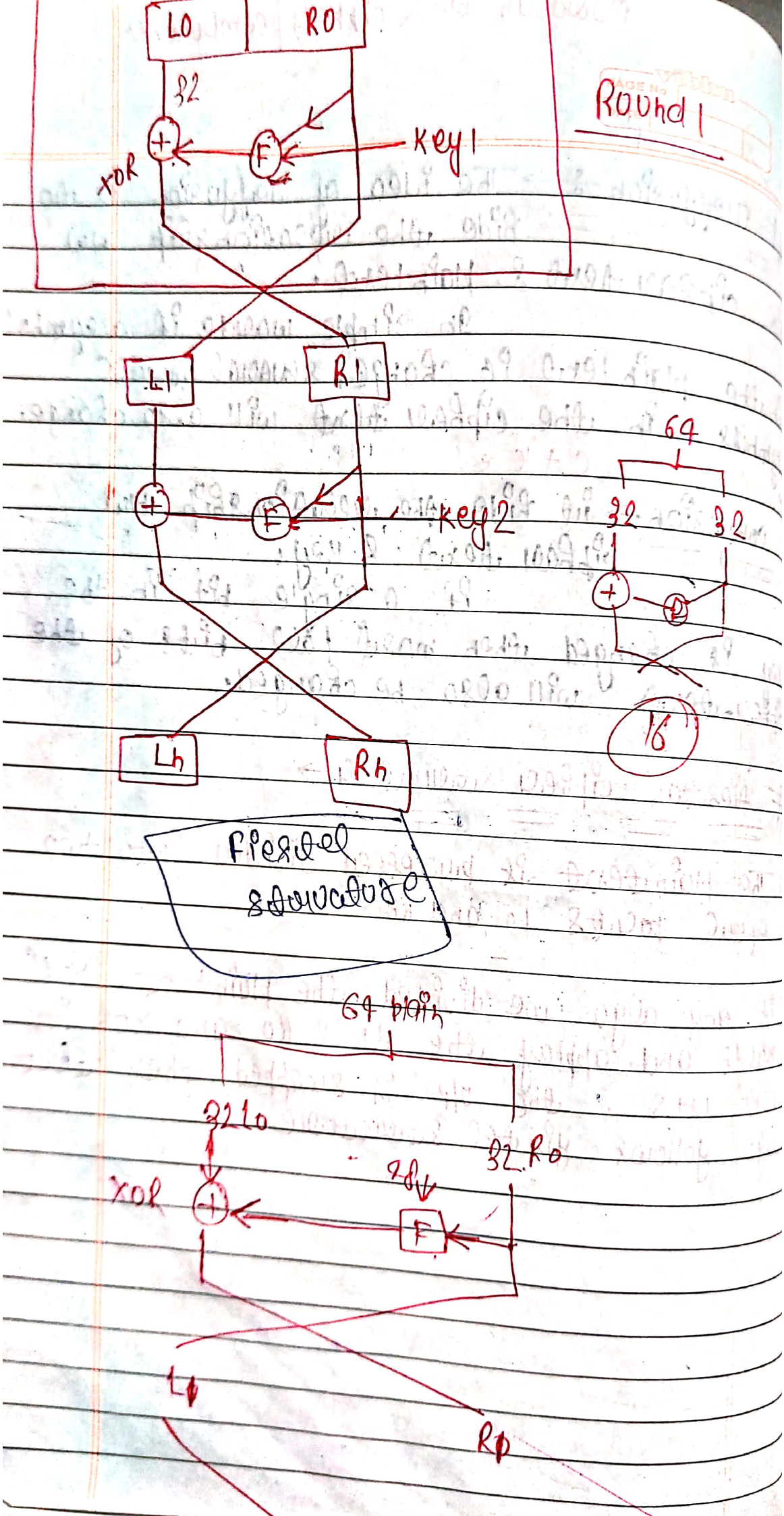
Confusion → it hide the relationship b/w ciphertext & key.

If a single bit in the key is changed then most / all bits of the ciphertext will also be changed.

Fiestal cipher structure →

i) The plaintext is processed divided into two equal parts Lo and Ro

ii) in any algo we divided the plaintext in 2 halfs and apply the F0 & Ro and XOR it. wif LHS & the o/p is swapped then that algo follows fiestel structure.


L0
R0
32
XOR
F
key1
Round 1
L1
R1
key2
64
32
32
16
Lh
Rh
Fiestel structure
64 bits
32 Lo
32 Ro
XOR
F
Lf
Rf

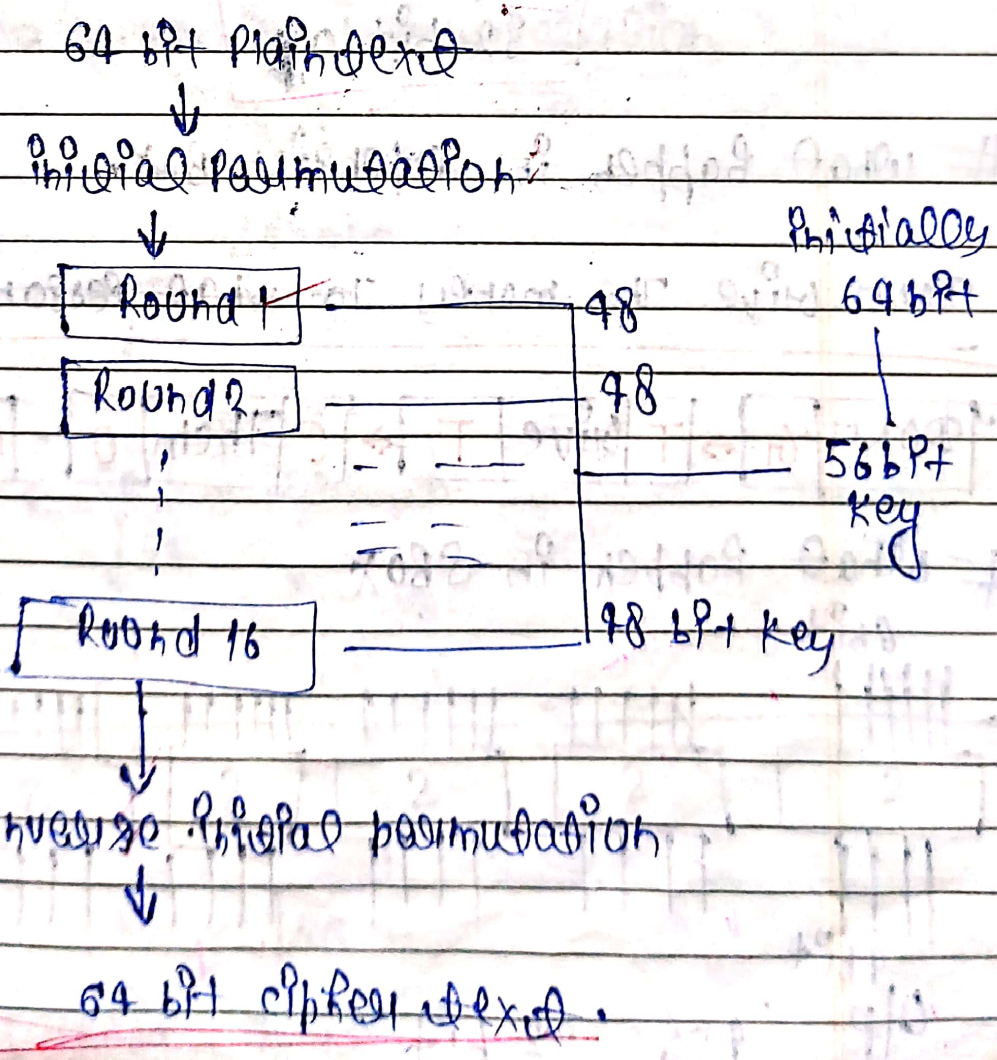
DES → Data Encryption Standard.

computing concept provide

i) block cipher
ii) symmetric cipher
iii) 64 bit plain text block (it encrypt the data in block of size 64 bit each)
iv) 16 round (each round is a Feistal round.

steps → i) initial Permutation
ii) 16 Feistal round
iii) swapping (left right swap
iv) final permutation. (reverse of initial Permutation

Basic structure -



Function definition →

32 bit data

↓

expension Box

↓ 48 bit

key k1 48 → ⊕

↓ 48 bit

S → [S] [S] [S] [S] [S] [S] [S] [S] SBox

Box (Substitution Box)

↓ 32 bit

permutation Box

↓

32 bit o/p

what happen in expension Box.

DON'T give the money To ~~that person ever~~

DON'T G ⇔ T Give T ⇔ e Them O m oney D

what happen in SBox

6 bit

S S S S S S S S

4 bit o/p

4 × 8 = 32 bit

next subkey we have a no:

0 010 1 → Row

↓

column

01 → 1 (Row)

0101 → 5 (col)

check in table

	0	1	2	3	4	5
0	0	3	C	1	4	0
1	1	4	7	2	5	F
2	2	5	8	3	6	2

7 → 0111

Row to generate key generation

Key

↓ 64 bit

PC-1

↓ 56 bit

C0 | D0

↓ 28 ↓ 28

shift | shift

↓ 28 ↓ 28

C1 | D1

↓ 28 ↓ 28

shift | shift

48 ↑

PC-2

56

PC-1

64 bit key divided into 8×8

1 2 3 4 5 6 7 (8)	9 10 11 12 13 14 15 (16)	...	58 59 (64)

gives each half 28 bit discard.

8×7 = 56 bit

1, 2, 9, 16 → 1 bit shifting
3 4 5 6 15 → 2 bit shifting

DES Analysis → (Properties) →

i) Avalanche effect → it means a small change in plain text should cause a significant change in cipher text.

Example

PT → 0000000000000000
CT → 4789FD476E82A561
PT → 0000000000000001
CT → 0A4C8092CER Log

} key K1

ii) Completeness effect → it means that each bit of the cipher text needs to depend on many bits of the plain-text.

① Avalanche effect
② complex

DES weakness (Disadvantages) →

i) Key size → in DES we use 56 bit of key so combination of key 2^{56} so

ii) weak key → four out of 2^{56} keys are weak keys.

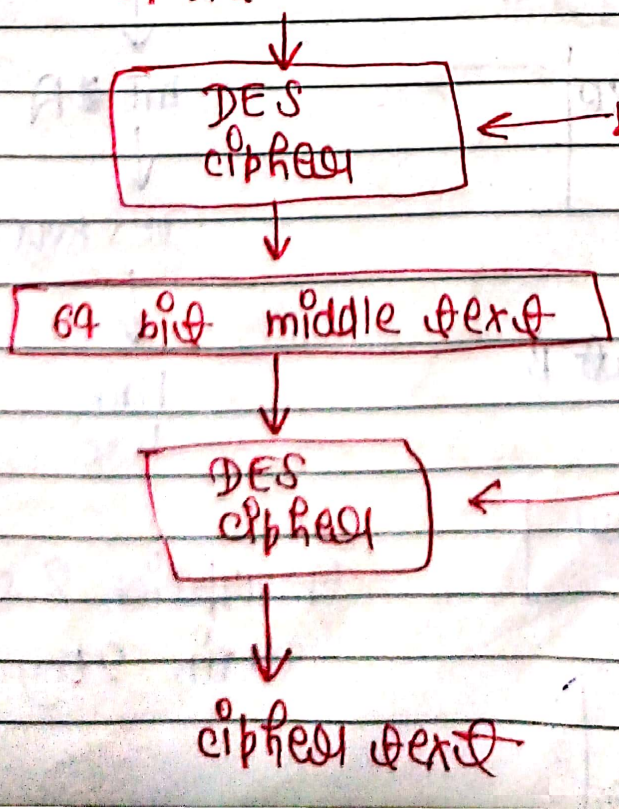
iii) Semi weak keys → six pairs are called semi weak key.

iv) Possible weak key

v) Key clustering → means 2 or more diff key can generate the same cipher text from the plain text.

Double DES →

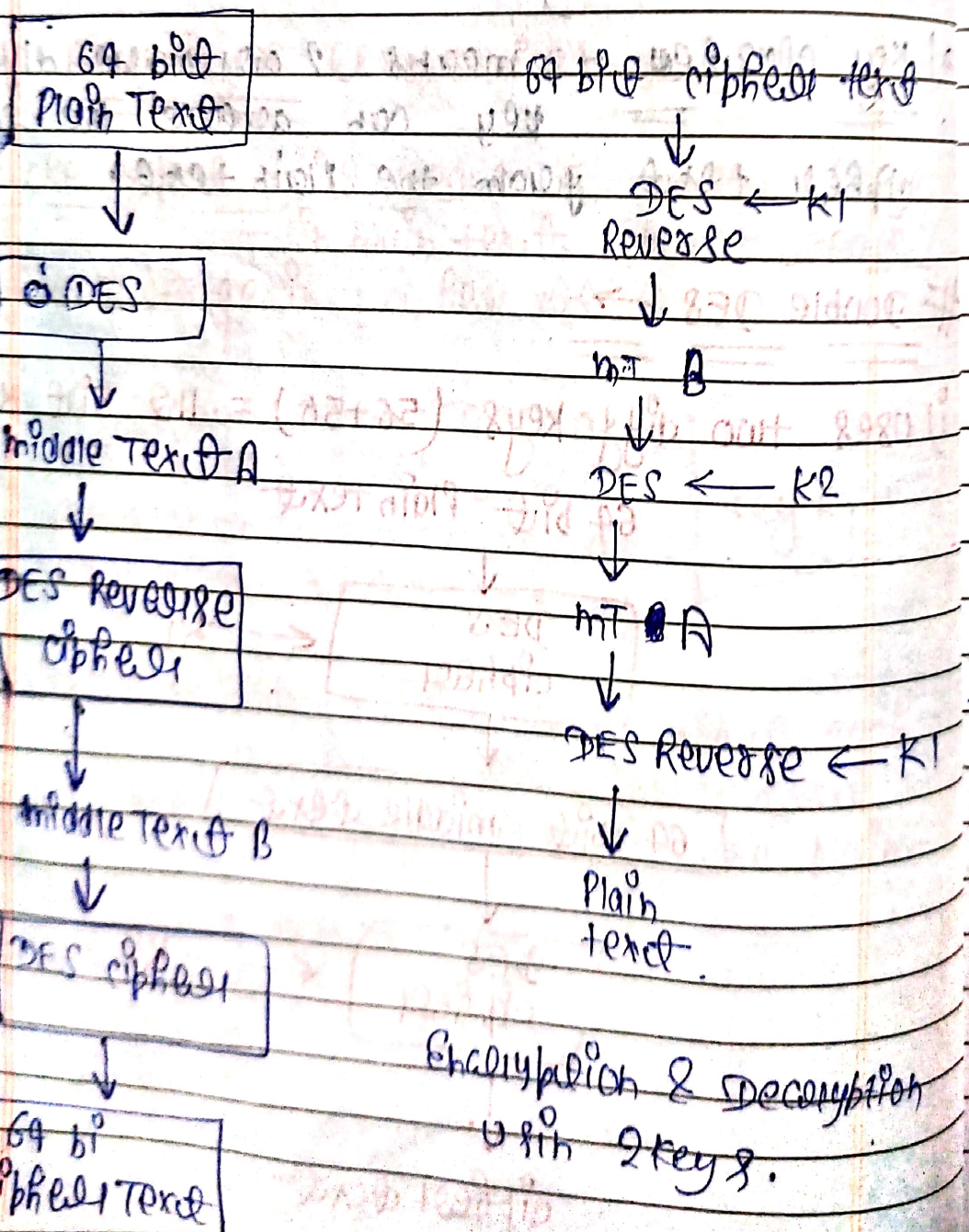
i) uses two diff keys (56+56) = 112 bit key



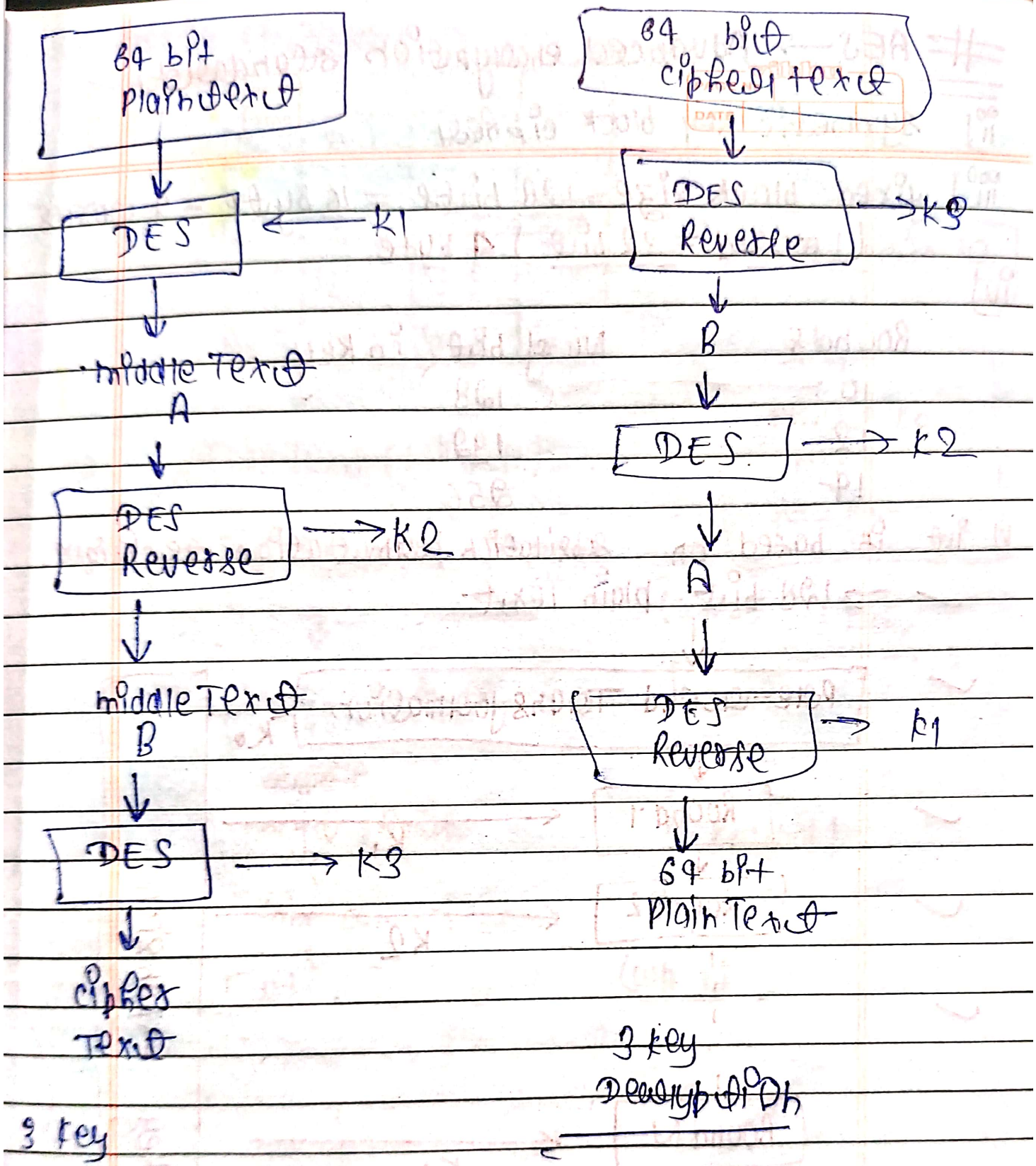
Drawbacks of Double DES →

i) meet-in-the middle attack → The attack involves encryption from one end and decryption from the other end and then matching the message from the other in the middle and hence the name it is also known as mim attack.

Triple DES (3 DES) → in 3DES we can use two keys and 3 keys in much stronger than 2DES.



Encryption & Decryption with 2 keys.



3 key Encryption

3 key Decryption

AES → Advanced encryption standard

ii) symmetric key block cipher

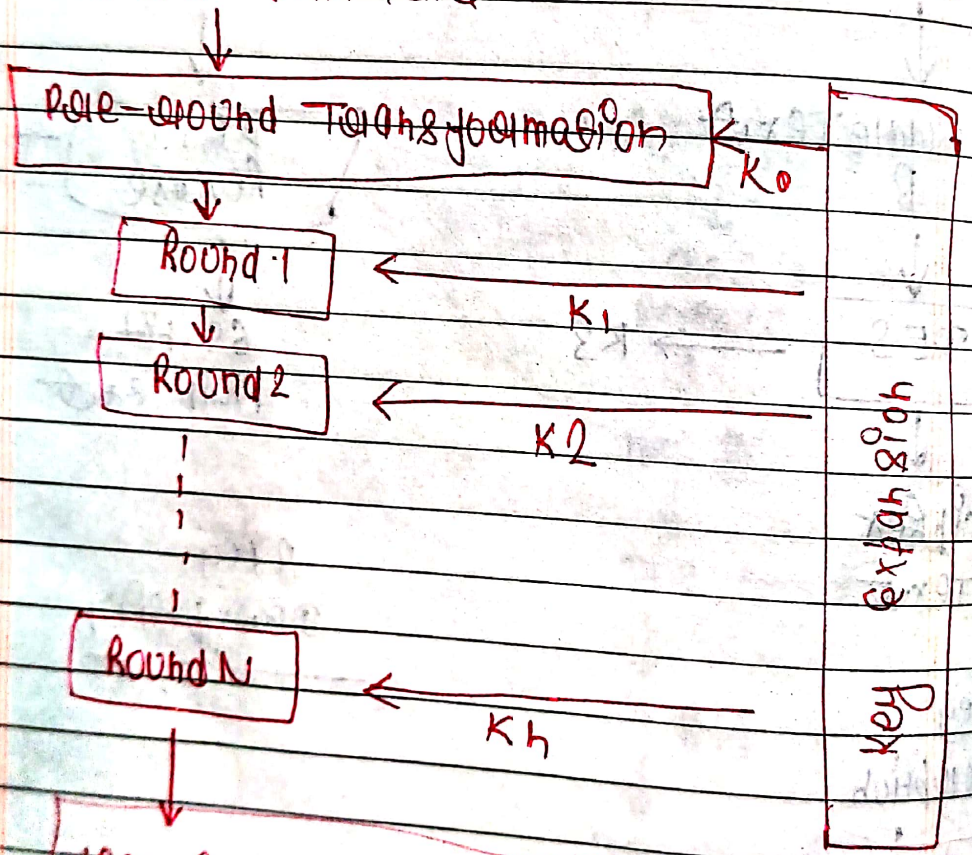
iii) fixed block size = 128 bit = 16 byte = 4 words
(1 word = 32 bit) 4 byte

iv)

Rounds	No of bit in key
10	128
12	192
14	256

v) it is based on substitution permutation technique

→ 128 bit plain Text



vi) No of keys generated by key expansion algorithm = n+1
↓
no of rounds

State of Array →

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

→ word, 4 byte

→ $[w_0, w_1, w_2, w_3]$

Plain Text (128 bit)

↓

Add Round Key ← $(w_0 - 3)$ 4 key

↓

Substitute Bytes

↓

Shift Row

↓

Mix column

↓

Add round key ← $(w_4 - 7)$

Round 1

Substitute Byte

↓

Shift Row

↓

Add round key ← $w_{40} - 43$

Round 10

↓

Cipher Text

AES V/S DES

	AES	DES
i)	AES stands your Advanced Encryption Standard.	DES stands your data Encryption standard.
ii)	Key length can be 128 bits, 192 bits or 256 bits.	Key length is 64 bits (56 bits in each round)
iii)	No of rounds depends on the key length.	DES involves 16 rounds of Round identical operation.
	bits 10 → 128 12 → 192 14 → 256	
iv)	The structure is based on the substitution-permu-tation network.	The structure is based on feistel network.
v)	AES is more secure than it is the de facto word standard.	it is less secure. DES and
vi)	Rounds in AES → Substitution shift Row Mix column key addition	Rounds in DES are → Expansion xor operation with round key substitution & permutation.
vii)	It can encrypt 128 bits of plain text.	It can encrypt 64 bit of plain text.
viii)	No Attack known	Brute force attack, Linear cryptanalysis
ix)	AES is faster	DES is slower.

Blowfish Algorithm

i) Symmetric algorithm
ii) block cipher (64 bit) algo
iii) It is an alternative to DES encryption technique & IDEA algo.
iv) It is based on feistel structure
v) block-size - 64 bit
key size → variable (32 to 448) bits
No of rounds → 16
No of subkeys → 18

#

i) Generation of subkeys → 18 subkey P[0]-P[17] are used for encryption as well as decryption.

P[0] = "0D21C821" Hexadecimal no.
P[1] = "12dc120a"
P[7] = "1209120c"

Now each of the subkey is changed with respect to the i/p key as:

P[0] = P[0] XOR 1st 32 bit of i/p key
P[1] = P[1] XOR 2nd 32 bit of i/p key.
P[13] = P[13] XOR 14th key of i/p
P[14] = P[14] XOR 15th 32 key of i/p key
P[17] = P[17] XOR 18th

Step 2 → Initialize substitution boxes →