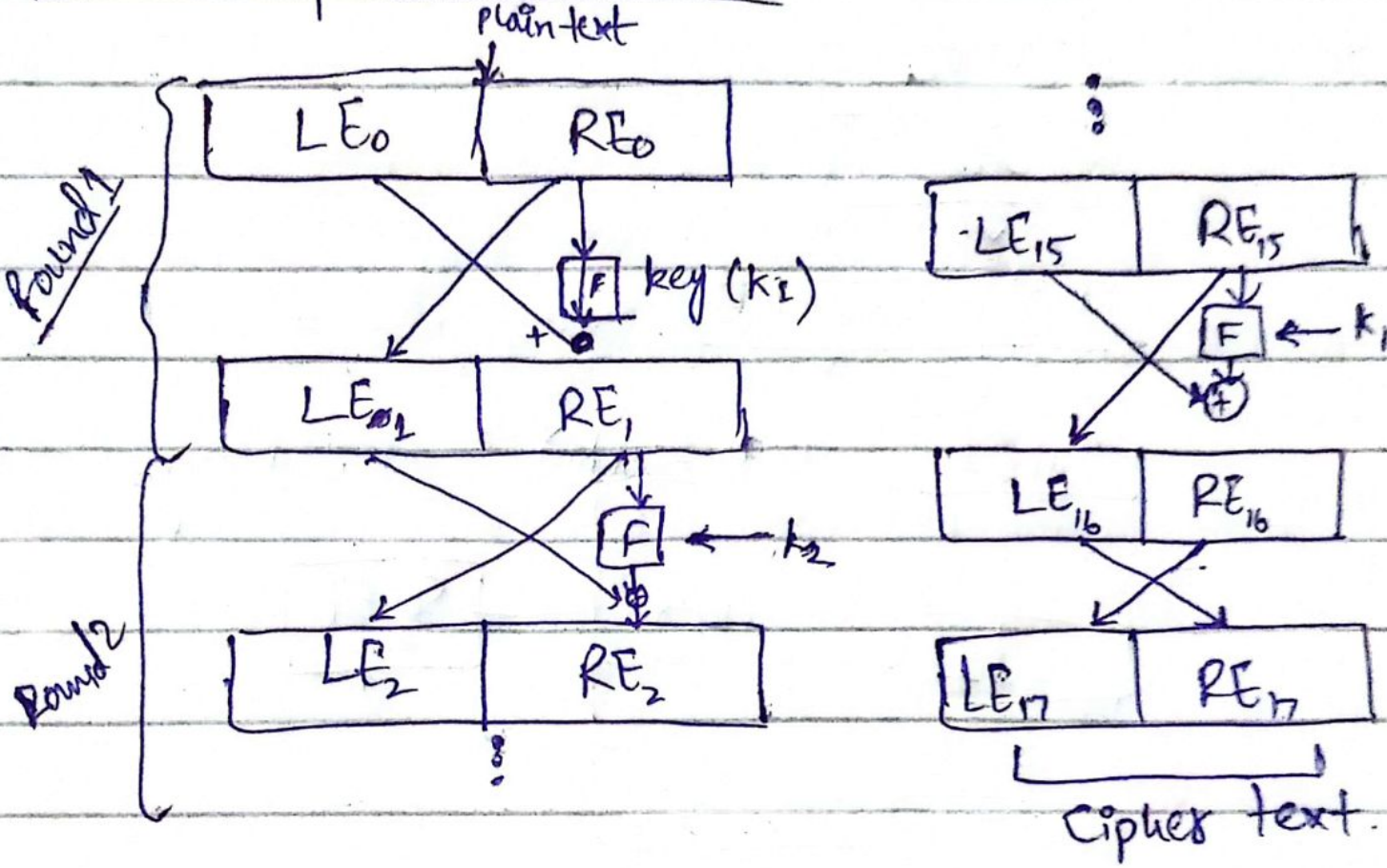
⇒ Feistel Cipher Structure :-



⇒ Block Cipher Design Principles

- → Block size 64 bits
- → key size
- → No of Rounds
- → Subkey Count
- → Round Function
- → Plain divided into 2 halfs.

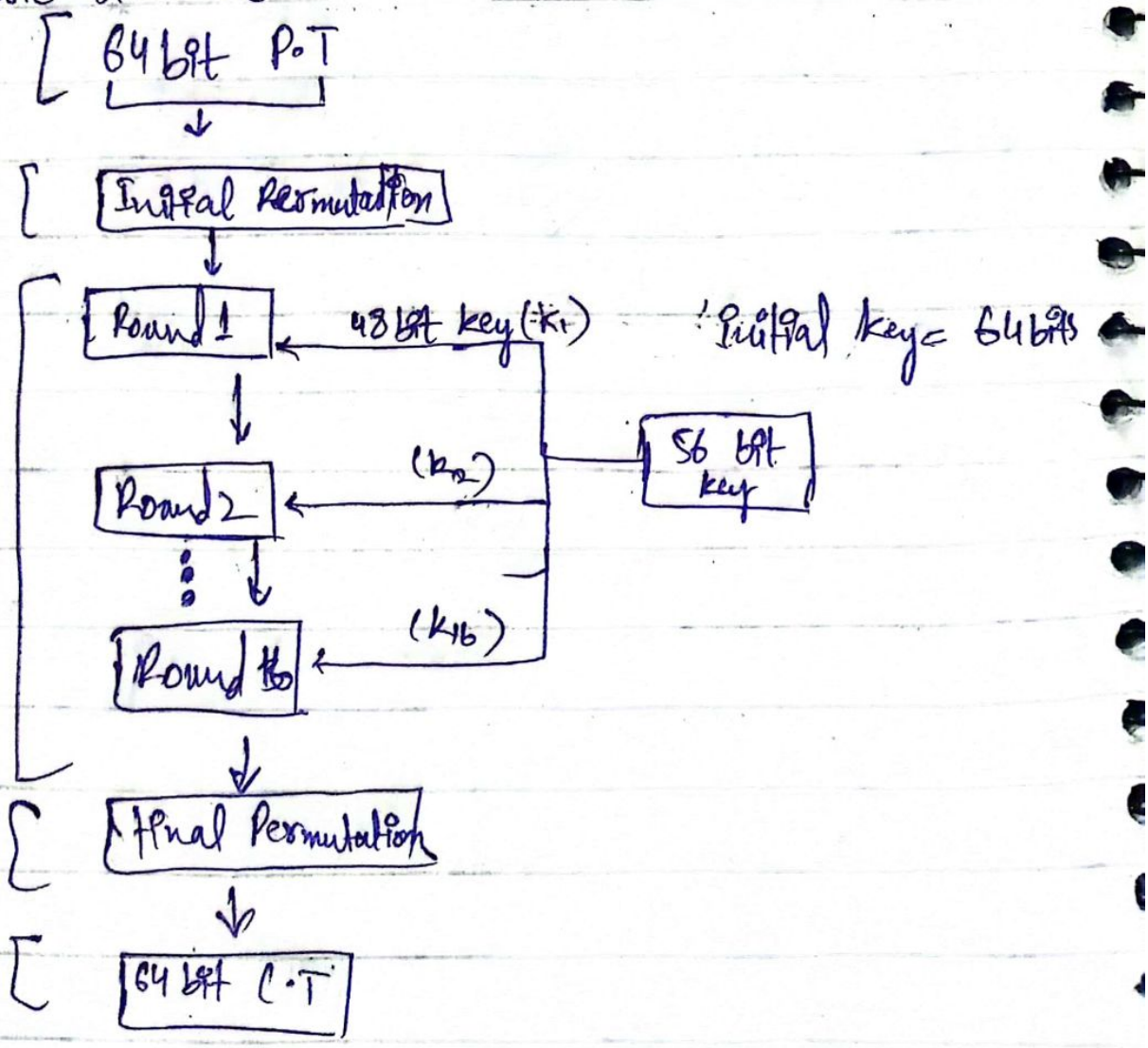
⇒ Data Encryption Standard (DES)

- ⇒ Block ciphers
- ⇒ Symmetric
- ⇒ 64 bit Plaintext Block
- ⇒ 16 rounds (Feistal rounds)

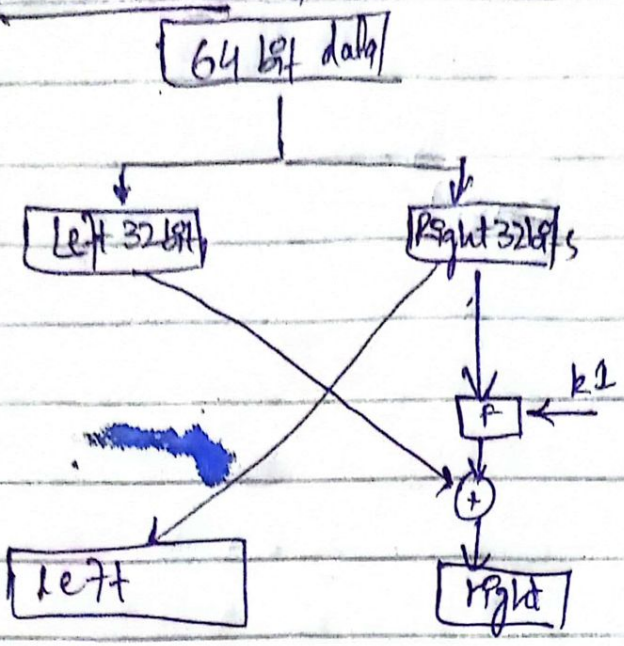
⇒ 4 Steps

(i) Initial Permutation
(ii) 16 Feistal round
(iii) Swapping
(iv) Final Permutation

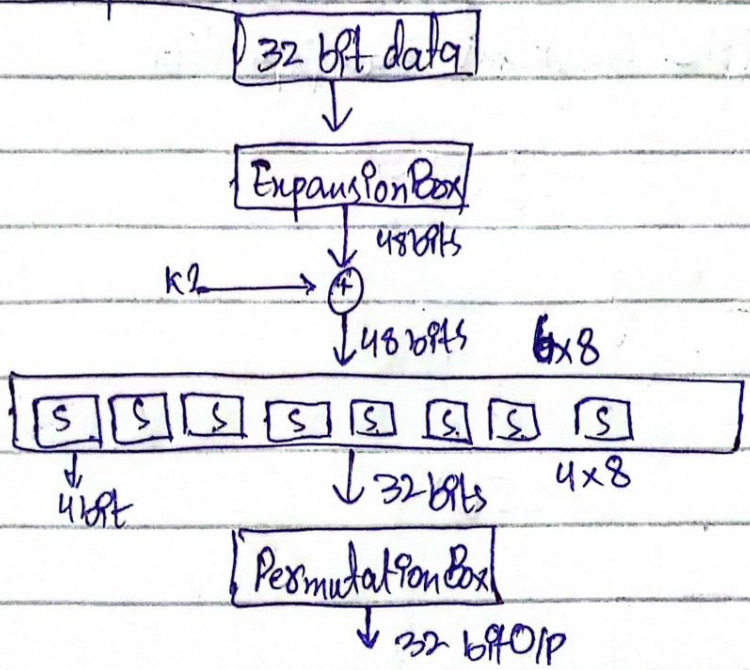
⇒ Basic structure



⇒ Feistal Round



⇒ Round function



⇒ Expansion Box

data - don't give the money to that person ever

4 block size

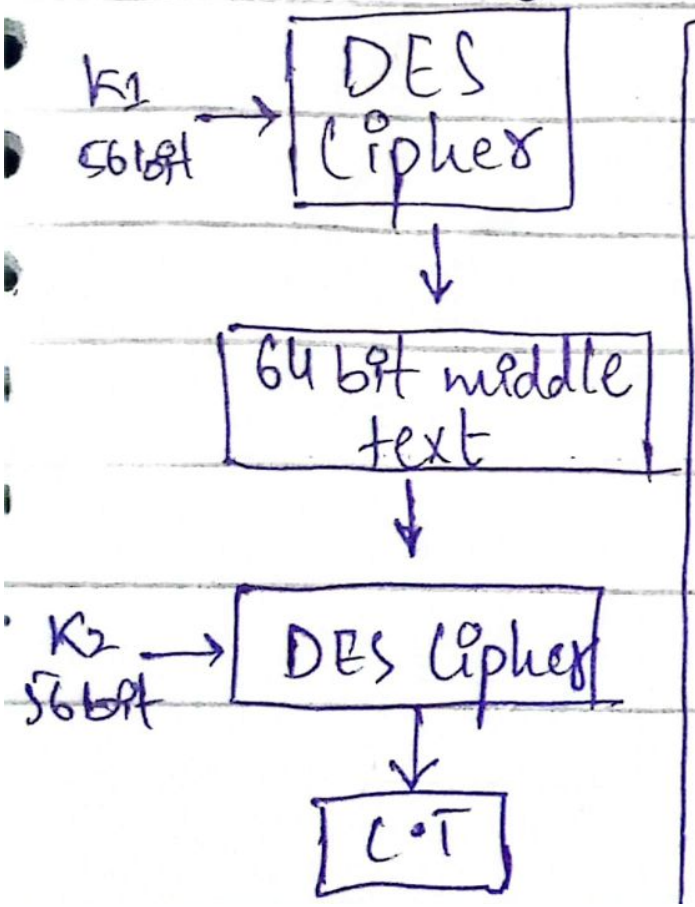
DONT	G	IT	GIVE	T	Them

{IS}

⇒ Multiple DES

1) Double DES (2 DES)

↓ 64 Bit P.T



Encryption:

$C.T = E(K_2, E(K_1, P.T))$

Decryption:

$P.T = D(K_1, D(K_2, C$

⇒ DES

key = 64 bit

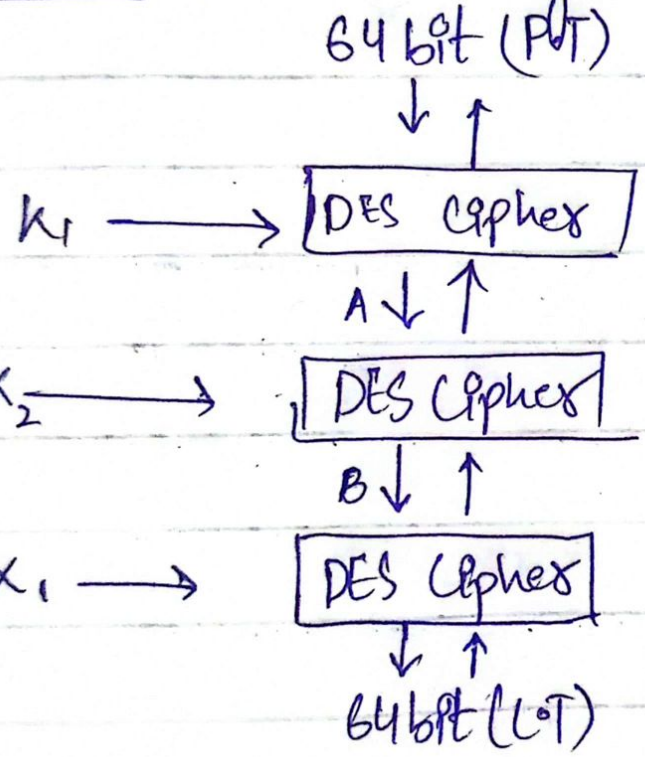
64 − 8 = 56

$2^{56} \cdot 2 = 2^{57}$

⇒ Meet-in-the-middle Attack :

If a person has both PT and CT he can generate possible outcomes of both keys using 56 combination and the middle text.

⇒ Triple DES (3DES with 2keys).



(3DES) using 3 keys

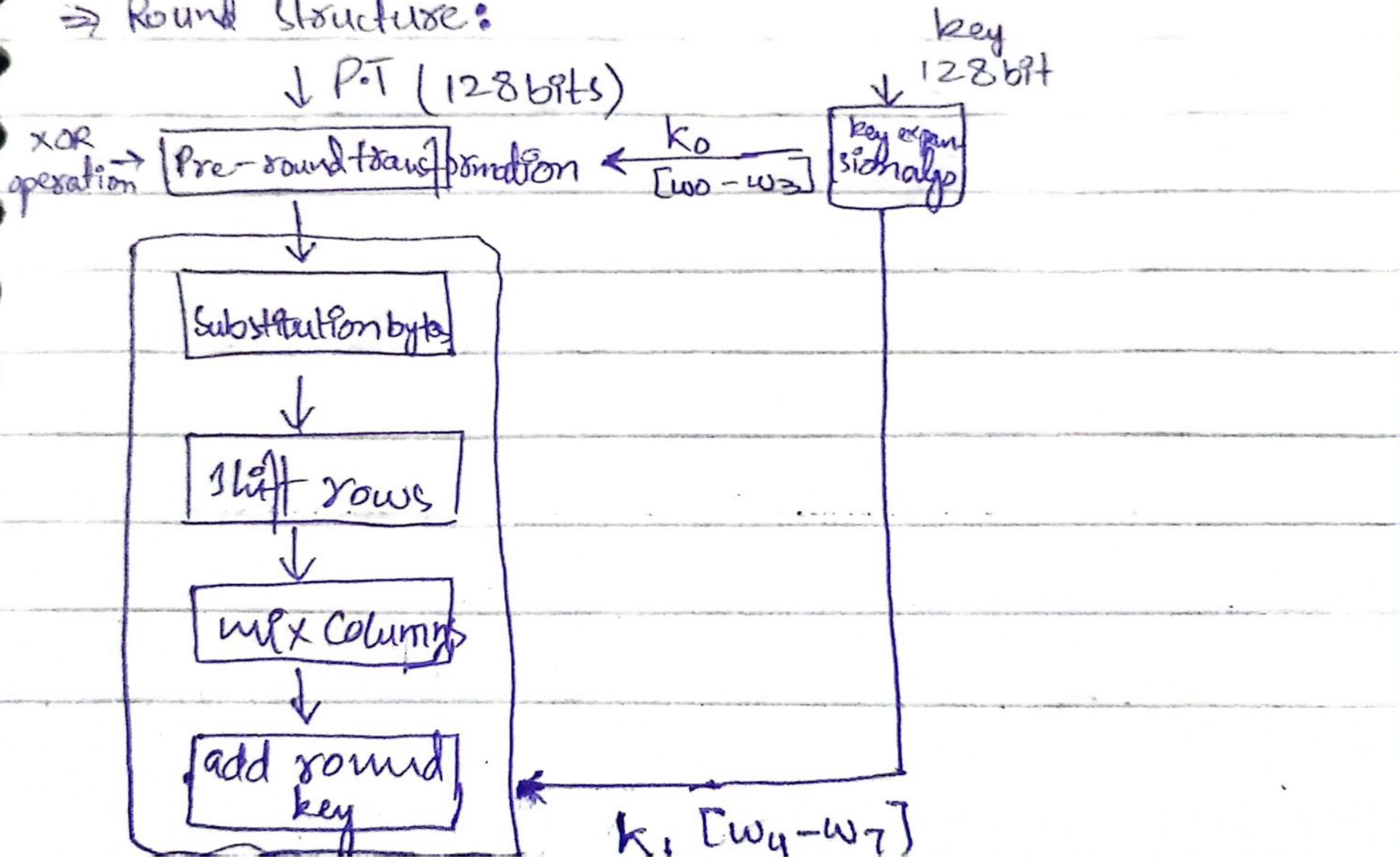
$C = E(K_3, D(K_2, E(K_1, P.T))$

$P.T = D(K_1, E(K_2, D(K_3, C.T)))$

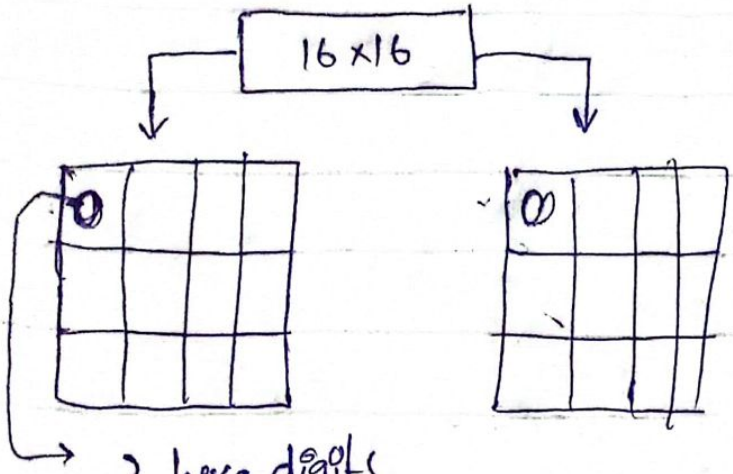
{IS}

Advanced Encryption Standard (AES)

⇒ Round Structure:



1) Substitution table (Bytes)



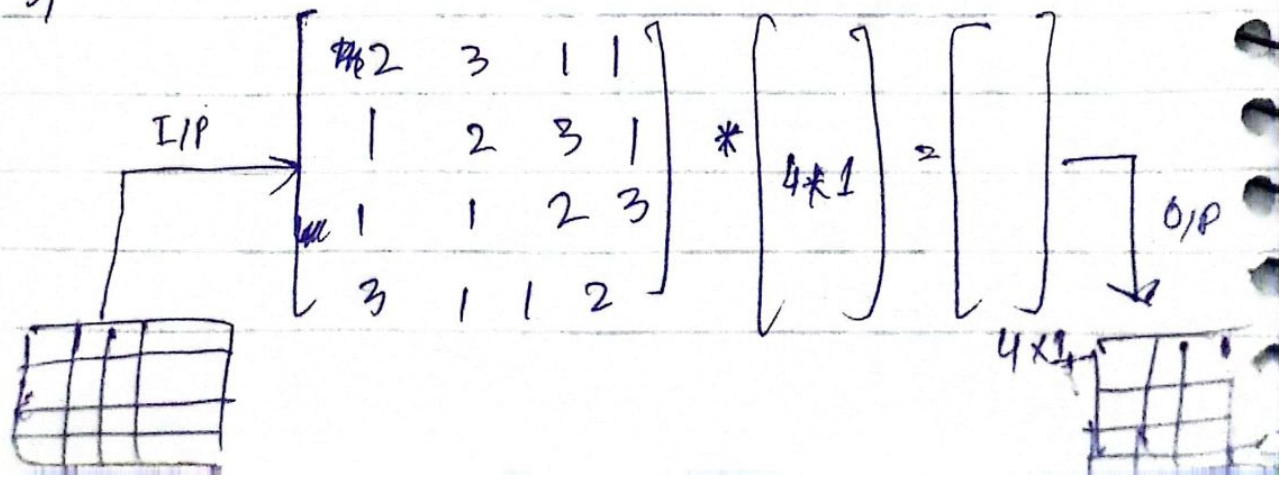
2)

R_0	63	C9	FE	30
R_1	F2	F2	63	26
R_2	C9	C3	7D	D4
R_3	BA	63	82	D4

↓ Shift to left by Row #

63	C9	FE	30
F2	63	26	F2
7D	D4	C9	C3
D4	BA	63	82

3)



{IS}

Eular's Totient Function:

⇒ $\phi(n)$

⇒ no. of +ve integers less than 'n' that are co-prime to 'n' where $(n \geq 1)$

Ex $\phi(1) = 1$

$\phi(5) = ?$

No. < 5 are → 1, 2, 3, 4

GCD(1,5) = 1

GCD(2,5) = 1 ⇒ $\phi(5) = 4$

GCD(3,5) = 1 $\phi(6) = ?$

GCD(4,5) = 1

⇒ Theorem

if 'x' & 'n' are positive coprime integers

then $x^{\phi(n)} \equiv 1 \bmod n$

⇒ $x^{\phi(n)} \bmod n = 1 \bmod n$

Ex

$x = 11, \quad n = 10$

$11^{\phi(10)} = 1 \bmod 10$

$\phi(10) = \phi(2) \times \phi(5)$

$= 1 * 4 = 4$

$= 11^4 \equiv 1 \bmod 10$

$1461 = 1 \bmod 10$

P

$x^{\phi(n)-a} \equiv 1 \bmod n$

Ex $11^{4*2} \equiv 1 \bmod 10$, $11^{40} \equiv 1 \bmod 10$

Ex $4^{99} \bmod 35$

$a = 4, n = 35 \rightarrow$ co-prime

By Euler's theorem

$4^{\phi(35)} = 1 \bmod 35$

$\phi(35) = \phi(7) * \phi(5)$

$= 6 * 4 = 24$

$\Rightarrow 4^{24} = 1 \bmod 35$

$\Rightarrow 4^{99} \rightarrow 4^{24*4+3}$

$= (4^{24})^4 \bmod 35$

$= +4^3 \bmod 35$

$= 1 \cdot 4^3 \bmod 35$

$= 64 \bmod 35$

$= 29 \bmod 35$

~~$3^{99} \bmod 13$~~

Ex $4^{532} \bmod 11$

$x^{n-1} \equiv 1 \bmod n$

$x^4, n = 11$

$4^{11-1} \equiv 1 \bmod 11$

$4^{10} \equiv 1 \bmod 11$

$4^{532} \rightarrow 4^{10*53+2}$

$\cdot 4^{(10)53} \cdot 4^2 \bmod 11$

$= (1 \cdot \bmod 11) \cdot (4^2 \bmod 11)$

$= 16 \bmod 11 = 8$

Fermat's Theorem:

⇒ Specific case of eulas's theorem where n is

RSA

zoom

-it