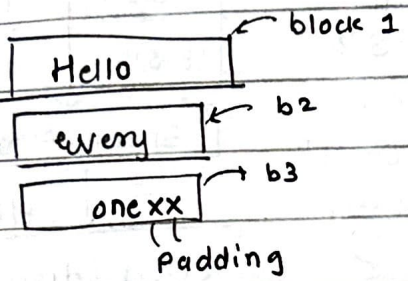
18/01/23

2. Block Cipher & Public Key Cryptography.

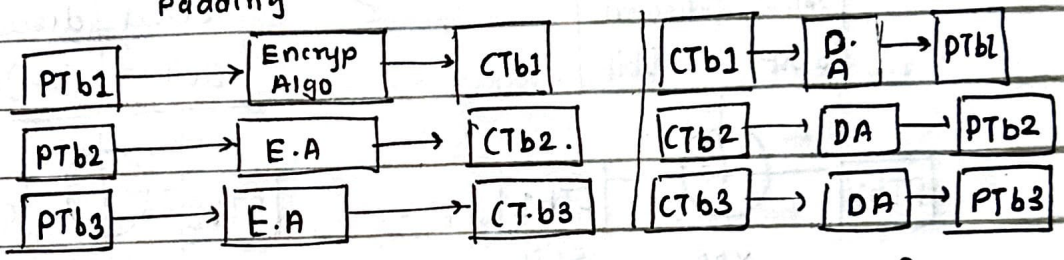
* BC operations (modes)

(1) ECB (Electronic code block)
(2) CBC (cipher Block chaining)
(3) CFB (Cipher Feedback block)
(4) OFB (output Feedback block)
(5) CTR (Counter mode).

Eg (1)
ECB →



Block = 5 size

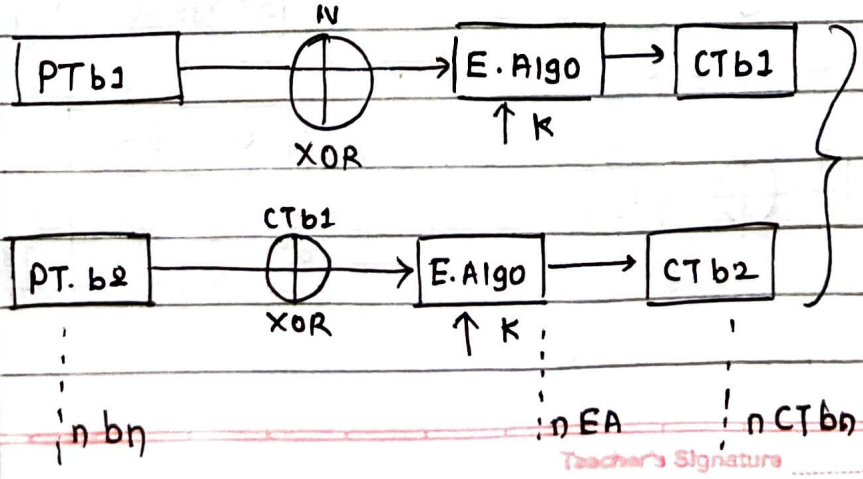


disadvantage:- Repeation of PT (same plain text) can cause same Cypher text.

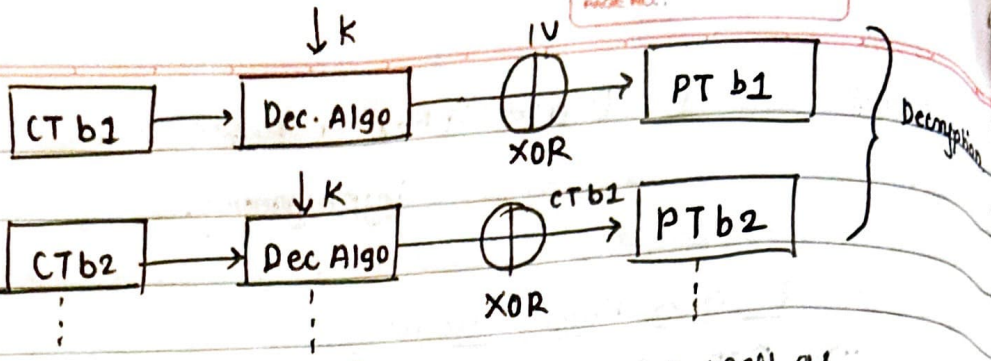
CBC (2) In CBC, if PT is same, because of initialization vector, the cipher text cant be same.

IV= initialization vector.

XOR operation

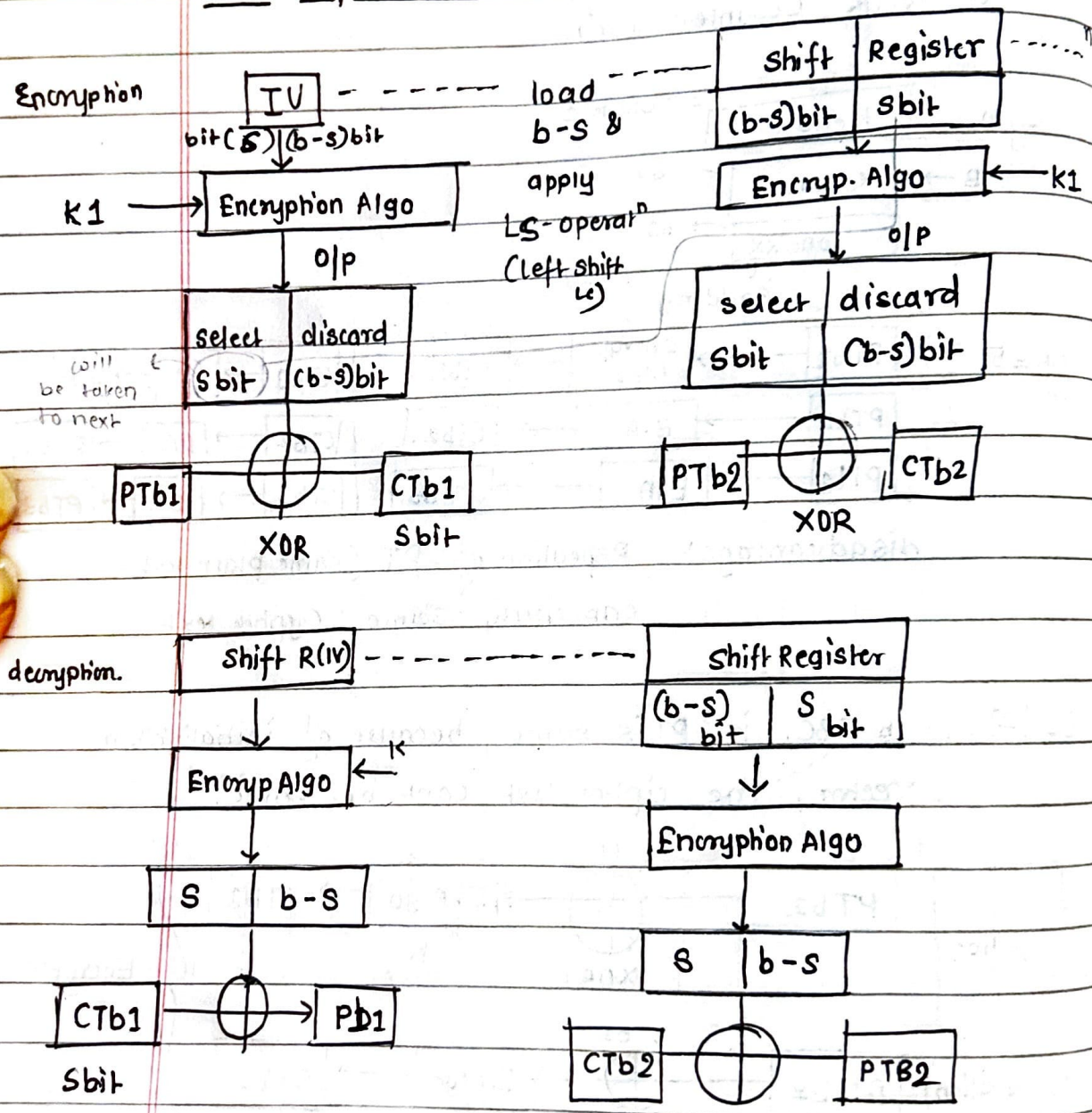


Teacher's Signature



- Same key is used for encryption as well as decryption.

(8) CFB (Cipher Feedback block)



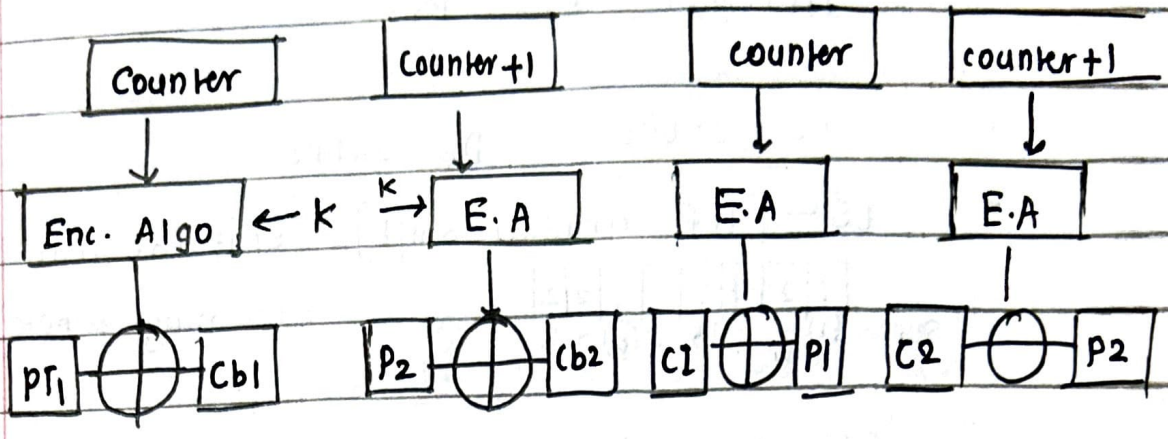
Teacher's Signature

(4) OFB

8 bit from o/p is taken on the other side

CT will not be considered as 8 bit.

(5) Counter mode.



* Data Encryption Standard. (DES)

PT → 64 bit

CT → 64 bit

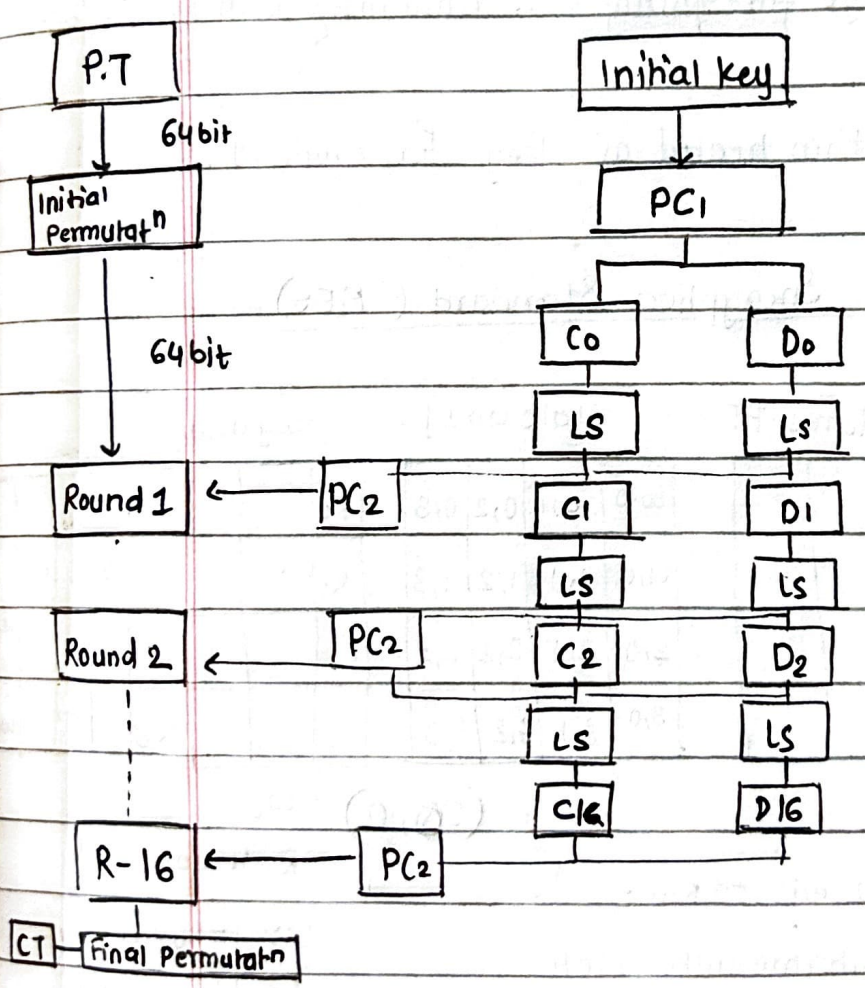
Round — 16

key size — 48 bit

PC_1 - (8 bit for parity)

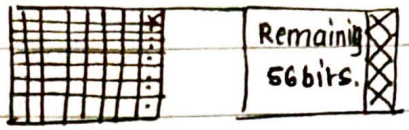
PC_2 - (8 bit for Rearrange, Permutation & selection)

PC [Permutated choice]

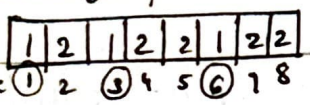


Teacher's Signature .....

- from the
  initial bits = 64 bits size.
  When we apply PC1, it removes 8th position from 64 bits, so total remaining will be 56 bits.



- C_0 = 28 bits D_0 = 28 bits
- LS – [left circular shift], shif the desired by 1 remaining denote by 2.

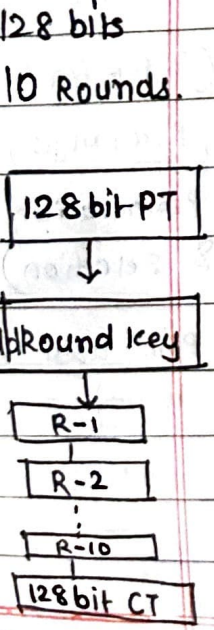


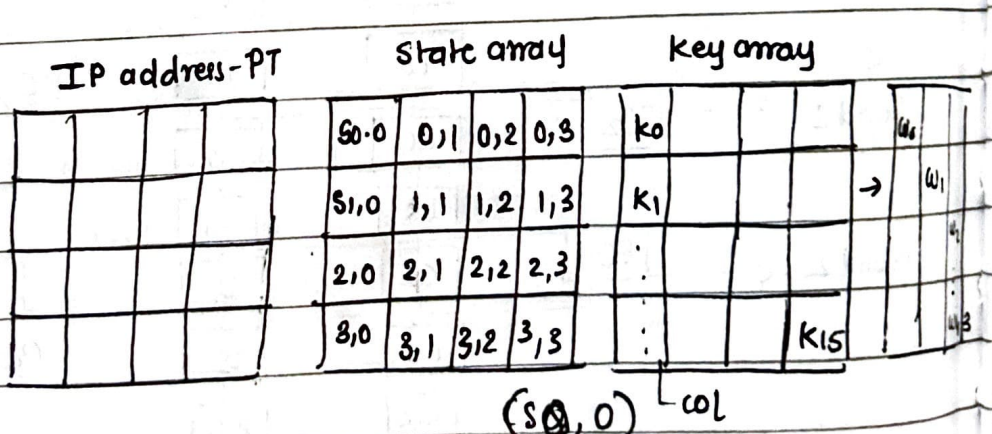
- After performing LCS, we get output i.e, C1 & D1.
- C1 (28) D1 (28) = 56 bits will go to PC1, where 8 bits will go for parity, ∴ remaining will be 48 bits.

48 bit is then treated as key for round 1.

* Advanced Encryption Standard (AES)

128 bits
10 Rounds.





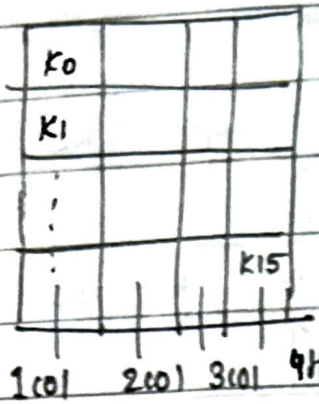
State array used to store intermediate state within the round

Teacher's Signature .....

- Sta $S(0,0)$
  byte / word. (total 4 words)

  (1 byte = 8 bits)

- each cell has 8 bits i.e 1 byte stored.

- 

  ∴ total round 10

  ∴ 10 × 4 colms

  = 40 + (4) Round key words.

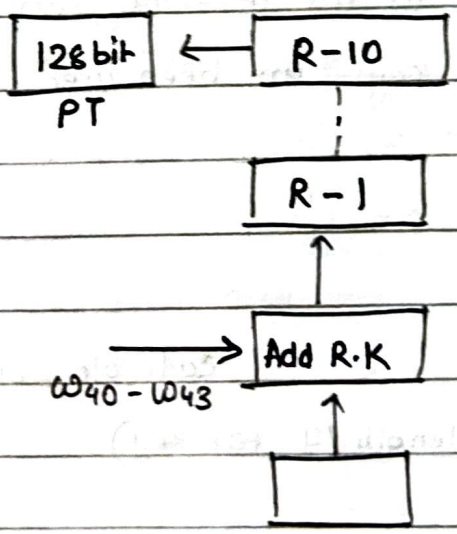
  = 44

- Whole column is represented in 1 word. ∴ there are 4 words (∵ 4 columns).
- In each round we have 4 words/steps.

  R1 (W_0 - W_3)

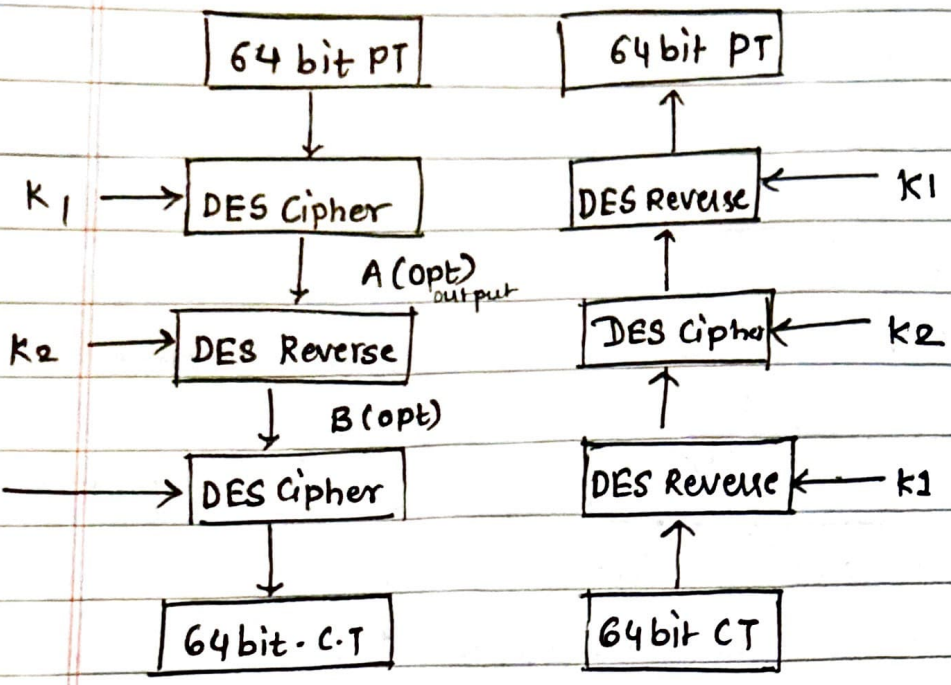
  R2 (W_4 - W_7)

- Decryption:



Teacher's Signature .....

* Triple DES



* * Blowfish Algorithm

- Symm key crypto
- 64 bit PT (I/P) (input)
- key size → variable length key (32 - 448)
- The key length will be changing throughout, hence it is more secure as the attacker cant recognize actually how many key's are been used.
- Each Block size is 32 bit.

[I] Key Generation

① - Stored in Array — Each block size = 32bit.

- 14 → size (max length 14 for key)
- $(1 \leq n \leq 14)$
- There are 14 block each of 32 bit.

$\therefore 14 \times 32 = 448$

- $K_1 \ldots K_2 \ldots K_3 \ldots \ldots K_{14}$
- 32, 64, 96 448

} ∴ There is change in size of key in each step.

Teacher's Signature

(2) Initialize P array (P) → array.

- Total size = 18 (word) (P1, P2 .... P18)
- length of each word = 32 bit.

(3) Initialize S. boxes (Substitution box)

S1 = S0 ..... S255

S2 = S0 ..... S255

S3 = S0 ..... S255

S4 = S0 ..... S255

(4) Initialize each element of P array & S box with Hexadecimal values

(5) XOR operations are performed.

P1 = P1 XOR K1

P2 = P2 XOR K2

P14 = P14 XOR (K14) → limitation of K.

P15 = P15 XOR (K1) → restart.

P18 = P18 XOR K4

(6) Take 64 bit PT (initially all bit are 0)

PT(0.....)

After assigning '0' ~~key~~ (sub keys) are generated.

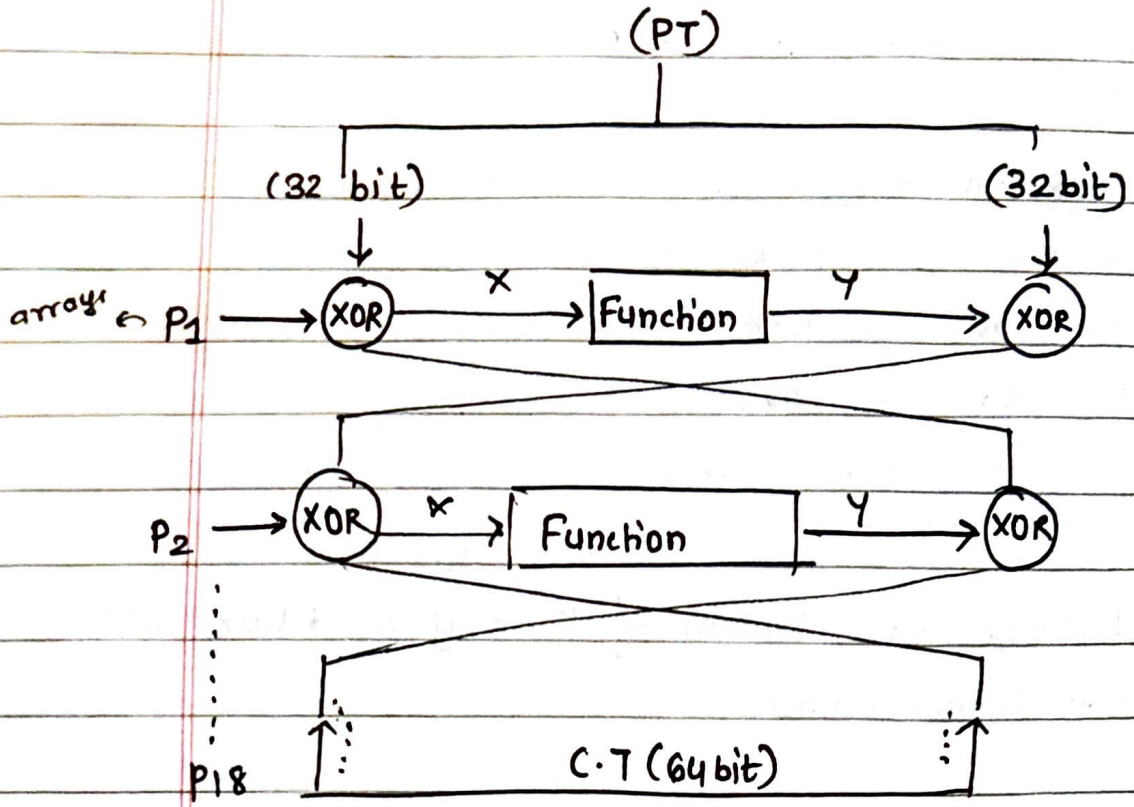
[II] DATA ENCRYPTION

~~(PT)~~

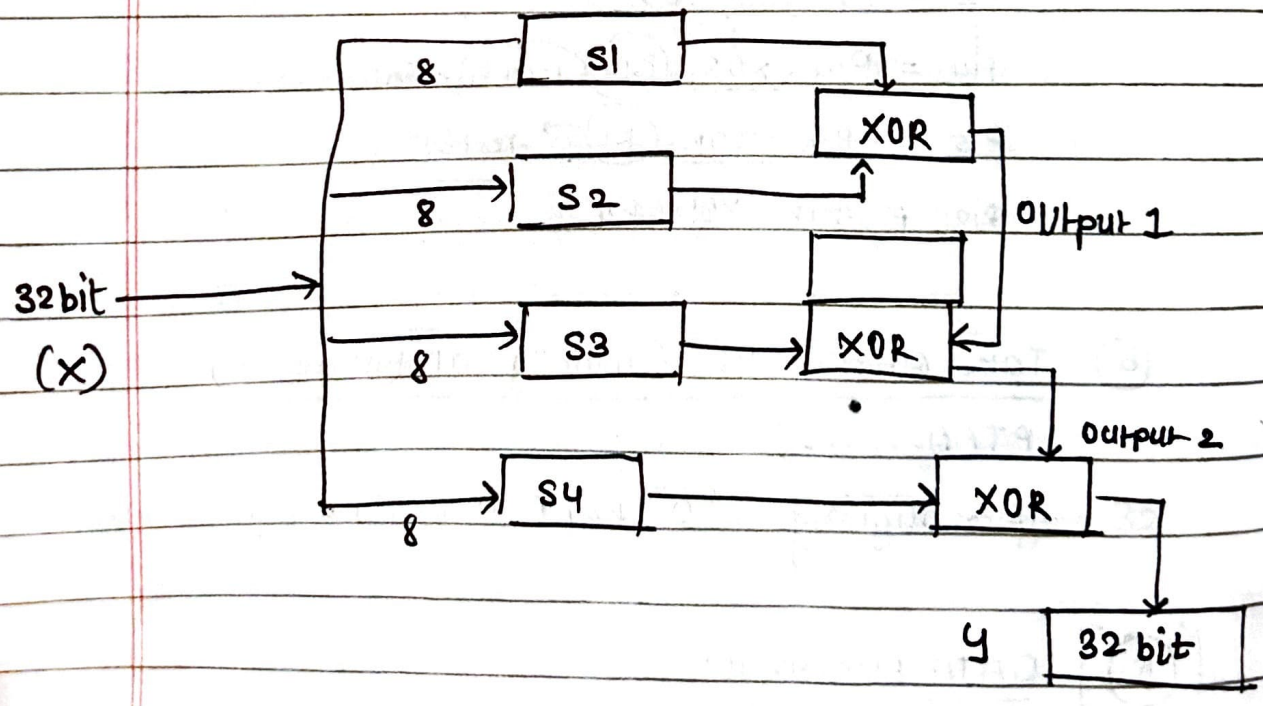
(P.T.O)

Teacher's Signature .....

II DATA ENCRYPTION



Representation of Function (function part)



Teacher's Signature

* RSA Algorithm

(I) Key Generation.

(i) Select 2 prime number. p and q

(ii) calculate $n = p \times q$

(iii) calculate $\phi(n) = (p-1) \times (q-1)$

(iv) choose the value of e such that $(1 < e < \phi(n))$
and $gcd(\phi(n), e) = 1$ ---- it should not be divisible by $\phi(n)$.
& should not be the factor.

(v) calculate d

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

$ed = \bmod \phi(n)$, $ed \bmod \phi(n) = 1$

(vi) Public key = (e, n) → Encryption.

(v) Private key = (d, n) → Decryption.

(II) Encryption

$$\boxed{C = m^e \bmod n}$$

m = no. of digit in msg (PT)

C = Cipher text.

Assume $(m < n)$

(III) Decryption

$$\boxed{(PT) = c^d \bmod n.}$$

Teacher's Signature

Example :- P=3, Q=11, m=31

→ ① $n = P \times Q = 33$

② $\phi n = (P-1)(Q-1) = (2)(10) = 20$

③ find e,

$\phi(n) = 20$

gcd = 2, 2, 5

∴ e = 1, 3, ~~5~~, (7), 11, ...

(e = 7)

④ $\boxed{ed \bmod \phi(n) = 1}$

$7 \times d \bmod 20 = 1$

$\boxed{d = 3}$

⑤ Public key = (e, n) = (7, 33)

⑥ Private key = (d, n) = (3, 33)

II Encryption:-

$C = m^e \bmod n$

$= (31)^7 \bmod 33$

$= \left[(31)^3 \bmod (33)\right]\left[(31)^3 \bmod (33)\right]\left[31 \bmod 33\right] \bmod (33)$

= 29791

= [25][25][31]

= 19375 mod 33

= 4

III Decryption

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

$= 4^3 \bmod (33)$

$= 64 \bmod (33)$

= 31.

Teacher's Signature

Example: $p = 7,\ Q = 13,\ M = 42$

① $n = 7 \times 13 = 91$

② $\phi(n) = (p-1)(q-1) = (6)(12) = 72$

③ Find e,

$\phi(n) = 72$

$gcd = 2 \times 3 \times 2 \times 2 \times 3$

$= 2, 3, 4$

$e = 1, 8, 5, 7, 11 \ldots$

$e = 5$

④ $\boxed{d = \frac{1 + K(\phi(n))}{e}} = \frac{1 + 2(72)}{5} = \frac{145}{5}$

$\boxed{d = 29}$

⑤ Public key $= (e, n) = (5, 91)$

⑥ Private key $= (d, n) = (29, 91)$

I Encryption

$C = m^e \bmod n$

$= (42)^5 \bmod 91$

$= 130691232 \bmod 91$

$C = 35$

III Decryption

$(PT) = C^d \bmod n$

$= (35)^{29} \bmod 91$

$= \left[\left[(35)^6 \bmod 91\right]\left[(35)^6 \bmod 91\right]\left[(35)^6 \bmod 91\right]\left[(35)^6 \bmod 91\right]\left[(35)^5 \bmod 91\right]\right] \bmod (91)$

$= \left[1838265625 \bmod 91\right] = 14$ | $52521875 \bmod 91$

Teacher's Signature .....

$= [14][14][14][14][42] \bmod (91)$

$= 1613472 \bmod 91$

$= (42)$

* **Digital signature (DS)**

$$C = m^e \bmod (n)$$

$$(DS) \quad C = m^d \bmod (n)$$

$$PT = C^d \bmod (n)$$

$$(DS) \quad PT = C^e \bmod (n)$$

- public key = (d, n)
- private key = (e, n)

31/1/23 * **KNAPSACK ALGORITHM**

(I) Key Generation

① Public key

② Private key.

Select 2 number. n & m

m > sum of all no. in sequence.

n = Select no. such that no common factor with m.

find public key → $(Di \times n) \bmod m$

Plain text.

(II) Encryption ⟹ CT = (PTi × Pub key i) +
(PTj × Pub key j) +
(PTn × Pub key n)

(III) Decryption n^{-1} ⟹ get x
calculate
(CT × x) mod m

Example (1) {1, 2, 4, 10, 20, 40} ⟹ wts

① D = {1, 2, 4, 10, 20, 40} = Private.
sum of seq = 76

② m > sof seq
∴ m > 76.
∴ m = 110 → factor of 110 → 2 × 5 × 11

③ ∴ n = 31 → prime no.

④ ... public key → (Di × n) mod m
(1 × 31) mod 110 = 31
(2 × 31) mod 110 = 62
(4 × 31) mod 110 = 14
(10 × 31) mod 110 = 90
(20 × 31) mod 110 = 70
(40 × 31) mod 110 = 30
Public key = {31, 62, 14, 90, 70, 30}

Encryp ⑤ PT = 100100 111001 011110
CT = (PTi × PKi) + (PTj × PKj) + ... (PTn × PKn)
1st part C1 = (1 × 31) + (0 × 62) + (0 × 14) + (1 × 90) + (0 × 70) + (0 × 30)

C1 = 121

Teacher's Signature

$C_2 = (1\times31) + (1\times62) + (1\times14) + (1\times90) + (70\times0) + (0\times30)$

$= 197$

$C_3 = (1\times31) + (0\times62) + (1\times14) + (1\times90) + (1\times70) + (0\times30).$

$= 205$

$CT = \{121, 197, 205\}$

⑥ Decryption $n^{-1} = 31^{-1}$

To find n inverse,

$n \times x \bmod 110 = 1$

$\therefore 31 \times x \bmod 110 = 1$

$31 \times 71 \bmod 110 = 1$

$\boxed{x = 71}$

$(CT \times x) \bmod m$

$CT = \{121, 197, 205\}$. , $D = \{1, 2, 4, 10, 20, 40\}$

$= (121 \times 71) \bmod 110 = 11 \rightarrow (100100)$

$= (197 \times 71) \bmod 110 = 17 \rightarrow (111100)$

$= (205 \times 71) \bmod 110 = 35 \rightarrow$ (

Example ⑫ ★IA Private key = $\{1, 2, 4, 7, 12, 20, 33, 54\}$

$n = 147$

$m = 250$

$D = \{01100110)$

Eg. ③ Private key = $\{2, 3, 6, 13, 27, 52\}$

$n = 31$

$m = 105$

PT = 110101

Ex.2 P = {1, 2, 4, 7, 12, 20, 33, 54}

m = 250

n = 147

Public key = (Di x n) mod m

- 147 = (1 x 147) mod 250 = 147
- 294 = (2 x 147) mod 250 = 44
- 588 = (4 x 147) mod 250 = 88
- 1029 = (7 x 147) mod 250 = 29
- 1764 = (12 x 147) mod 250 = 14
- 2940 = (20 x 147) mod 250 = 190
- 4851 = (33 x 147) mod 250 = 101
- 7938 = (54 x 147) mod 250 = 188

① Public key = {147, 44, 88, 29, 14, 190, 101, 188}

② PT = 01100110

C1 = (0 x 147) + (1 x 44) + (1 x 88) + (0 x 29) + (0 x 14) + (1 x 190) + (1 x 101) + (0 x 188)

C1 = 423

③ Decryption: $n^{-1} = 147^{-1}$

147 x mod 250 = 1

x =

CT = 423 → (423 x) mod 250

Teacher's Signature .....

e3 : Private key

2/2/23

* Deffie Hellman key Exchange Algorithm

(1) Consider a prime no. q

(2) Select α ..... $\alpha < q$ & α is primitive root

(3) X_A ..... $X_A < q$ (X_A private key of A

$$Y_A = \alpha^{X_A} \bmod q$$

(4) X_B (Private key of B) & $X_B < q$

$$Y_B = \alpha^{X_B} \bmod q$$

(5) Calculate secret key k_1 & k_2

k_1 = Person A

k_2 = Person B

$$k_1 = (y_B)^{X_A} \bmod q$$

$$k_2 = (y_A)^{X_B} \bmod q$$

Example:- $q = 7$

1) find α,

PT = { 1, 2, 3, 4, 5, 6 }

find α such that ~~$\alpha = 5$~~ it shouldn't be repeating value. $\alpha^n \bmod q$ { here 1-6 }

eg. $\therefore \alpha^1 \bmod q = 1$ $\quad \alpha^1 \bmod = 1$

$\alpha^2 \bmod q = 1$ ✗ $\quad \alpha^2 \bmod = 2$ ✓

$\alpha^3 \bmod q = 2$ $\quad \alpha^6 \bmod = 3$

α^6

Teacher's Signature .....

(2) $X_A = 3$, $X_B = 4$

(i) $Y_A = \alpha^{X_A} \bmod q$

$Y_A = 5^3 \bmod 7$

$\boxed{Y_A = 6}$

(ii) $Y_B = \alpha^{X_B} \bmod q$

$y_B = 5^4 \bmod q$

$\boxed{y_B = 2}$

(3) $K_1 = (y_B)^{X_A} \bmod q$

(i) $K_1 = (2)^3 \bmod 7$

$\boxed{K_1 = 1}$

(ii) $K_2 = (y_A)^{X_B} \bmod q$

$K_2 = (6)^4 \bmod 7$

$\boxed{K_2 = 1}$

$\therefore \boxed{K_1 = K_2}$ the message can be successfully exchanged.

* ElGamal Cryptography (No relation between keys)

(I) Key Generation.

(1) Select large prime no. p

(2) Select decryption key D (Also known as Private)

(3) Select Encryption key OR E_1

(4) Select $E_2 = E_1^D \bmod p$.

(5) Public key (E_1, E_2, P, D)

II Encryption

(1) Select Random integer (R) (If given)

(2) $C_1 = E_1^R \bmod P$

(3) $C_2 = (PT \times E_2^R) \bmod P$

(4) $CT = (C_1, C_2)$

III Decryption

$$PT = \left[C_2 \times (C_1^D)^{-1}\right] \bmod p.$$

Q Example $PT = 7$

(D) Privatekey = 3

$E_1 = 2$

assume Prime No. (P) = 11

Sol:- $E_2 = E_1^D \bmod p$

$E_2 = 2^3 \bmod 11$

$\boxed{E_2 = 8}$

(II) Encryption:-

random integer = 2

$C_1 = E_1^R \bmod P$

$= 2^2 \bmod 11$

$\boxed{C_1 = 4}$

$C_2 = (PT \times E_2^R) \bmod P$

$C_2 = (7 \times 8^2) \bmod 11$

$\boxed{C_2 = 8}$

Teacher's Signature

CT. (4, 8)

(iii) Decryption.

$$PT = [C_2 \times (C_1^D)^{-1}] \bmod p.$$

$$= [8 \times (4^3)^{-1}] \bmod 11$$

$$= \left[8 \times \frac{1}{64}\right] \bmod 11.$$

$$\therefore (C_1^D)^{-1}$$

$$= (C_1^D)\, x \bmod p = 1$$

$$= (4^3)\, x \bmod p = 1$$

$$= 64 \times x \bmod 11 = 1$$

$$\therefore 64 \times (5) \bmod 11 = 1$$

$$(x = 5)$$

$$\therefore [8 \times 5] \bmod 11$$

$$= (7)$$

Decryption = 7

PT = Decryption.

[Q] Alice and Bob get a public key no. 23 & 9
Alice have Private key = 4
Bob private key = 3
compute the public key of Alice & Bob
and what will be the symmetric key value.

Teacher's Signature