Cryptography :-

⇒ Classical Encryption Techniques :-

1, Substitution :- Caesar, monoalphabetic, Playfair, Hill, polyalphabetic, one-Time pad

2, Transposition :- Rail fence & row column Transposition

(1) Key

i, Caesar Cipher :- (replace (3) alphabet future down)

Ex:- 0 1 2 3 ---- 23 24 25
A B C D ---- X Y Z

P :- V I S H N U K = 3.

C(V) = E(p, K) mod 26 C(H) = 10
= (P+K) mod 26 = K
= (21+3) 26 C(N) = Q
= (24) 26 C(U) = X
= 24
= Y

C(I) = (8+3) 26 ∴ Cipher text = YLVKX
= 11 26
= L

C(S) = (18+3) 26 Note :- If the key = 3 then
= (21) 26 it is Caesar cipher. Else
= V Shift Cipher. (Key = 2, 4, 5 ...)

(2) iii, Playfair Cipher :-

Plaintext :- hide the gold under the carpet

Key :- Neso Academy

Diagrams

Hi	de	th	eg	ol	dU	nd	er	th	eC	ar	pe	tx		
IK	GD	QK	dp	NR	CV	EC	Op	QK	ND	OT	ND	RZ		

N	E	S	O	A
C	d	M	V	B
F	G	H	I/J	K
L	P	Q	R	T
U	V	W	X	Z

iv, Hill cipher:-

$C = E(K, P) = (P \times K) \bmod 26$

$P = D(K, C) = CK^{-1} \bmod 26 = P \times K \times K^{-1} \bmod 26$

$$(C_1 C_2 C_3) = (P_1 P_2 P_3) \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \bmod 26$$

$C_1 = |P_1 K_{11} + P_2 K_{12} + P_3 K_{13}| 26$

$C_2 = |P_1 K_{21} + P_2 K_{22} + P_3 K_{23}| 26$

$C_3 = |P_1 K_{31} + P_2 K_{32} + P_3 K_{33}| 26$

Encryption EMO

~~Encryption~~ ~~EMVA~~

$$Key = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

$$\Rightarrow (C_1 C_2 C_3) = (4\ 12\ 14) \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

$= ((4 \times 17) + (12 \times 21) + (14 \times 2)$

$(4 \times 17) + (12 \times 18) + (4 \times 2)$

$(4 \times 5) + (12 \times 21) + (4 \times 19)$

$= (348\ 312\ 538) \bmod 26$

$= (10\ 0\ 8)$

$= (K\ A\ S)$

Decryption Key $= \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$ $K^{-1} = \frac{1}{\text{Det } K} \text{Adj } K$

$$\text{Det}\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} = \left| 17(18\times19 - 2\times21) - 17(21\times19 - 2\times21) + 5(21\times2 - 2\times18) \right| \bmod 26$$

$$= |-939| \bmod 26$$

$$= -3 \bmod 26$$

$$= 23$$

$$\text{Adj}(K) = \begin{vmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{vmatrix} = \begin{bmatrix} 18 & 21 & 21 & 18 \\ 2 & 19 & 2 & 2 \\ 17 & 5 & 17 & 17 \\ 21 & 21 & 21 & 18 \end{bmatrix}^T$$

$$= \begin{bmatrix} 300 & -357 & 6 \\ -313 & 313 & 0 \\ 267 & -252 & -51 \end{bmatrix}^T \Rightarrow \begin{bmatrix} 300 & -313 & 267 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{bmatrix} \bmod 26$$

$$= \begin{vmatrix} 14 & -1 & 7 \\ -19 & 1 & -18 \\ 6 & 0 & -25 \end{vmatrix} \bmod 26$$

Add 26 to -ve values

$$\Rightarrow \begin{bmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{bmatrix}$$

$$K^{-1} = \frac{1}{23}\begin{bmatrix} 14 & 23 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{bmatrix} \bmod 26$$

~~Ciphertext = KAS~~

~~$P_1P_2P_3 = (K\ A\ S)$~~

(A-1) $= 23^{-1} \begin{bmatrix} 14 & 23 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{bmatrix} \bmod 26$

↳ Extended Euclidean Alg. (KESO Academy)

$= 17 \times \begin{bmatrix} 14 & 23 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 4 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 4 & 9 & 15 \\ 17 & 7 & 6 \\ 24 & 0 & 17 \end{bmatrix}$

Cipher text = (K A S)

$\Rightarrow P_1 P_2 P_3 = (K A S) \begin{bmatrix} 4 & 9 & 15 \\ 17 & 7 & 6 \\ 24 & 0 & 17 \end{bmatrix} \bmod 26$

$= (10\ 0\ 8) \begin{bmatrix} 4 & 9 & 15 \\ 17 & 7 & 6 \\ 24 & 0 & 17 \end{bmatrix} \bmod 26$

$= [(10\times4)+(0\times17)+(8\times24) \quad (10\times9)+0+0 \quad (10\times15)+0+(8\times17)]$

$= [472 \quad 90 \quad 286] \bmod 26$

$= (4\ 12\ 14)$

$= [E\ M\ O]$ //

V, Polyalphabetic Cipher: (Vigenere Cipher)

Key :- deceptivedeceptivedeceptive

plain text :- wearediscoveredsaveyourself.

Key	3	4	2	4	15	19	8	21	4	3	4	2	4	15	19	8	21	4	3	4
PT	22	4	0	17	4	3	8	18	2	14	21	4	17	4	3	18	0	21	4	24
CT	25	8	2	21	19	22	16	13	6	17	25	6	21	19	22	8	21	25	7	2

Key	2	4	15	19	8	21	4
PT	14	20	17	18	4	11	5
CT	16	24	6	11	12	6	9

} (Key + PT = CT).

(b) Vernam Cipher :- $C_i = K_i \oplus P_i$

↳ Key is random (cons) $P_i = K \oplus C_i$

2. (a) Rail fence Tech :-

PT = Vishnu using mac laptop

Depth = 2

V		S		N		U		I		G		A		C		P		O	
	i		H		U		S		N		M		C		A		T		P

CT (row wise) = VSNUIGALPOIHUSNMCATP

(b) Rail column Transposition :-

PT = Kill Corona Virus! at twelve am tomorrow

~~Key = hexa~~ 4 3 1 2 5 6 7

Key

K	I	L	L	C	O	R
O	N	A	V	I	R	U
S	A	T	T	X	E	L
V	E	A	M	T	O	M
O	R	R	O	W	Y	Z

CT: Each column has a key value, write the column value in ascending order.

⇒ [illegible]

This CT generating can be repeated to increase security.

Abstract Algebra & Number theory

* Modern crypto
* plaintext & ciphertext
* Most encryption is based heavily on number theory.
* Abstract Algebra.
* No major contribution of calculus & Trigonometry.

⇒ Concepts

- The Division Algorithm.
- The Euclidean Algorithm.
- The Extended Euclidean Algo
- modular Arithmetic.
- Groups, rings, fields & finite fields
- polynomial Arithmetic.
- prime Numbers
- Fermat's & Euler's Theorem
- Testing for primality
- The chinese remainder theorem.
- Discrete logarithms.

Prime Numbers:

* Has exactly two divisors - 1 & itself
* All numbers have prime factors.

⇒ Modular Exponentiation:

Q $31^{5000} \bmod 30 = 1^{5000} \bmod 30$ (1 is because is small mod of 30 for 31)
$= 1 \bmod 30$
$= 1$ //

Q $242^{329} \bmod 243$
$= -1^{329} \bmod 243$
$= -1 \bmod 243$
$= 242$ //

Q $11^{7} \bmod 13 = -2^{7} \bmod 13$
$= -2^{6} \times -2 \bmod 13$
$= -128 \bmod 13$
$= -11 \bmod 13$
$= 2$

Q, $88^{7} \bmod 187$

Sol $88^{1} \bmod 187 = 88$
$88^{2} \bmod 187 = 77$
$88^{4} \bmod 187 = 132$
$88^{7} \bmod 187 = (88^{4} \times 88^{2} \times 88^{1}) \bmod 187$
$= (132 \times 77 \times 88) \bmod 187$
$= 894432 \bmod 187 = 11$

⇒ 11 //

$3^{32} = 3^{16} \times 3^{16} \bmod 29$

$= -9 \times -9 \bmod 29$

$= 81 \bmod 29$

$= 23$ or -6

$3^{64} = 3^{32} \times 3^{32} \bmod 29$

$= -6 \times -6 \bmod 29$

$= 36 \bmod 29$

$= 7$

$3^{100} = 3^{64} \times 3^{32} \times 3^4$

$= 7 \times -6 \times -6$

$= 7 \times 36 \bmod 29$

$= 252 \bmod 29$

$= 20$ //

GCD - Euclidean Algo

	12	133
Divisors	1, 2, 3, 6, 4, 12	1, 3, 11, 33
Common Divisors	1, 3	
GCD	3	

Euclid for GCD $\Rightarrow$ (12, 33)

Q	A	B	R
2	33	12	9
1	12	9	3
3	9	3	0
✗	3	0	✗

GCD (750, 900)

Q	A	B	R
1	900	750	150
5	750	150	0
	150	0	

⇒ 150 //

Q; (252, 105)

Q	A	B	R
2	252	105	42
2	105	42	21
2	42	21	0
	21	0	

⇒ 21 //

Q (1005, 105) =

Q	A	B	R
9	1005	105	60
1	105	60	45
1	60	45	15
3	45	15	0
	15	0	

⇒ 15 //

Note: If $b \neq 0$

return gcd(b, a mod b)

⇒ (Method 2)

Relatively prime (Co-prime): A & B are said to be Co-prime, if they have no prime factors in common & their only common factor id 1.

⇒ Gcd (a, d) = 1

* Co-prime

Q: (4, 13)

Q	A	B	R
3	13	4	1
4	4	1	0
	1	0	

Gcd (13, 4) = 1 ∴ relatively prime

Euler's Totient function:

Q: $\phi(8)$

⇒ Numbers less than 8 are 1, 2, 3, 4, 5, 6, 7

GCD	Relatively prime
GCD (1, 8) = 1	✓
GCD (2, 8) = 2	✗
(3, 8) = 1	✓
(4, 8) = 4	✗
(5, 8) = 1	✓
(6, 8) = 2	✗
(7, 8) = 1	✓

formulas:

Q, $\phi(5)$

Sol: $n=5$

n is a prime number

$\phi(n) = (n-1)$

$\phi(5) = (5-1)$

$\phi(5) = 4$

∴ 4 no that are lesser than 5 & relatively prime to 5.

Q, $\phi(31)$

Sol: $n = 31$ (Prime)

$\phi(n) = (n-1)$

$= 30$

Q $\phi(35)$

Sol: $n = 35$ (not prime)

two prime numbers 5 & 7

let $p=5$ & $q=7$

$\boxed{\phi(n) = (p-1) \times (q-1)}$

$\phi(35) = (5-1) \times (7-1)$

$= 4 \times 6$

$= 24$

Q $\phi(1000)$

Sol: $n = 1000$

factors $= 2^3 \times 5^3$

$p_1 = 2, p_2 = 5$

$\phi(n) = n \times \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)$

$= 1000\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)$

$= 1000\left[\frac{1}{2}\right]\left[\frac{4}{5}\right]$

$= 400$

Q, $\phi(7000)$

Sol: $n = 7000$

factors $= 2^3 \times 5^3 \times 7$

$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_3}\right)$

$= 7000\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right)$

$= 2400$

Fermat's little theorem:

* If p is a prime & a is a +ve int not divisible by 'p' then $\boxed{a^{p-1} \equiv 1 \pmod{p}}$

Q, $P = 5$ & $a = 2$

$\Rightarrow 2^{5-1} \equiv 1 \pmod{5}$

$= 2^4 \equiv 1 \pmod{5}$

$16 \equiv 1 \pmod{5}$

∴ fermat's little theorem holds true.

Q, $p = 13$ & $a = 11$

$\Rightarrow 11^{13-1} \equiv 1 \pmod{13}$

$\Rightarrow 11^{12} \equiv 1 \pmod{13}$

$\Rightarrow -2^{12} \equiv 1 \pmod{13}$

$\Rightarrow -2^{4*3} \equiv 1 \pmod{13}$

$\Rightarrow 16^3 \equiv 1 \pmod{13}$

$\Rightarrow 3^3 \equiv 1 \pmod{13}$

$27 \equiv 1 \pmod{13}$ ✓

Q, $p = 6$ & $a = 2$

Q p is not prime ∴ Not hold the theorem

Euler's theorem :

$$a^{\phi(n)} = 1 \bmod n$$

Q,

$a = 2, \quad n = 10$

$$2^{\phi(10)} = 1 \bmod 10$$

$$\phi(10) = 10 \times \left[1 - \frac{1}{2}\right]\left[1 - \frac{1}{5}\right]$$

$$= 4$$

$$\Rightarrow 2^4 = 1 \bmod 10$$

$$= 16 \equiv 1 \bmod 10 \qquad (16) \bmod 10 = 6$$

$\Rightarrow \therefore$ Euler's theorm does not hold $a = 2$ & $n = 10$

Q, $a = 10, n = 11$

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

$$\phi(11) = (n-1)$$

$$= 10$$

$$10^{10} = 1 \bmod 11$$

$$-1^{10} = 1 \pmod{11}$$

$$-1/-1 = 1 \pmod{11}$$

$\therefore$ It hold's true.

Primitive roots: α is said to be a primitive root of prime number p, if $\alpha^1 \bmod p, \alpha^2 \bmod p, \alpha^3 \bmod p \ldots \alpha^{p-1} \bmod p$ are distinct.

Q, is 2 a primitive root of prime number 5?

Sol:

$2^1 \bmod 5$	$2 \bmod 5 = 2$
$2^2 \bmod 5$	$4 \bmod 5 = 4$
$2^3 \bmod 5$	$8 \bmod 5 = 3$
$2^4 \bmod 5$	$16 \bmod 5 = 1$

∴ Yes, 2 is primitive root of prime 5

Q, 2 & 7.

$2^1 \bmod 7$	$2 \bmod 7 = 2$ ✓
$2^2 \bmod 7$	$4 \bmod 7 = 4$ ✓
$2^3 \bmod 7$	$8 \bmod 7 = 1$ ✓
$2^4 \bmod 7$	$16 \bmod 7 = 2$ ✗
$2^5 \bmod 7$	$4 \bmod 7 = 4$ ✗
$2^6 \bmod 7$	$8 \bmod 7 = 1$ ✗

∴ No, Not a primitive root.

Multiplicative Inverse :- $(A \times A^{-1} = 1)$

$\Rightarrow A \times A^{-1} \equiv 1 \bmod n$

Q, $3 \cdot x ? \equiv 1 \bmod 5$

$\Rightarrow 3 \times 2 \equiv 1 \bmod 6$

↳ multiplicative Inverse

If we have large prime then we use

Extended Euclidean Algo :

Q. ME of 3 mod 5 [A > B]

$T = T_1 - T_2 \times Q$

Q	A	B	R	T_1	T_2	T
1	5	3	2	0	1	1
1	3	2	1	1	-1	2
2	2	1	0	-1	2	-5
	1	0		2	-5	

$T = 1 + 1 \times 1$

$= 2 \times 1$

$T = 2$

$\Rightarrow 2$ is ME of 3 mod 5

$= -1 - 2 \times 2$

$= -5$

Q ME of 11 & 13 $\quad T = T_1 - T_2 \times Q$

Q	A	B	R	T_1	T_2	T
1	13	11	2	0	1	-1
5	11	2	1	1	-1	6
2	2	1	0	-1	6	-23
	1	0		6	-23	

6 is ME of 11 mod 13

$1 - (-1 \times 5)$ $\quad 1 - 5$

$-1 - 6 \times 2$ $\quad$ Filter

$-1 - 12$ $\quad 1 + 5$

$-1 - 20$ $\quad 26$

-21

Q 10 mod 11 ME?

$T = T_1 - T_2 \times Q$

Sol

Q	A	B	R	T_1	T_2	T
1	11	10	1	0	1	-1
10	10	1	0	1	-1	
	1	0		-1	11	

Q = 1 ✗

1 − (−1) × 10.

1 − (−10)

1 + 11

~~1 is ME of 10 & 11~~ ∴ -ve ~~T~~ $T_1 + T_2$

∴ −1 + 11 → mod y

~~$\Rightarrow 10 \times 1 \equiv 1 \pmod{11}$~~ $= 10$

Chinese Remainder Theorem :-

Q

$X \equiv a_1 \pmod{m_1}$

$X \equiv a_2 \pmod{m_2}$

$X \equiv a_n \pmod{m_n}$

$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \cdots + a_n M_n M_n^{-1}) \bmod M$

Q. $X \equiv 2 \pmod 3$

$X \equiv 3 \pmod 5$

$X \equiv 2 \pmod 7$

$\Rightarrow a_1 = 2 \quad m_1 = 3$

$a_2 = 3 \quad m_2 = 5$

$a_3 = 2 \quad m_3 = 7$

~~2.3~~ To find ⇒

m_1	m_1^{-1}	M
m_2	m_2^{-1}	
m_3	m_3^{-1}	

$M = m_1 \times m_2 \times m_3$

$M = 3 \times 5 \times 7$

$\boxed{M = 105}$

$M_1 = \frac{M}{m_1}$; $M_2 = \frac{M}{m_2}$; $M_3 = \frac{M}{m_3}$

$M_1 = \frac{105}{3}$ $M_2 = \frac{105}{5}$ $M_3 = \frac{105}{7}$

$M_1 = 35$ $M_2 = 21$ $M_3 = 15$

$M_1 \times M_1^{-1} = 1 \bmod m_1$

$35 \times ? = 1 \bmod 3$

$35 \times 2 = 1 \bmod 3$

$\boxed{M_1^{-1} = 2}$

$M_2 \times M_2^{-1} = 1 \bmod m_2$

$21 \times ? = 1 \bmod 5$

$21 \times 1 = 1 \bmod 5$

$\boxed{M_2^{-1} = 1}$

$M_3 \times M_3^{-1} = 1 \bmod m_3$

$\Rightarrow 15 \times ? = 1 \bmod 7$

$\Rightarrow 15 \times 1 = 1 \bmod 7$

$\Rightarrow M_3^{-1} = 1$

$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$

$= (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 105$

$= (140 + 63 + 30) \bmod 105$

$= 233 \bmod 105$

$\boxed{X = 23}$

Q $4X \equiv 5 \pmod 9$

$2X \equiv 6 \pmod{20}$

$X = 4^{-1} \times 5 \pmod 9$

$= 4^{-1} \pmod 9 \times 5 \pmod 9$

$= 7 \pmod 9 \times 5 \pmod 9 \Rightarrow 35 \pmod 7$

$X \equiv 8 \pmod 9$ — (1)

(2) $\rightarrow 2X \equiv 8 \pmod{20}$

$X = 2^{-1} \pmod{20} \times 6 \pmod{20}$

$= 10 \pmod{20} \times 6 \pmod{20}$

$= 60 \pmod{20}$

$X = 3 \pmod{20}$ — (2)

$X \equiv 8 \pmod 9$ & $a_1 = 8$ $m_1 = 9$

$X \equiv 3 \pmod{20}$ $a_2 = 3$ $m_2 = 20$

$M = m_1 \times m_2$

$M = 180$ $M_1 = \frac{M}{m_1}$; $M_2 = \frac{M_2}{m_2}$

$= \frac{180}{9}$; $= \frac{180}{20}$

$M_1 = 20$ $M_2 = 9$

$M_1 \times M_1^{-1} = 1 \bmod m_1$; $M_2 \times M^{-1} = 1 \bmod m_2$

$20 \times ? = 1 \bmod 9$; $9 \times ? = 1 \bmod 20$

$20 \times 5 = 1 \bmod 9$ $M_2^{-1} = 9$

~~$100 = 1 \bmod 9$~~ ~~$M_2^{-1} = 1$~~

$M_1^{-1} = 5$

$X = (a_1 \times M_1 M_1^{-1} + a_2 M_2 M_2^{-1}) \bmod M$

$= (8 \times 20 \times 5 + 3 \times 9 \times 9) \bmod 180$

$= (800 + 243) \bmod 180$

$= 1043 \bmod 180$

$X = 143$

Discrete logarithm problem

⇒ $g^x \bmod p$

Q $\log_2 9 \bmod 11$

⇒ $p=11$; $g=2$; $x=9$

$\log_g x \equiv n \pmod p$

$x = g^n \pmod p$

$9 = 2^n \pmod{11}$

let $n = 1, 2, 3, \ldots$

$9 = 2^6 \pmod{11}$

⇒ 9

Q, $4 \equiv 2^x \pmod 7$

$4 \equiv 2^2 \pmod 7$

2 is ans. or 5, or 11. —

Prime factorization & (Fermat's factoring method)

Primality testing :- (Miller - Rabin Primality Test)

Q, $n = 561$ is prime?

Sol $n-1 = 2^k \times m$

$560 = 2^5 \times 35 \Rightarrow$

$k = 4$

$m = 35$

Choosing $a = 2$ $1 < 2 < 560$

$b_0 = a^m \pmod n$

$= 2^{35} \pmod{561}$

$= 263$

is $b_0 \pm 1 \pmod{561}$? No

$b_1 = b_0^2 \pmod n$

$= 263^2 \pmod n$

$= 166$

$b_2 = b_1^2 \pmod n$

$b_3 = b_2^2 \pmod n$

$= 67^2 \pmod{561}$

$= 1$ composite # If 1 may be prime

$560 - 280$

$2^1 \downarrow$

$\frac{560}{2^2} = 140$

$\downarrow$

$\frac{560}{2^3} = 70$

$\downarrow$

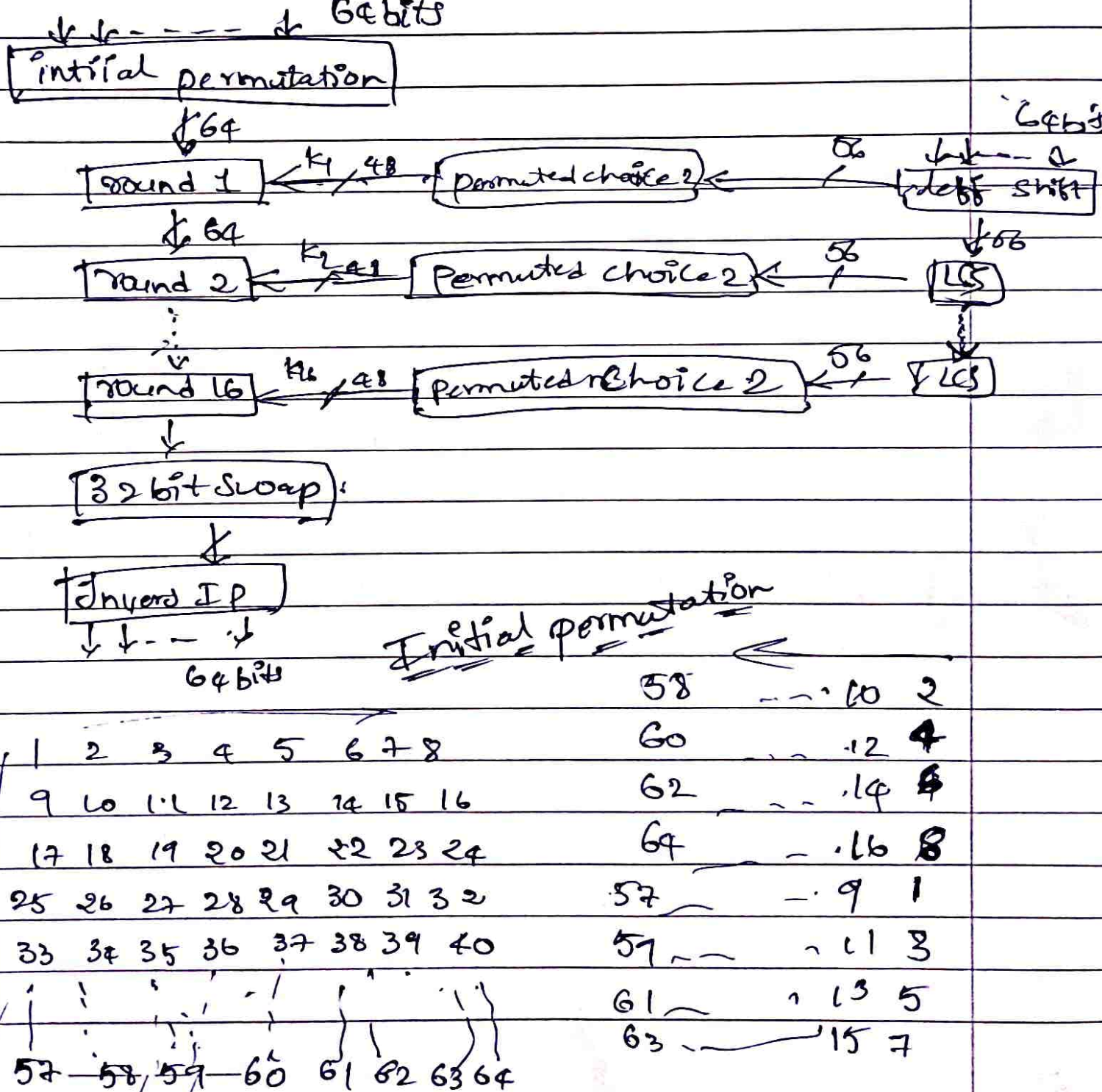
$\frac{560}{2^4} = 35$

$\downarrow$

$\frac{560}{2^5} = 17.5$ X

DES (Data Encryption Standard) :-

* PT size 64 bit
* CT size 64 bit
* Main key 64 bit
* Sub key 48 bit
* No of round : 16 rounds



Initial permutation

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
57	58	59	60	61	62	63	64

Initial permutation

58	→	10	2
60	→	12	4
62	→	14	6
64	→	16	8
57	→	9	1
59	→	11	3
61	→	13	5
63	→	15	7

Inverse IP

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14		22		30
37	5	45	13		21		29
36	4	44	12		20		28
35	3	43	11		19		27
34	2	42	10	50	18		26
33	1	41	9	49	17	57	25

In round we got some function :- $L_i = R_{i-1}$

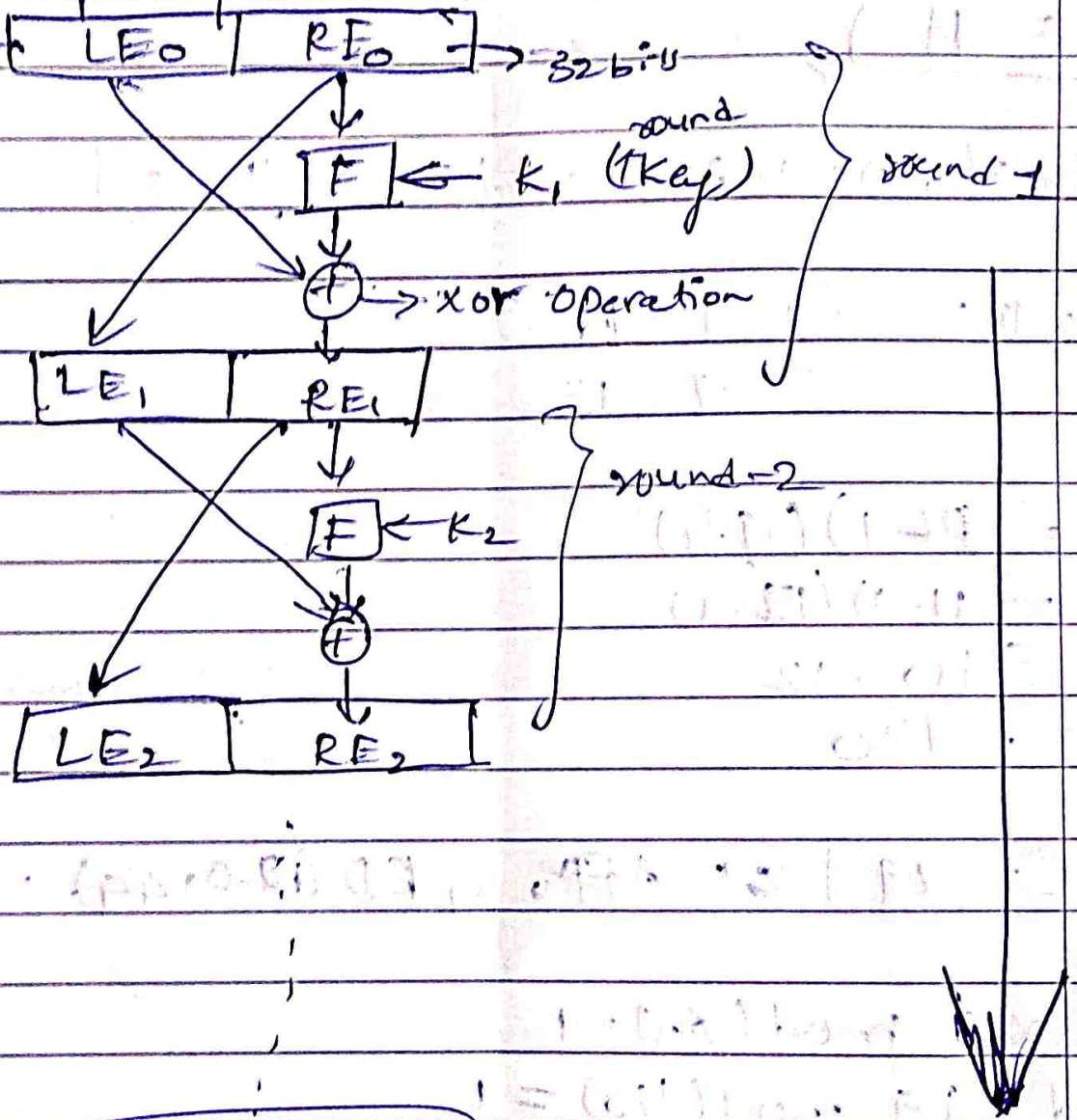
$R_i = L_{i-1} \oplus F(R_{i-1}, K)$

$\Rightarrow F(R_{i-1}, K_i) \Rightarrow$ mangalor function

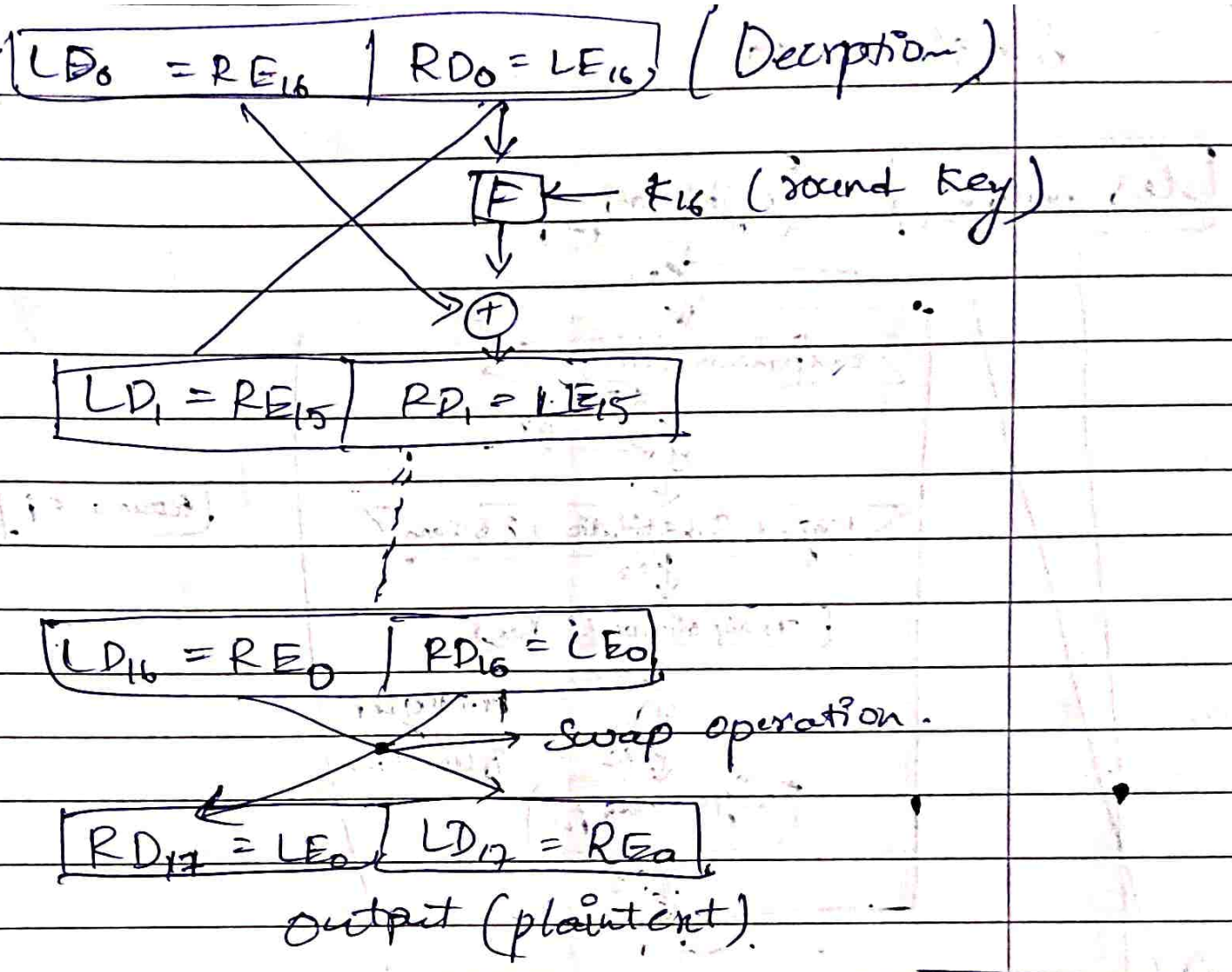
Feistel Structure

Encryption

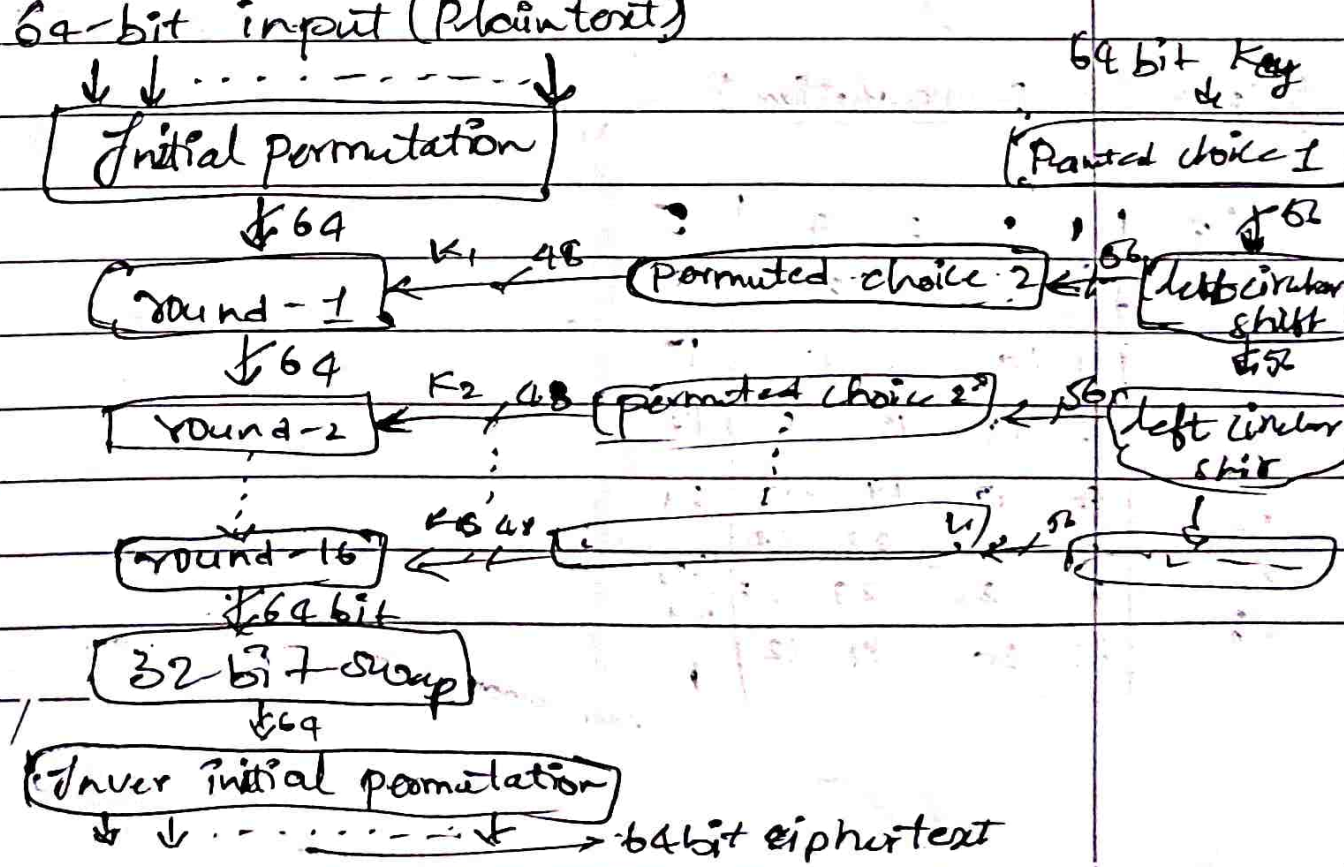
Input (plaintext) - 64 bits



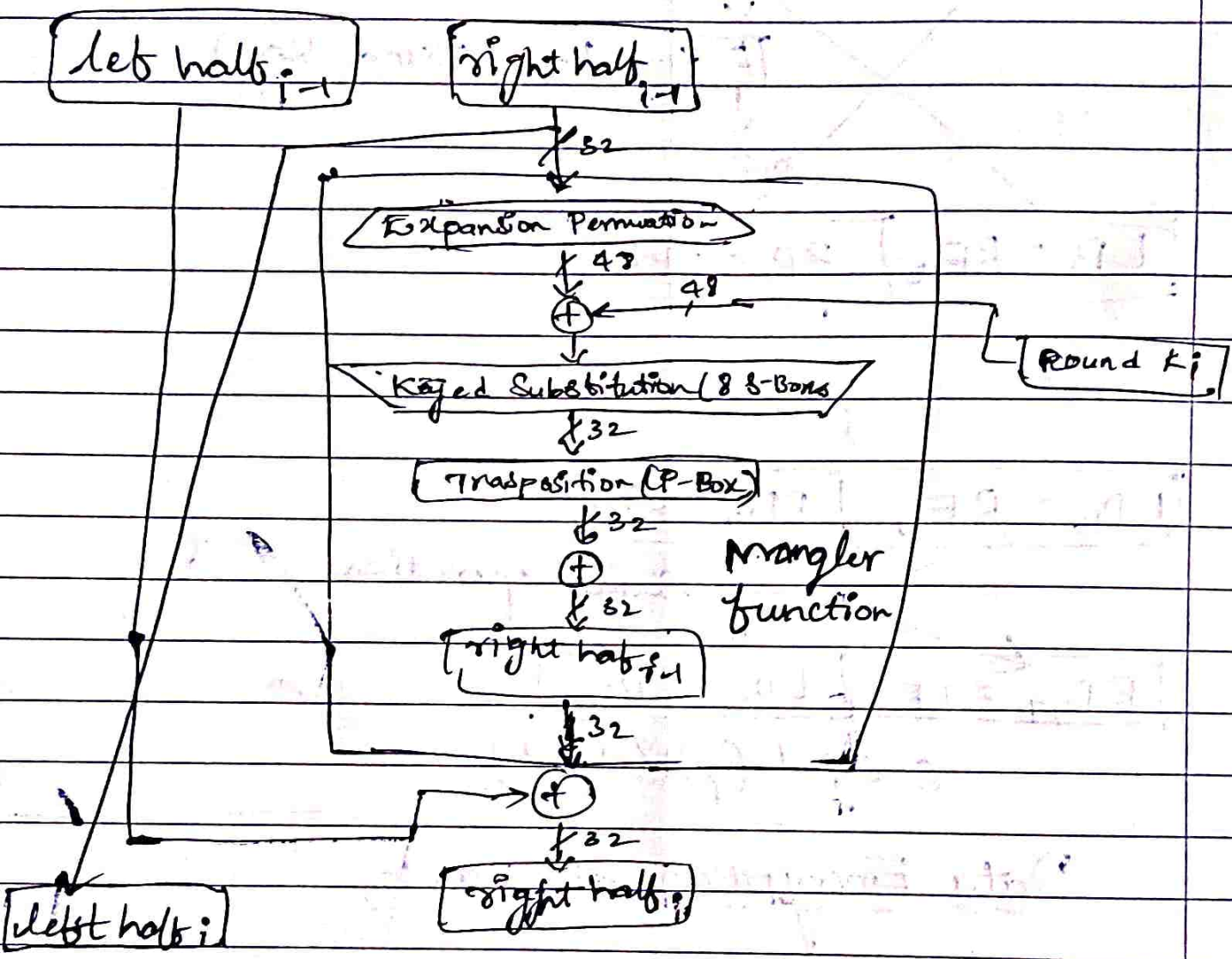
output (ciphertext)



Data Encryption standard :-



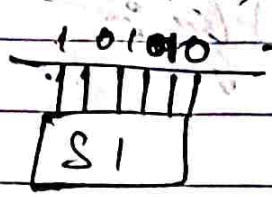
Single round



Expansion permutation:

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

8-(S-Boxes) for each 6-Bits



⇒ 101010 → represents P-Box

01010 → represents row of Sbox

those combination will give a number 5x26 ⇒ 0110

P-Boxes a random arranging of bits.ie (32 bit)

Key Scheduling :-

⇒ 64-bits key will reduced to 56 by removing/dropped 8, 16, 24, 32 = 64, remaining bits are 56 Effective key length 56 bits

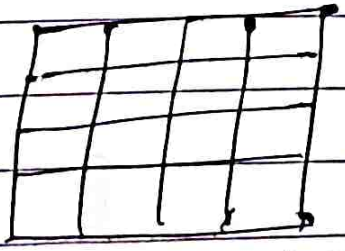
⇒ left circular shift :- we have total of 16-Shifts for rounds for only round 1, 2, 9, 16 we use only 1 shift, for other 2 shifts.

Avalanche effect :- (Bruteforce attack)

AES :-

⇒ had i/p array, State array & a Key array

↓ 4x4 matrics ⇒ Each cell = 1byte / 8bits



total = 16 cells

16x8 = 128 bits

⇒ 4 words (32 Each)

State array

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,3}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,4}$	$S_{3,3}$

→ 4 words

Blowfish Algorithm

- Block Cipher Algo
- Symmetric key cryptography

i/p size = 64 bits

Key size = Variable length key
(from 32 to 448 bits)

Properties:

- fast
- takes less memory
- Simple to understand & implement
- more secured (bcz of var. length key)

⇒ **Step 1: Key generation**

1, Key are stored in an array

$K_1, K_2, K_3, \ldots\ldots K_n \; [1 \le n \le 14]$

length of each block = 32 bits (32 x 14 = 448 bits)

2, Initialise an array (P)

$P_1, P_2, \ldots\ldots P_{18}$

length of each word = 32 bits

3, Initialise S-boxes (4)

$S_1 \Rightarrow S0, S1, \ldots\ldots S255$

$S_2 \Rightarrow S0, \ldots\ldots S255$

$S_3 \Rightarrow$ " "

$S_4 \Rightarrow$ " "

4, Initialise each element of P-array & S-boxes with

Hexadecimal Values

5, XOR operations are performed

$P_1 = P_1 \text{ XOR } K_1$

$P_{14} = P_{14} \text{ XOR } K_{14}$

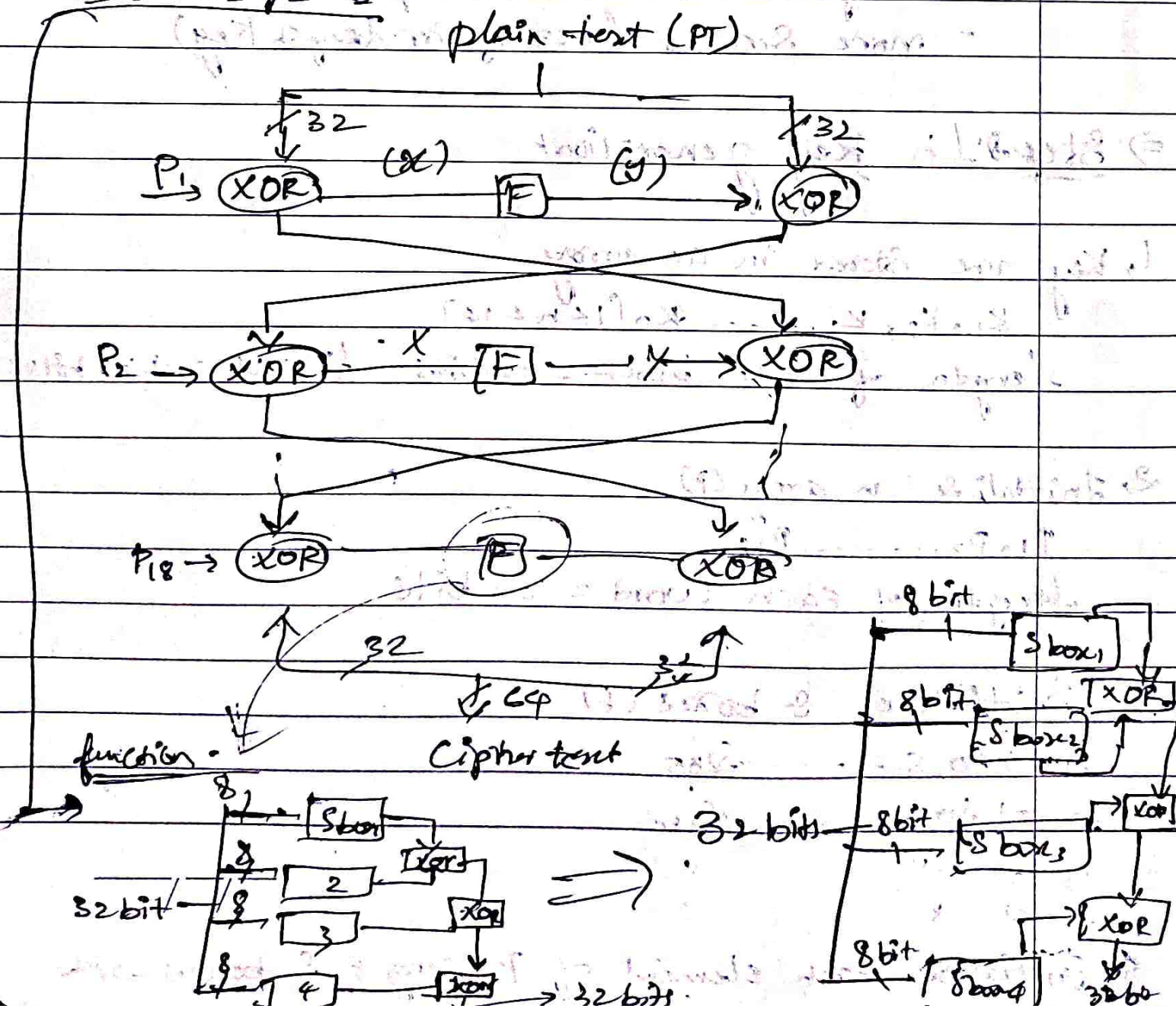
$P_{18} = P_{18} \text{ XOR } K_4^{K_1}$

6, Take 64bit PT (Initially all bits are 0)

(0, 0, — 0)

Sub Key is generated.

* Data encryption:



IDEA Algo – [International data Encryption Algo]

It is Block Cipher Algo

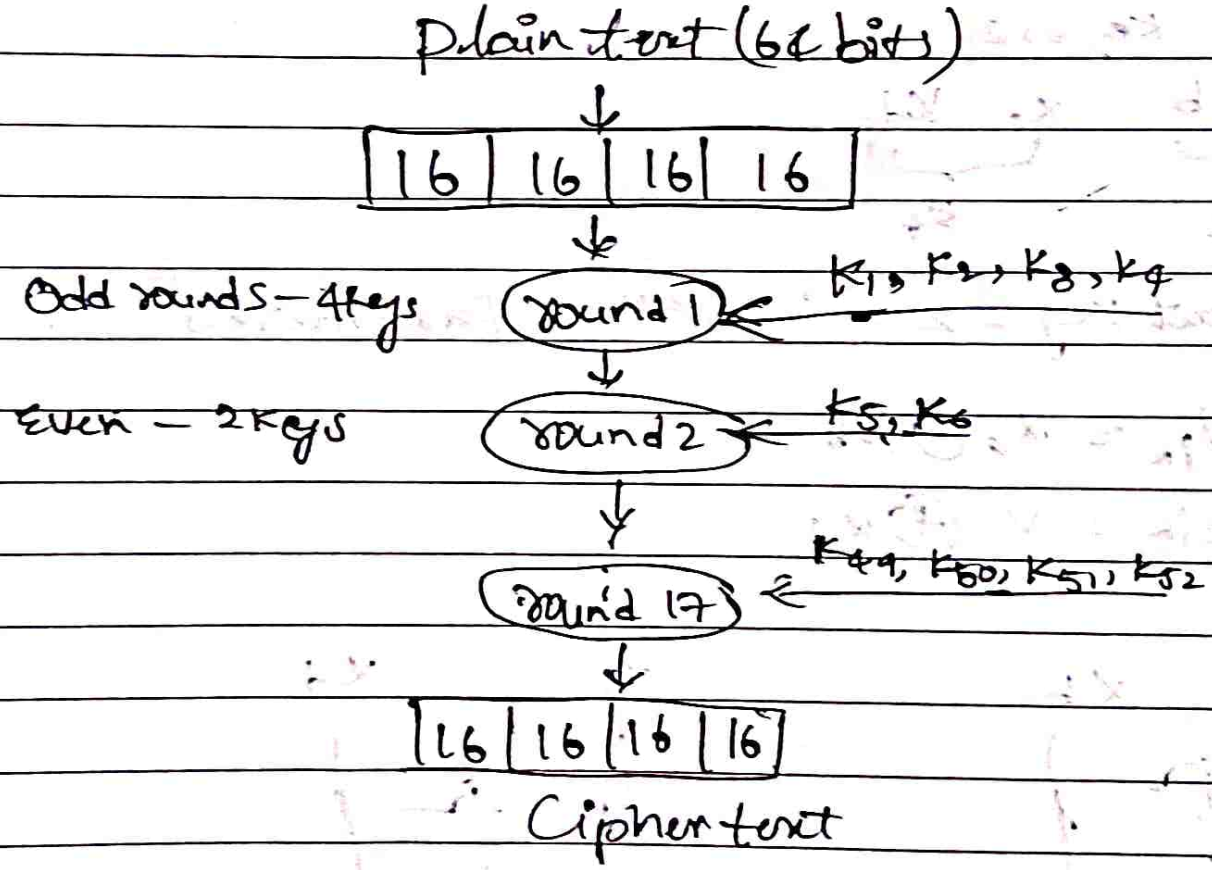
It is a Symmetric key cryptography

It is a Feistel Cipher

i/p size = 64 size – 16, 16, 16, 16

Key size = 128 bits – into 52 Sub keys

No. of rounds = 17



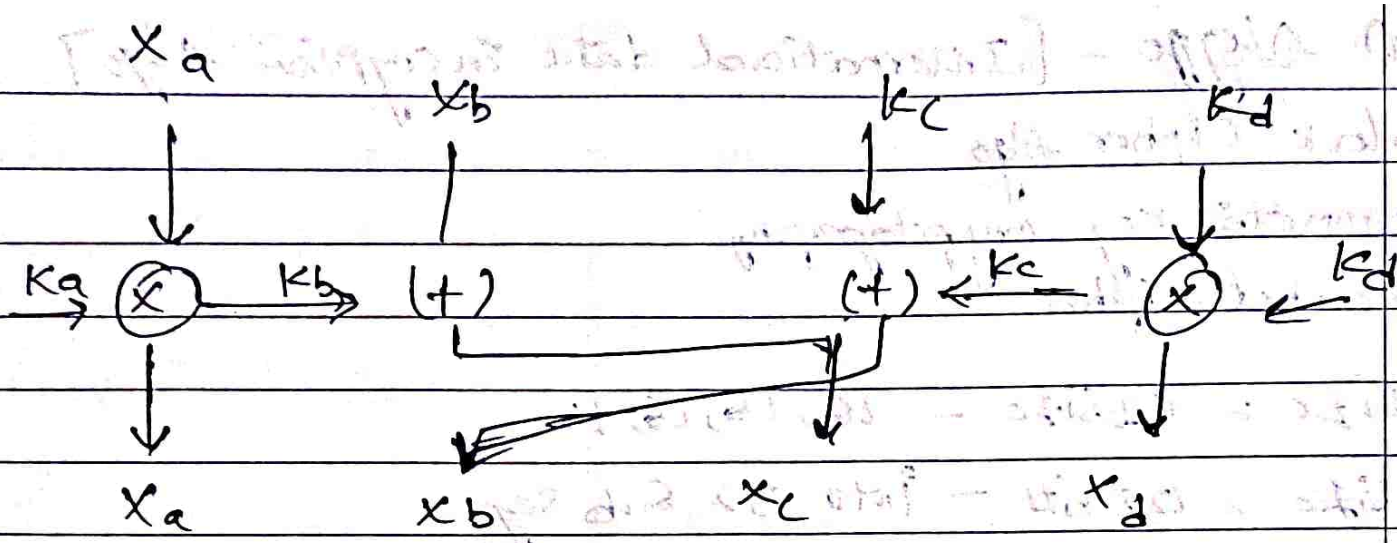
⇒ Rounds
- Even
- Odd

i/P = 4

Key = 4

Xa, Xb, Xc, Xd (16 16 16 16)

Ka Kb Kc Kd



⇒ Even i/p ⇒ 4

Key ⇒ 2

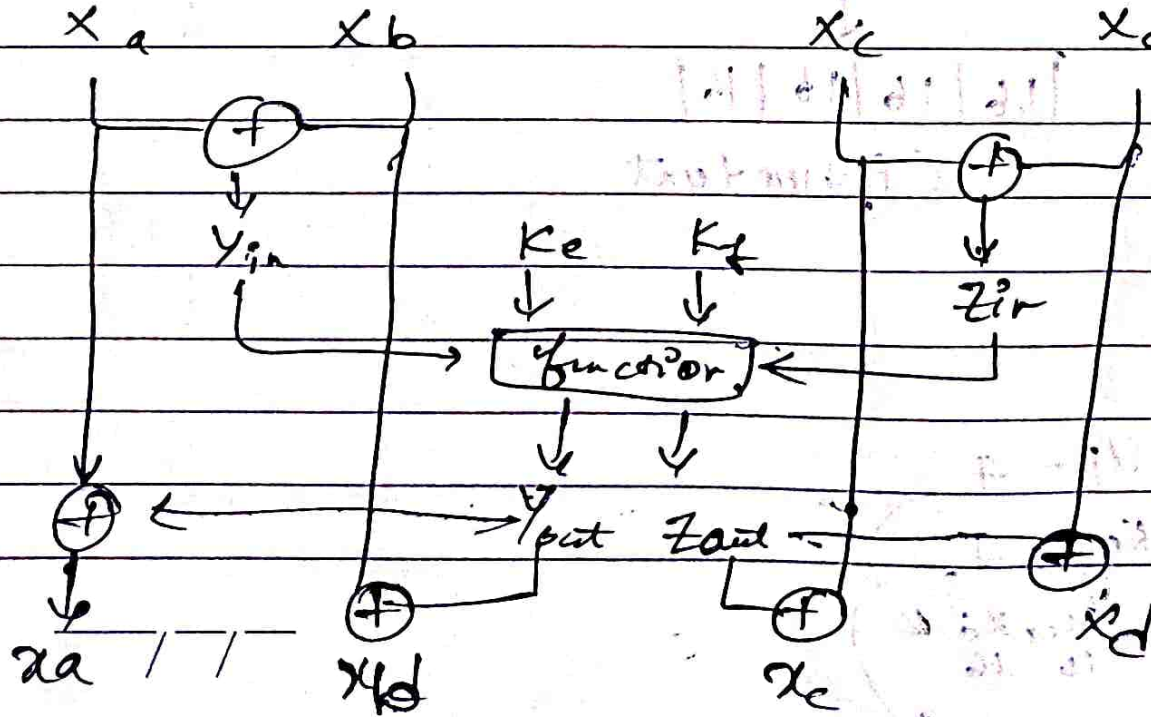
x_a x_b x_c x_d

k_e k_f

i/p = 4 but key = 2 ∴ take 2 parameters

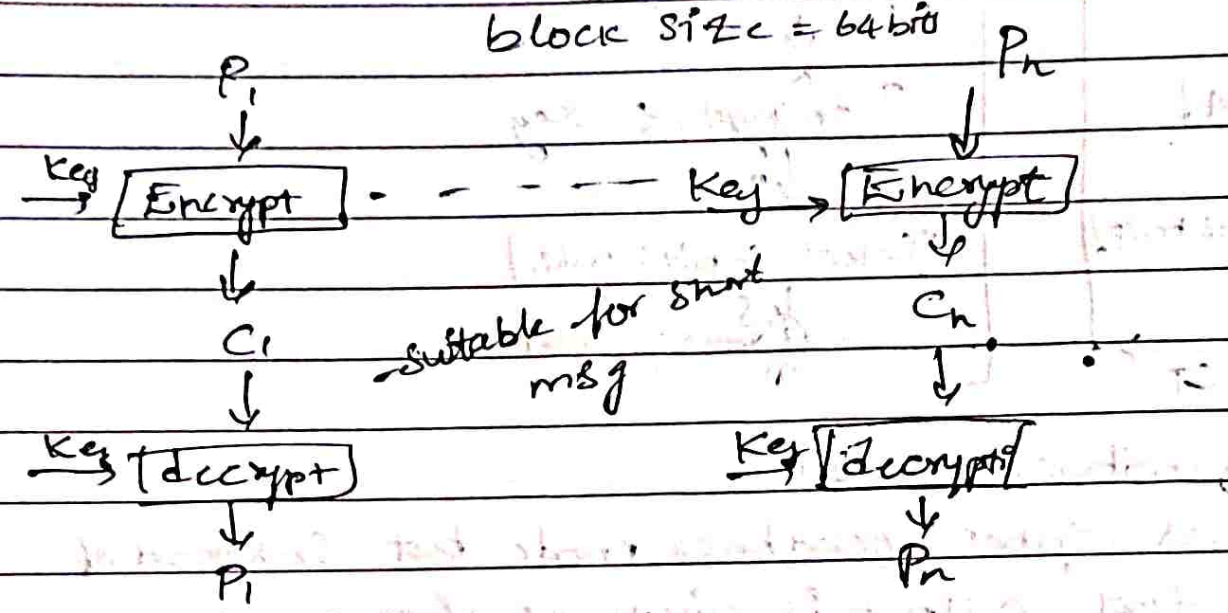
$$y_{in} = x_a \oplus x_b$$

$$z_{in} = x_c \oplus x_d$$

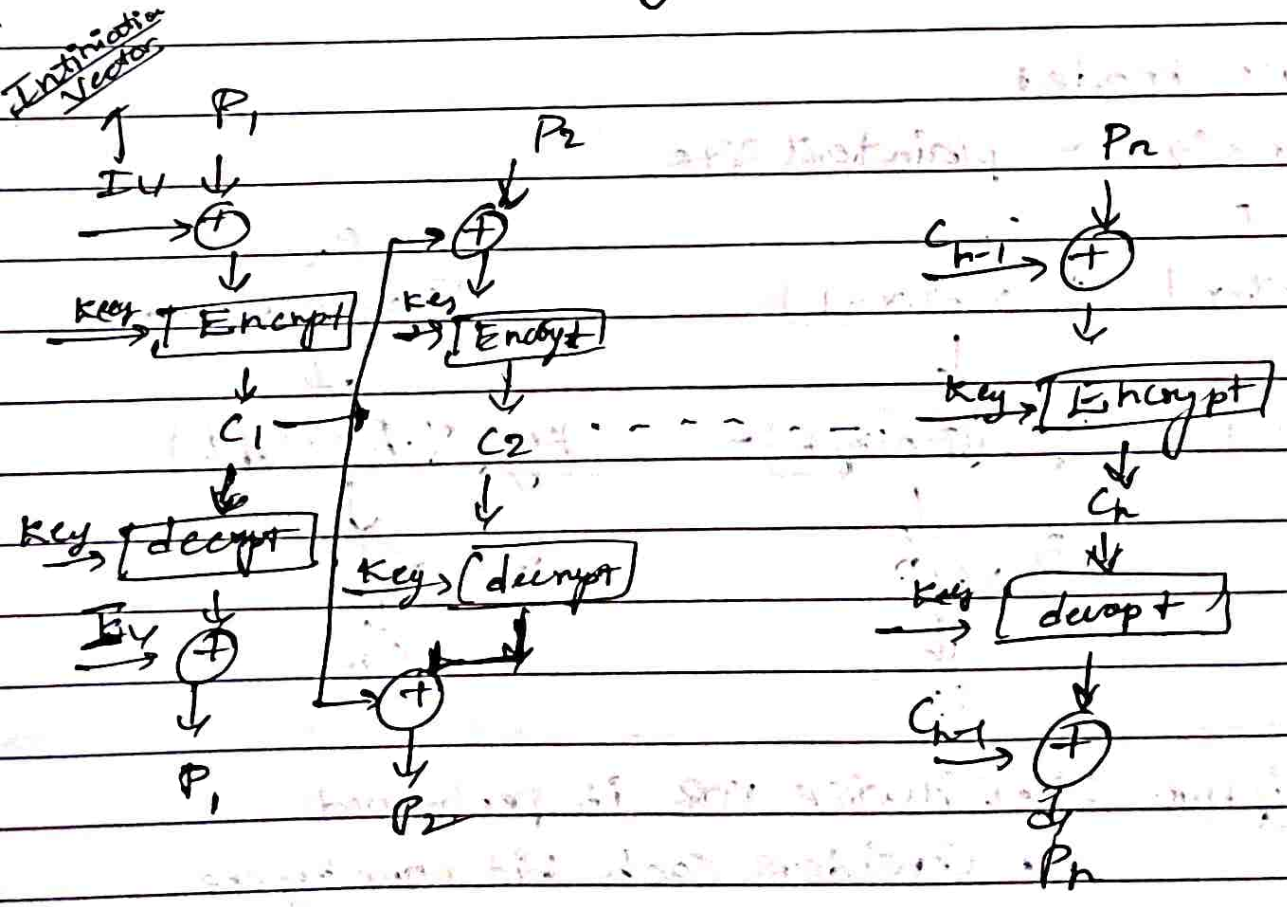


* Block Cipher MODES of operation *

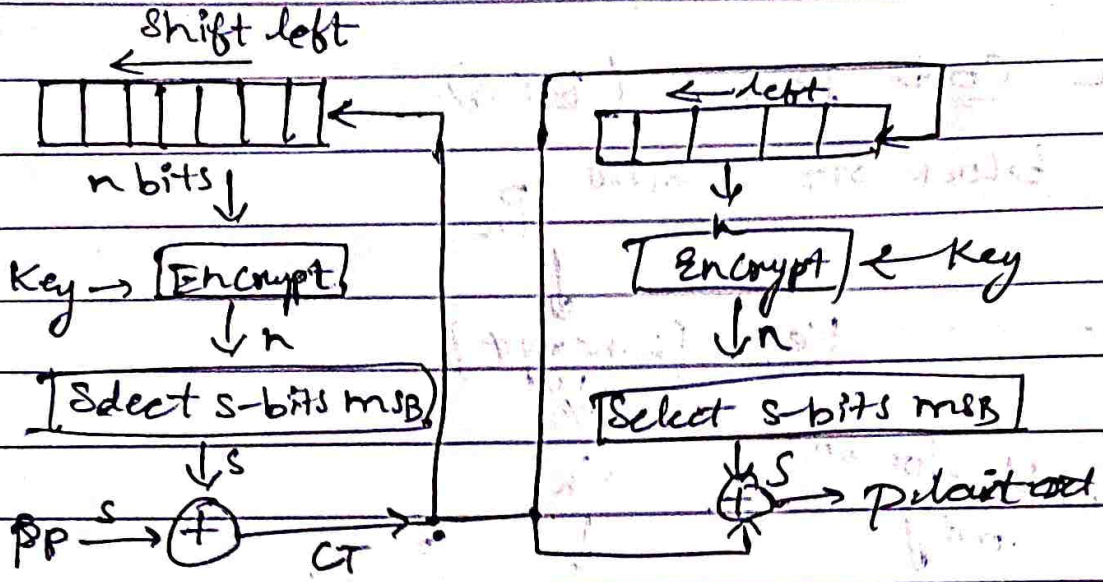
(1) Electronic Code Book (ECB)



(2) Cipher block chaining (CBC)



(3) Cipher Feedback mode

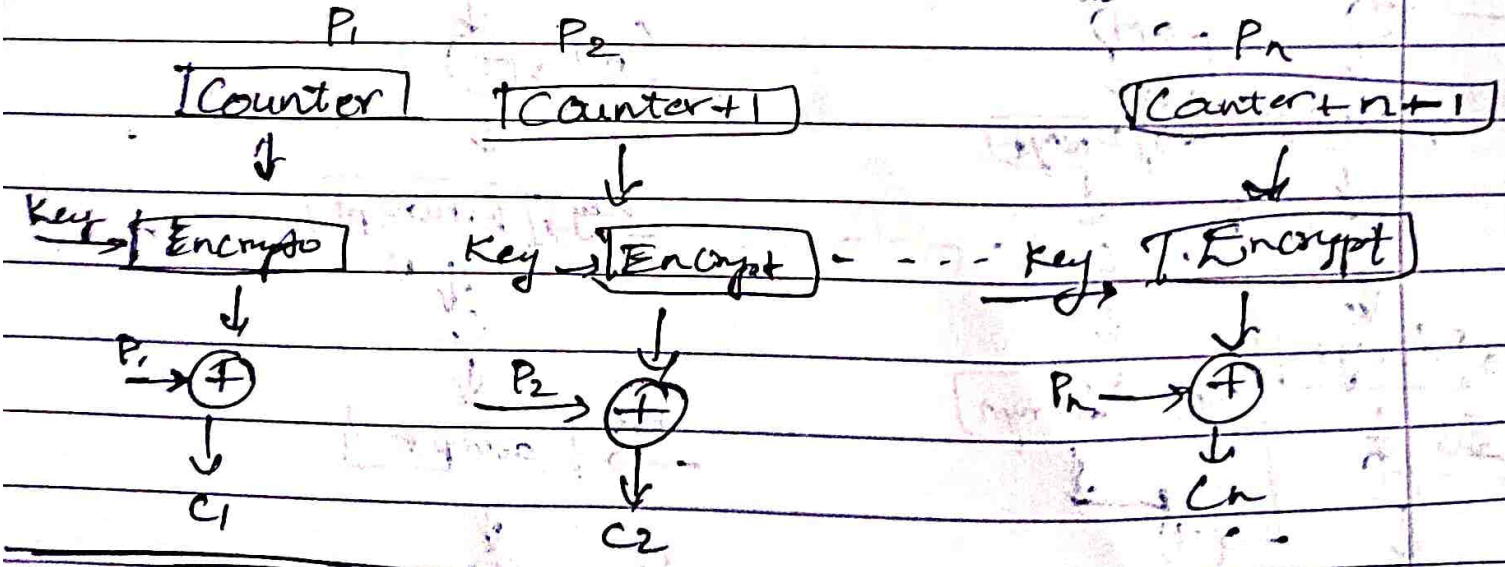


(4) Output feedback mode

- Same as cipher feedback mode but instead of cipher text, output is given as feedback.
* o/p refers to s-MSB bits.

(5) Counter mode

Counter size = plaintext size



Stream Cipher :- • Bitwise XOR is performed
• Considers each bit done by one

$m_1, m_2 \ldots m_q \rightarrow$ plaintext

(4) $k_1/k_2/\ldots k_q \rightarrow$ Key

$c_1\ c_2\ c_3 \ldots c_q \rightarrow$ Ciphertext

* RC4 Algorithm
- Stream Cipher Algorithm

Procedure:
1, Uses an array(S) - State Vector of length 256 (0-255)
2, It has a key encoded with ASCII
3, It has a key array of length 256 (0-255)

Steps: 1, Key scheduling
2, Key stream Generation
3, Encryption & decryption

→ (1) : No. of iterations = Size of S array.

j = 0
for i = 0 to 255 do
j = [j + S(i) + T(i)] mod 256
Swap (S[i], S[j])

Here
S[i] → State Vector
T[i] → Key array

Ex S - array = [0 1 2 3 4 5 6 7]
Key array = [1 2 3 6]
plain Text = [1 2 2 2]

Initialise T - array with key

T = [1 2 3 6 1 2 3 6]
→ Repeate, b/c Key ≠ S-array size

Size

(1) j = 0
For i = 0 to 7
j = [0 + 0 + 1] mod 8
= 1 mod 8
j = 1
Swap [S(0) & S(1)]
⇒ S[1 0 2 3 4 5 6 7]

(2) for i = 1 to 7 ---- (1)
j = [1 + 0 + 2] mod 8
= 3 mod 8
j = 3
Swap [S[1] & S[3]]
⇒ S[1 3 2 0 4 5 6 7]

(2) Stream Generation:

No. of iterations = Size of key (4)

```
i,j = 0;
While (true)
i = (i+1) mod 256;
j = (j + S[i]) mod 256
Swap [S[i], S[j]);
t = ((S[i] + S[j]) mod 256)
K = S[t];
```

New key is obtained (used for Encryption & decryption)

(3) Encryption & Decryption

⇒ Enc = PT XOR New key (In binary)
- we get CT

⇒ Decrypt = CT XOR New key (In binary)
- to get plaintext back

---

* Key Distribution:

1, Physical delivery
2, Key distribution Center
3, Using previous keys
4, Using third party.

Public Key Cryptography :

Conventional	Public-Key
Same Algorithm	Different Alg.
Same Key	Diff Key
Key is Kept Secret	one of the Keys is kept Secret
~~faster~~ Faster	Slower
classical Cryptosystem	RSA, Diffie-Hellman, ECC, Rabin cryptosystem.

RSA — Algorithm :

⇒ Select prime no. p, q : $q \neq p$

⇒ Calculate ⇒ $n = p \times q$

⇒ $\phi(n) = (p-1)(q-1)$

⇒ Select int e ⇒ GCD $(\phi(n), e) = 1$ $1 < e < \phi(n)$

⇒ calculate d ⇒ $e \times d \equiv 1 \bmod \phi(n)$

Plaintext $P = C^d \bmod n$

ciphertext $C = P^e \bmod n$

Q. plaintext = 20

$p = 5$

$q = 11$

$n = 5 \times 11$

$n = 55$

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

$= (4)(10) = 40$

e = 13

GCD(40, 13) = 1

Q	A	B	R
10	40	13	4
3	13	4	1
4	4	1	0
	1	0	

Any

⇒ $13x ? \equiv 1 \pmod{40}$

⇒ 13 mod 40

Q	A	B	R	T_1	T_2	T
10	40	13	4	0	1	-10
3	13	4	1	1	-10	31
4	4	1	0	-10	31	-134
	1	0		31	-134	

$T = T_1 - (T_2 \times Q)$

$T = 0 - (1 \times 10)$

$= 1 + 10$

$= 11$

$T = 1 - (-10 \times 3)$

$= 1 + 30$

$= 31$

$= -10 - (31 \times 4)$

$= -134$

GCD ⇒

Q	A	B	R
3	40	13	1
13	13	1	0
	1	0	

⇒ $13x ? \equiv 1 \pmod{40}$

⇒

Q	A	B	R	T_1	T_2	T
3	40	13	1	0	1	-3
13	13	1	0	1	-3	40
	1	0		-3	40	

$1 - (-3 \times 13)$

$1 - (-34)$

$= 40$

$-3 + 40 \Rightarrow 37$

$13 \times 37 \equiv 1 \pmod{(40)}$

$\Rightarrow d = 37$

$C = P^e \bmod n$

$= 20^{13} \bmod 55$

$= 20 \times 20^{12} \bmod 55 \Rightarrow 20$

$= 20 \times 20 \bmod 55 \Rightarrow$

$= 20^4 \Rightarrow 20^2 \times 20^2 \bmod 55$

$\Rightarrow 40 \times 40 \bmod 55 \Rightarrow 5$

$\Rightarrow 20^{16} \bmod 55$

$\Rightarrow 25 \bmod 55 \Rightarrow 25$

$\Rightarrow 20^4 \times 20^4 \times 20^4 \times 20 \bmod 55$

$\Rightarrow 5 \times 5 \times 5 \times 20$

$\boxed{C = 25}$

Q, Plain text = 85.

$P = 17$

$q = 11$

$n = 17 \times 11$

$\boxed{n = 187}$

$\phi(n) = (16)(10)$

$= 160$

$\boxed{e = 7} \Rightarrow GCD(e, \phi(n)) = 1$

$= (160, 7) = 1$

Q	A	B	R
22	160	7	6
1	7	1	1
6	4	1	0

$13 \times 37 \equiv 1 \pmod{(160)}$

$\Rightarrow d = 37$

$C = P^e \bmod n$

$= 20^{13} \bmod 55$

$= 20 \times 20^{12} \bmod 55 \Rightarrow 20$

$= 20 \times 20 \bmod 55 \Rightarrow$

$= 20^4 \Rightarrow 20^2 \times 20^2 \bmod 55$

$\Rightarrow 40 \times 40 \bmod 55 \Rightarrow 5$

$\Rightarrow 20^{16} \bmod 55$

$\Rightarrow 25 \bmod 55 \Rightarrow 25$

$\Rightarrow 20^4 \times 20^4 \times 20^4 \times 20 \bmod 55$

$\Rightarrow 5 \times 5 \times 5 \times 20$

$C = 25$

Q, Plain text = 85.

$P = 17$

$q = 11$

$n = 17 \times 11$

$n = 187$

$\phi(n) = (16)(10)$

$= 160$

$e = 7 \Rightarrow GCD(e, \phi(n)) = 1$

$= (160, 7) = 1$

Q	A	B	R
22	160	7	6
6	7	6	1
6	6	1	0

1 1 0

$\Rightarrow e \times d \equiv 1 \bmod 160$

$\Rightarrow 7 \bmod 160$

$\Rightarrow$

Q	A	B	R	T_1	T_2	T
22	160	7	6	0	1	-22
1	7	6	1	1	-22	23
6	6	1	0	-22	23	-146
1	0			23	-146	
				23		

$T = 1 - (-22 \times 1)$
$= 1 + 22$
$= -22 - (23 \times 6)$
$= -146$

$\Rightarrow d = 23$

$\Rightarrow C = P^e \bmod n$

$= 85^7 \bmod 160$

$= 85 \times 85 \bmod 160 \Rightarrow 25$

$\Rightarrow 85^2 \times 85^2 \bmod 160 \Rightarrow 145$

$\Rightarrow 85^4 \times 85^2 \times 85^1 \bmod (160) =$

$= 145 \times 25 \times 85 \bmod (160) =$

$= 125 \times 85 \bmod (160) = 125$

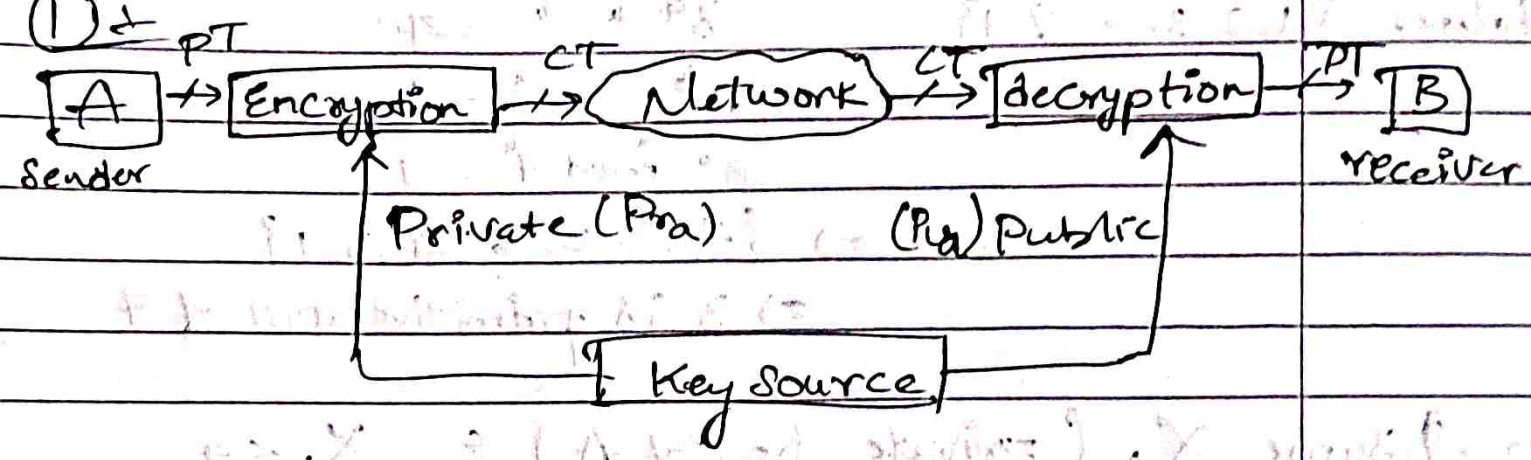
$C = 125$

* Principles of Public Key cryptosystems
(Asymmetric key cryptography)

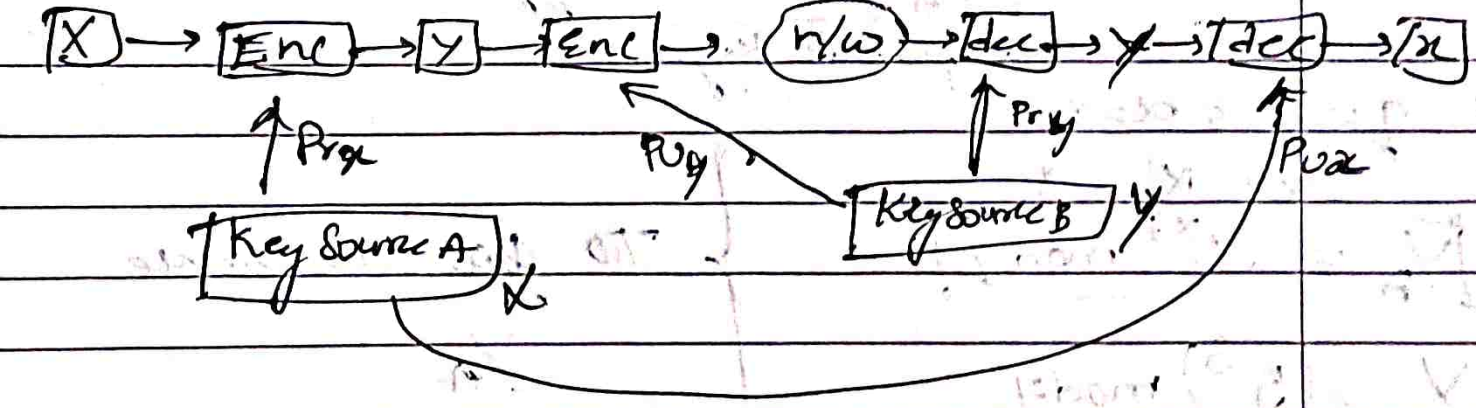
1, Authentication:

2, Confidentiality:

(1) :



(2) Sender



⇒ Algorithms :

(1) DIFFIE - HELLMAN Key Exchange Algor

⇒ (1) Consider a prime number q

let q = 7

(2) Select α such that α < q & α is primitive root of q

P / / /

Primitive root

$\Rightarrow \alpha^1 \bmod q$

$\alpha^2 \bmod q$

!

$\alpha^{q-1} \bmod q$ should have values: $\{1, 2, 3 \dots q-1\}$

Ex $\alpha = 3$ & $q = 7$

$3^1 \bmod 7 = 3$

$3^2 \bmod 7 = 2$

3^3 " " $= 6$

3^4 " " $= 4$

3^5 " " $= 5$

$3^6 \bmod 7 = 1$

$\Rightarrow \{7, 3, 2, 6, 4, 5, 1\}$

$\Rightarrow$ 3 is primitive root of 7

3, Assume X_A (private key of A) & $X_A < q$

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

(public key = A

Ex $q = 7$ & $\alpha = 3$

let $X_A = 3$

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

$Y_A = (5^3) \bmod 7$

$= 125 \bmod 7$

$\boxed{Y_A = 6}$

} To get the value Y_A

4, Assume X_B & $X_B < q$

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

$\Rightarrow$ let $X_B = 4$

$Y_B = 5^4 \bmod 7$

$= 625 \bmod 7$

$\boxed{Y_B = 2}$

} Y_B.

(5) Calculate Key K_1 & K_2

K_1 = person A

K_2 = person B

$K_1 = (Y_B)^{X_A} \bmod q$; $K_2 = (Y_A)^{X_B} \bmod q$

$= (2)^3 \bmod 7$; $K_2 = (6)^4 \bmod 7$

$= 8 \bmod 7$ $K_2 = 1296 \bmod 7$

$\boxed{K_1 = 1}$ $\boxed{K_2 = 1}$

$K_1 = K_2$ ∴ Succeed

Key Exchanged successfully.//

* Elgamal : It is Asymmetric

(1) Key generation

→ Select large prime number (P) $\boxed{P = 11}$

→ Select a dec. key also called private key. (d)

$\boxed{d = 3}$

→ Select second part of Encryption key (e_1) = 2

Calculate $\boxed{e_1 = 2}$

→ Select third part of Encryption key (e_2)

$e_2 = e_1^d \bmod p$

$= 2^3 \bmod 11$

$\boxed{e_2 = 8}$

→ Public key = (E_1, E_2, P) & private key = d

$= (2, 8, 11)$

2, Encryption

↳ Select a random int (R)

R = 4

↳ cal $C_1 = e_1^r \bmod p$

$= 2^4 \bmod 11$

$C_1 = 5$

↳ cal $C_2 = (PT \times e_2^R) \bmod p$ PT = Assume (7)

$= (7 \times 8^4) \bmod 11$

$C_2 = 6$

↳ Cipher text = (C_1, C_2)

$= (5, 6)$

3, Decryption

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

$= 6 \times (5^3)^{-1} \bmod 11$

$= 6 \times (125)^{-1}$ = 3

$\Rightarrow 125 \times (x) \bmod 11 = 1$

125 mod 11 $\Rightarrow$ 6 × 3 mod 11 = 7

$T = T_1 - (T_2 \times Q)$

Q	A	B	R	T_1	T_2	T
10	125	11	2	0	1	-10
4	11	4	3	1	-10	34
1	3	2	1	-11	34	-45
2	2	1	0	34	-45	124
	1	0		-45	124	

$\Rightarrow 10$

$T = 0 - (1 \times 10)$
$= 1 - (-11 \times 3)$
$= 1 - (-33)$
$= 34$

$T = -11 - (34 \times 1)$
$= -11 - 34$
$= -45$

$T = 34 - (-45 \times 2)$
$= 34 - (-90)$
$= 124$

* Key Distribution

① Public Announcement — Key will be broadcast to all users in the N/w

② public key directory — (telephone directory)
User R store the key in public key directory, then User B search for user R key

③ public key Authority — 3rd party A send request to 3rd party. for B & gets
⇒ the 3rd party will check ...
if that users A is same network or some hacker or not

④ Certificate Authority — Same → but it contain certificate of all users like. id, publickg.

* Knapsack - Algorithm

Ex: weights = (1, 6, 8, 15 & 24)

-> In general knapsack, we select weights to achieve a sum if we want sum = 30

we select 1, 6, 8 & 15

let plain-text = 10011 11010

1, 6 8 15 24 | 1 8 6 8 15 24

1+5+24 = 40 | 1+6+15 = 22

CT => 40 20

Key generation :

- Public Key (Hard Knapsack)
- private Key (Easy KS)

Ex :- {1, 2, 4, 9, 20, 40}

1, -first, find private key (Assume)

D' = {1, 2, 4, 10, 20, 40} → Pvt Key

Select 2 numbers "n" & "m"

⇒ m > Sum of all no.s in Sequence

Sum = 77 ∴ let m = 110

⇒ n = Select so that it has no common factor with m

let n = 31

Now (D_i × n) mod m ∀ element in D

⇒ 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

Publickey = {31, 62, 14, 90, 70, 30}

* Encryption:

Now, Assume PT

let PT = 100100 | 111100 | 101110

devide into 6-6 parts (no. of Element in Sequence = 6)

1st part = 100100 = 1×31 + 0×62 + 0×14 + 1×90 + 0×70 + 0×30

= 31 + 90 = 120

2nd part = 111100

31 62 14 90 70 30

31 + 62 + 14 + 90 = 197

3rd part = 101110

31 62 14 90 70 30

31 + 14 + 90 + 70 = 205

CT = (122 197 205)

* Decryption:

Calc $\Rightarrow r^{-1} = 31^{-1} \bmod 110$

$\Rightarrow$

r	q	p	q
110		0	1
31	3	1	0
17	1	-3	1
14	1	4	-1
3	4	-7	2
2	1	32	-9
1	2	[-39]	11
[10]			

$0 - (1 \times -3)$

$-3 = 4$

$1 - (-1)$

$4 - (-3)$

$-1 - (8)$

$2 - (-9) - 9$

$11 - 7 - (32)$

-39

$110 - 39$

$[x = 71]$

$\Rightarrow (CT \times x) \bmod m.$

$\Rightarrow 121 \times 71 \bmod 110 = 11$

$\Rightarrow 197 \times 71 \bmod 110 = 17$

$\Rightarrow 205 \times 71 \bmod 110 = 35$

$D_2 = \{1, 2, 4, 10, 20, 40\}$

$\Rightarrow 11 \Rightarrow 1\ 0\ 0\ 1\ 0\ 0$

$\Rightarrow 17 \Rightarrow 1\ 1\ 1\ 1\ 0\ 0$

$\Rightarrow 35 \Rightarrow 1\ 0\ 1\ 1\ 1\ 0$

* Message Authentication :

⇒ Authentication ?

↓ Verifying the identify of User (from correct person or not)

How it is done ? - by authenticator

↓ generated by authentication function

That can be numeric, alphabatic or ailphanumeric ..etc

⇒ 3 type of functions :- (to generate authenticator

↳ message Encryption

↳ message Authentication Code (MAC)

↳ Hash function (H)

① Message Encryption :-

Plaintext → Cipher text

↓ acts as authentication

② msg Authentication Code :-

C (M, K) = Output (fixed length code)

C = authentication function

M = message (PT)

K = key

—"— O/P = mac code ↳ CT - act as authenticator

3, Hash function (H): Similar to MAC, but

H(m) = Hash code h Key ↔ hash function

H - Hash function

h - hash code.

↳ acts as authenticator.

MD5 (message Digest - 5)

↳ Working of MD5

i, padding: Original msg + (padding) ← extra bits

⇒ So that total length is 64 bit less than exact multiple of 512

Eg: original msg = 1000 bits + Padding

512 x1 = 512 bits − 64 ✗

512 x 2 = 1024 − 64 ✗

512 x 3 = 1536 − 64 ✓ = 1472

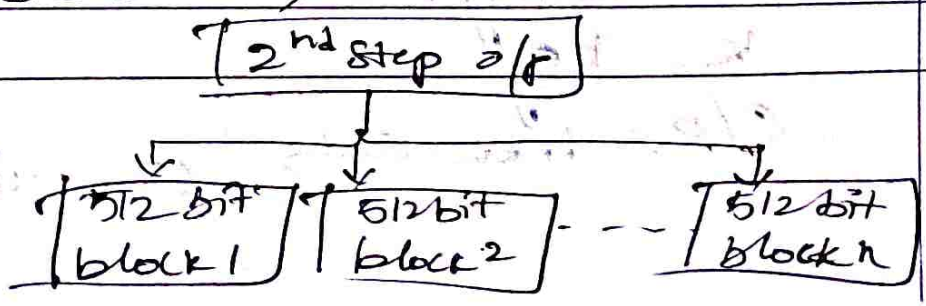
⇒ Add 472 bits //

ii, Appending: Append the original length before padding

Calc length mod 64 ⇒ 1000 mod 64 = 40

Append = 40 bits

iii, Dividing (Each 512 bits)



4, Initialising :- (4 chaining Variables)

Each = 32 bit.

A, B, C & D - Values predefined.

5, processing :- (512 bit blocks)

↳ Copy 4 chaining variables into some corresponding variables

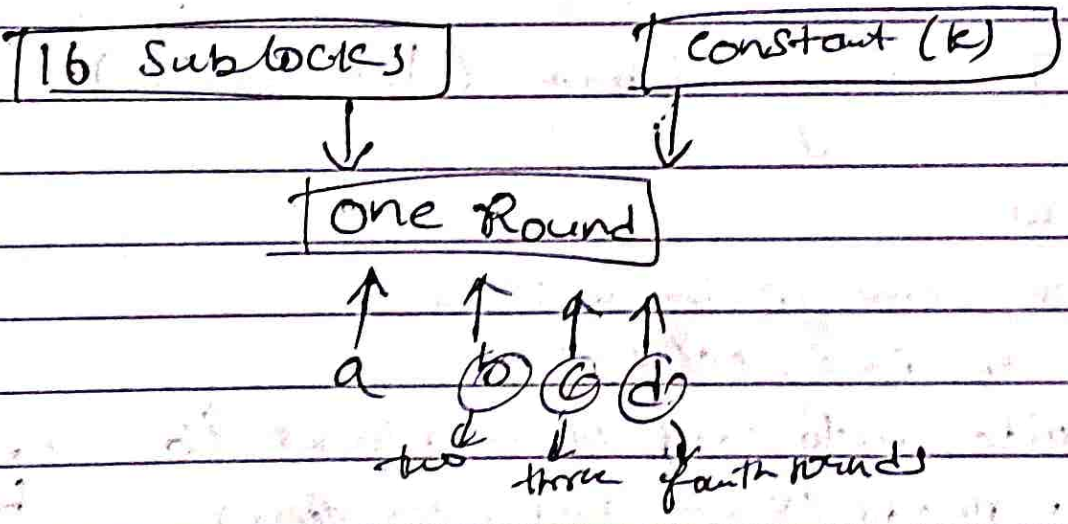
A = a, B = b, C = c, D = d

↳ Divided 512 bit blocks into 16 - 32 bit blocks

⇒ 16 block → 32 bits each

↳ four rounds :-

16 Sub blocks & a Constant (K)



$a = b + (a + \text{process.. } P(b, c, d) + m[j] + T[k])$

* Secure Hash Algo :- (SHA)

- modified version of MD5

⇒ In MD5 - length of O/P = 128 bits

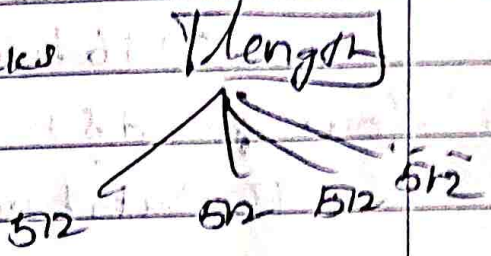
⇒ In SHA length of O/P = 160 bits

* working :-

1. Padding :- Same as MD5 → (64bit < n * 512)

2. Appending :- Same i length mod 64 :→ (x) 512

3) Divide the i/p into 512 bit blocks



4) Initialise 5 chaining variables (A, B, C, D & E)

5. process blocks

- Copy corresponding variables

A=a, B=b, C=c, D=d, E=e

(same) :- divide into no. of 512 bit blocks (16 - 32 bit blocks)

- four rounds (each round = 20 steps)

1 MAC :- (similar to message digest) [Symmetric Key]

↳ Working of MAC :- If Sender wants to send a message 'M'

↓ Symmetric Key (K)

H1 (MAC Code)

Now M → PT + H → CT → Sent to Receiver

↳ Calculate his own MAC H2 using Key → K

Now,

On Receiver side H1 & H2 are compared

$H_1 = H_2 \Rightarrow$ No change in message

$H_1 \neq H_2 \Rightarrow$ message is changed

⇒ Significance of MAC :

1, receiver can know if message is changed/not

2, receiver has assurance that msg is from correct Sender

-(because same key for (S) & (R))

---

* HMAC : (Hash Based MAC)

-used in SSL

* working of MAC :-

Original msg (M) → Message digest is generated

↓ (MD5/SHA)

Key (K) → encryption

↓

MAC

In MAC - direct MAC is generated

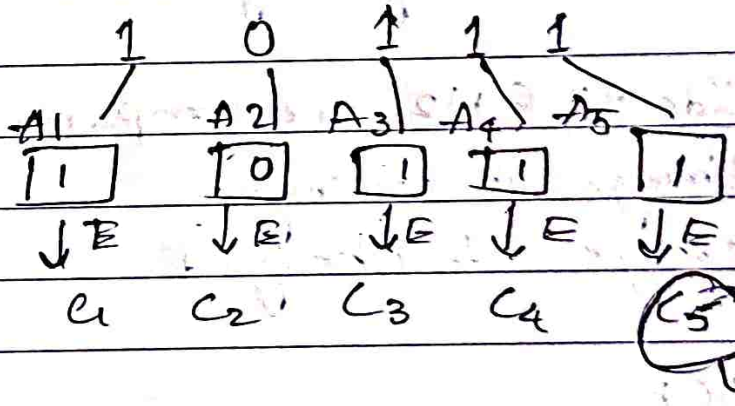
In HMAC - MAC is generated with help of msg digest

* Cipher Based MAC (CMAC):

⇒ Has msg size limit
- based on block cipher

- given message is divided into Equal number of blocks & Each block is encrypted Separately.

Eg:



$C_1 = E(K_1, A1)$

$C_2 = E(K_1, (A_1 \oplus C_1))$

$C_3 = E(K, (A_1 \oplus C_2))$

$C_4 = E(K, (A_1 \oplus C_3))$

$C_5 = E(K, (A_1 \oplus C_4))$

↳ act as MAC