By- Pathik455

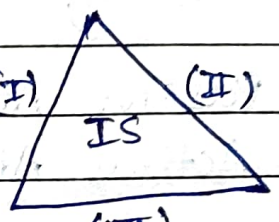
IS.

FULLSCAPE PAGE NO.: DATE

V-1

Security Goals - /objectives

1. Confidentiality (readx)
2. Integrity (modifyx)
3. Availibility (DOSx)
4. Authentication
5. Accountibility



CIA ~~triangle~~ Triad

V-2 ## Elements of IS:

1. Physical Elements (Gaurd, Camera, Rzone, Downloading, Access Right.)
2. System Elements (Anti-Virus, Malicious s/w detection soln. Disable USB ports.)
3. Process Elements (Authorised user/Access control, s/w details, log entry)

V-3 ## Security Policy:

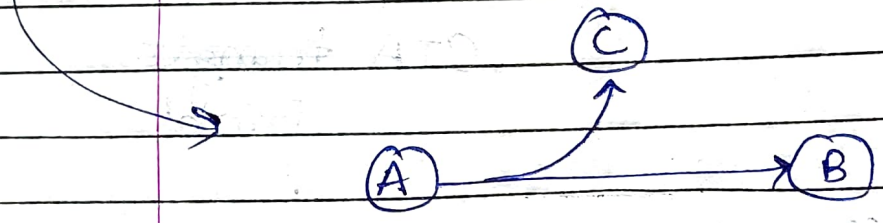
1) Regulatory
2) Advisory
3) User policies

Needs: 1) Control security Risk
2) Identify theft
3) system ~~fraud~~ fraud
4) system misuse detection

V-4

Security Attacks:

1) Passive Attack: → ① Release of msg content (confidentiality X)
   → ② Traffic analysis
2) ~~Active Attack~~

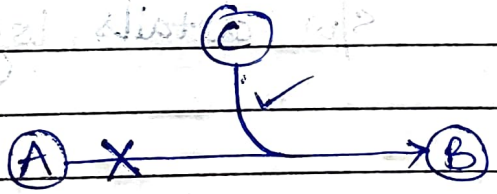


Passive attack
↓
(Only Reads info)

V-5

2) Active Attack: (information gets modified)
(Corrupt files)

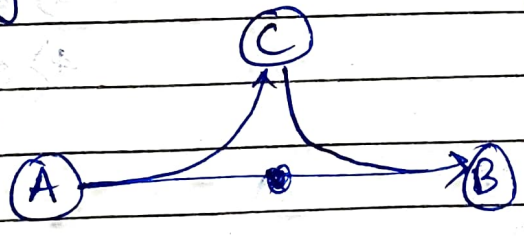
① Masquerade-



C gets acc. of A and sends msg to B from A's account.

② Replay:

(i)

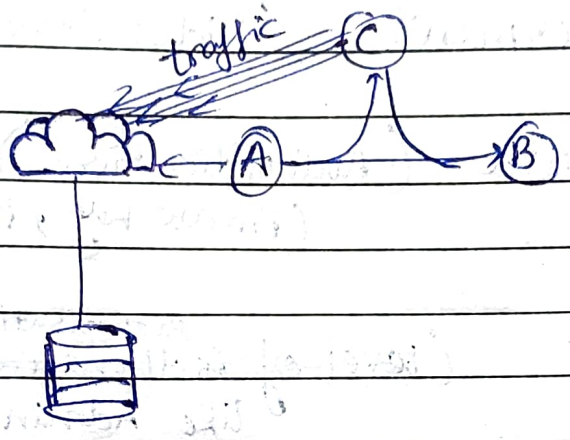


C currupted the data and sends to B.

Confidentiality X
Intigrity x
(Original msg was not received)

(2) (ii) Modification of msg attack:

(3) Denial of service: (DOS) fake traffic to crash system server



C X
I X
A X

V-6

Active Attack	Passive Attack
• Modifies the data.	• Monitors the data
• Affect the system	• Doesn't affect the system.
• Can be easily detected.	• Cannot be easily detected.
• Threat to Integrity & Availability	• Thread to confidentiality.
• Capture Physical control over the link.	• Just Observe the transmission
• Detection	• Prevention

FULLSCAPE
PAGE NO.: DATE

V-7 Security Mechanism:

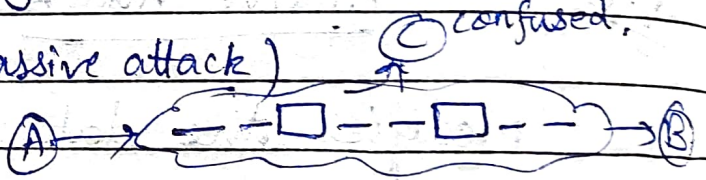
① ~~En~~Chip Encipherment (Hides data, by encryption)

② Digital Signature (Authentication)
(Private Key, Public Key)

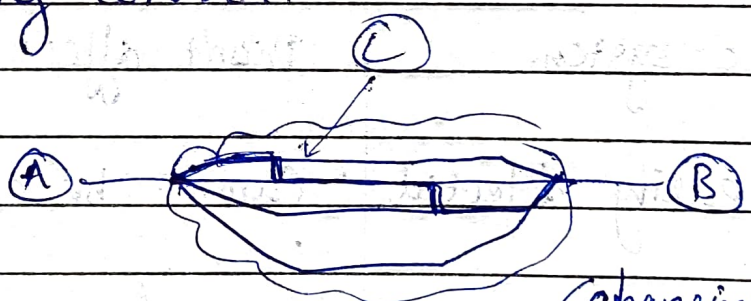
③ Access Control (~~Level of Authentication~~ Authorisation
like Admin, User, employee)

④ Authentication Exchange

⑤ Traffic padding (Passive attack)



⑥ Routing Control.



(changing the path so that C cannot track.)

FULLSCAPE
PAGE NO.: DATE

V-8 Categories of Security Services:

1. Authentication: (eg: OTP)
2. Authorization.
3. Non-Repudiation.
4. Auditing (Analysing the problem) Not protection

V-9 Basics of Network Security:

Plain Text

Cipher Text

Encryption

Decryption

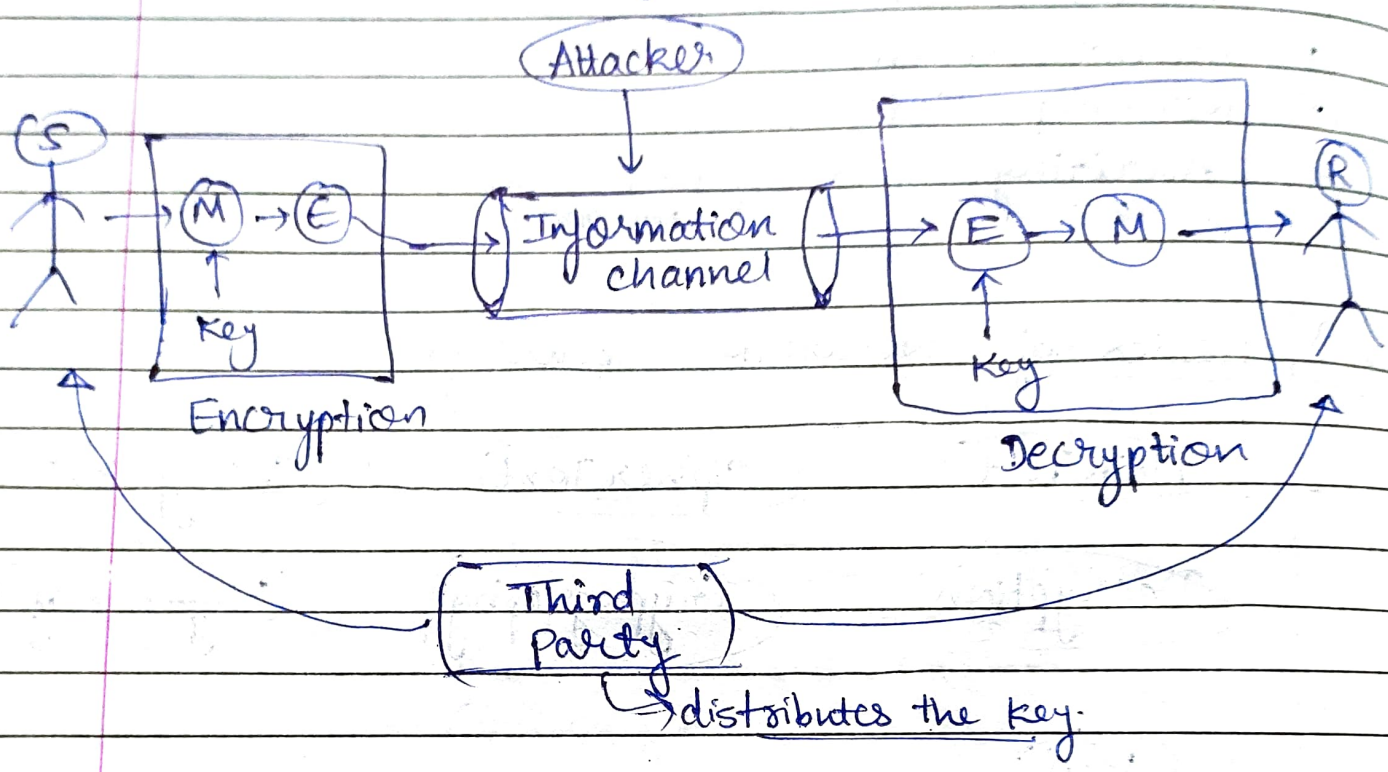
Cryptography

Cryptanalyst

Key

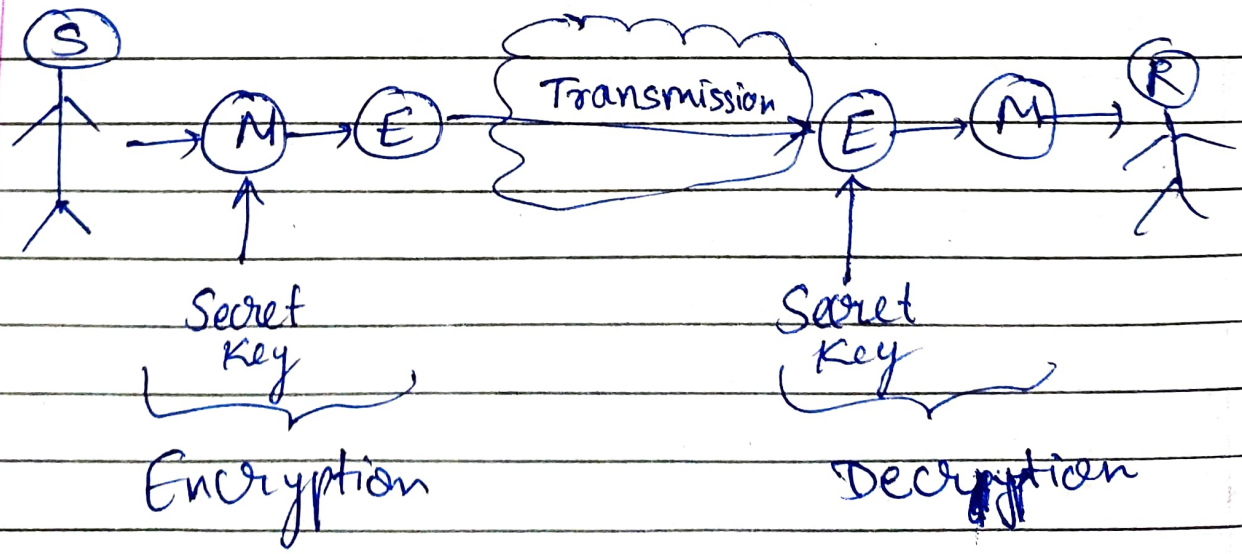
V-10.

Network Security Model :-



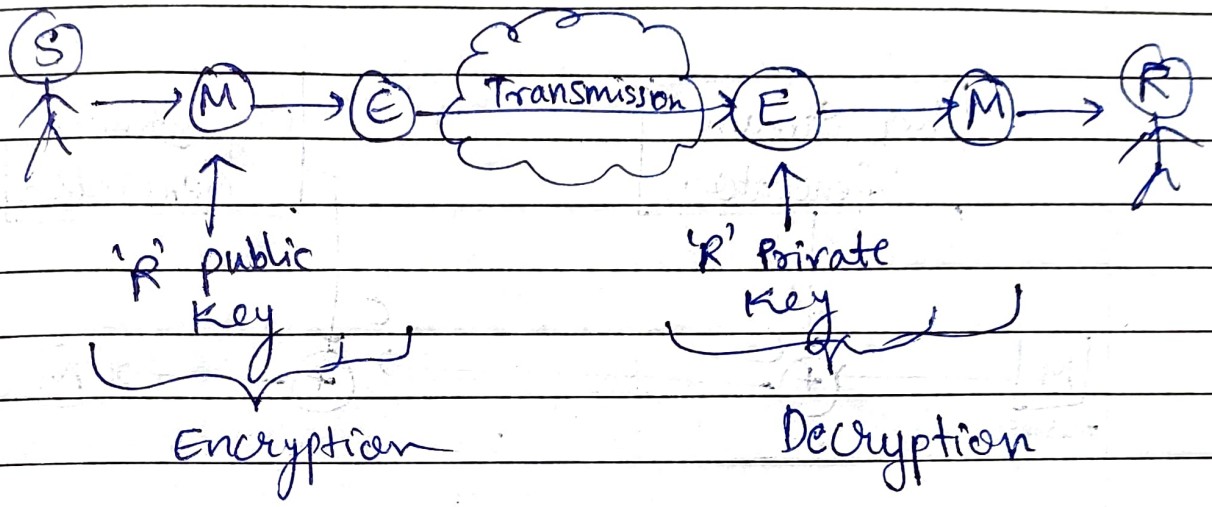
V-11

Symmetric Key Cryptography :



V-12

Asymmetric Key Cryptography:

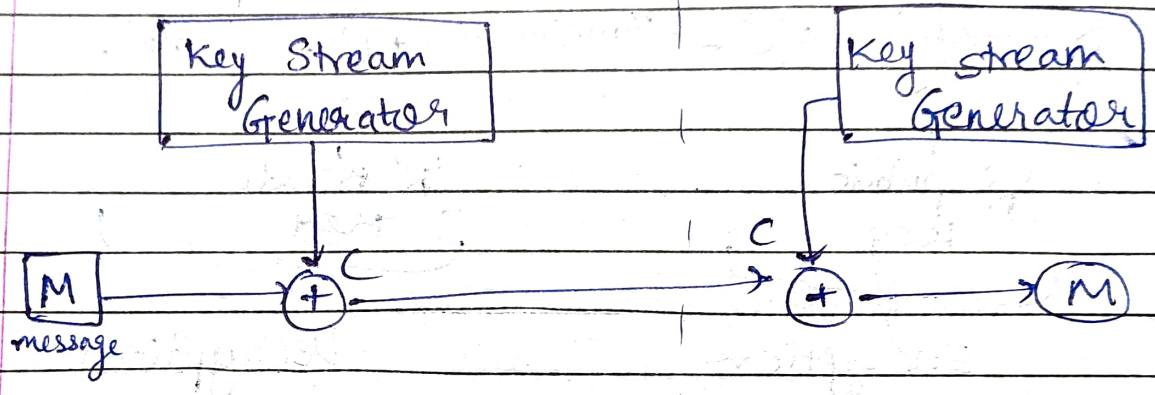


V-13

SKC	ASKC
• Single Key used	• 2 keys used
• Secret Key / Private Key Cryptography	• Public key cryptography
• Faster (complexity ↓)	• Slow (complexity ↑)
• Utilizes less Resources	• Utilizes more Resources
• DES & AES Algorithm used	• RSA and Diffie-Hellman algorithms used
• Bulk data transmission.	• Securely exchanging the key

V-19

Stream Cipher:



10110110
⊕ 01010101
11100011

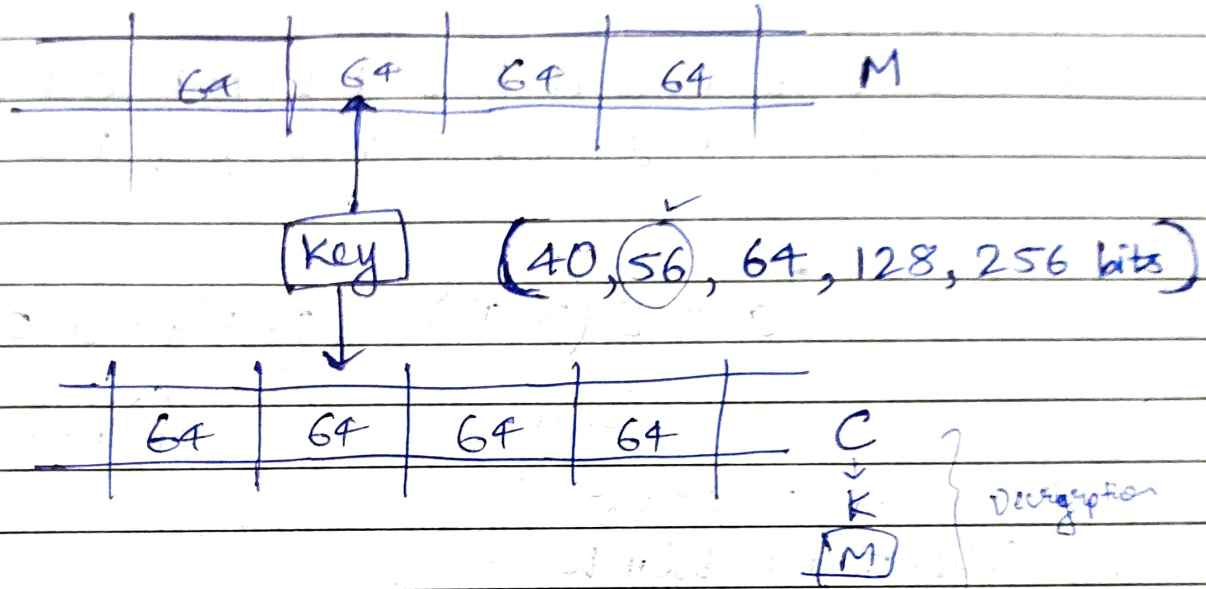
11100011
⊕ 01010101
10110110

XOR

$M_1 M_2 M_3 M_4 \dots M_n$
$\oplus K_1 K_2 K_3 K_4 \dots K_n$
$C_1 C_2 C_3 C_4 \dots C_n$

V-15

Block Cipher:



Substitution Cipher Technique-

V-16

V-17/18

Caesar Cipher :-

0 1 2 3 4
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
d e f g h i j k l m n o p q r s t u v w x y z a b c

$$C = E(3, P) = (P + 3) \bmod 26$$

↓ Encrypt.

C = cipher text
P = plain text

Plain text : FIVE
Cipher Text : ilyh

$$P = D(3, C) = (C - 3) \bmod 26$$

↓ decryption.

* Simple to implement
* less complexity ↓

V-18

* Security ↓

Mono Alphabatic - A→C C→Y ... B→X Z→D ... Given Table (same as Caesar cipher)

V-17/18

Playfair Cipher :

→ Take 2 letters.
→ if 2 same letter then add x between 2
→ last letter single ? add x.

row : → rectangle : row →
column : ↓

X Y Z
a b c

Message ⇒ Jazz
Key ⇒ Monarchy

m	o	n	a	r
c	h	y	b	d
e	f	g	i/j	k
l	p	q	s	t
u	v	w	x	z

⇒ Ja zz
Ja zx z
Ja zx zx

⇒ Cipher : sb uz uz
= sbuzuz

message = off
Key = Monarchy
⇒ of fx
Cipher : hp iv = phiv

V-18/9

One-Time Pad : (Vernam Cipher) ⇒ XOR ⇒ C = P ⊕ K, P = K ⊕ K

(Vigenere cipher)

Plain text : H E L L O
7 4 11 11 14

A B C D E F ...
0 1 2 3 4 5 ...

Key : b a x y c
1 0 23 24 2

Add : 8 4 34 35 16
(mod 26) ⇒ 8 4 8 9 16

Cipher text : i e i j q

(No substitution)

FULLSCAPE PAGE NO.: DATE

V-20

Transposition Cipher:

① Columnar Transposition technique:

P: FIVE
MINUTE
ENGINEERING

1	2	3	4	5
F	I	V	E	M
I	N	U	T	E
E	N	G	I	N
E	E	R	I	N
G				

Key = 43512 (Top to down)

C: ~~EOMEI~~ ETII VUGR MENN FIEEG INNE

V-21

② Keyless Transposition technique:

ROW 1: I E I V E

ROW 2: F V M N T

C: IEIVE FVMNT

V-50

Hill Cipher:

A=0 B=1 C=2 ... X=23 Y=24 Z=25

Key: $\begin{bmatrix} H & I \\ L & L \end{bmatrix}_{2\times2} = \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix}$

Plain text: Short example ⇒ $\begin{bmatrix} S \\ h \end{bmatrix}_{2\times1} \begin{bmatrix} O \\ r \end{bmatrix} \begin{bmatrix} t \\ e \end{bmatrix} \begin{bmatrix} x \\ a \end{bmatrix} \begin{bmatrix} m \\ p \end{bmatrix} \begin{bmatrix} L \\ e \end{bmatrix}$

$\Rightarrow \begin{bmatrix} 18 \\ 7 \end{bmatrix} \begin{bmatrix} 14 \\ 17 \end{bmatrix} \begin{bmatrix} 19 \\ 4 \end{bmatrix} \begin{bmatrix} 23 \\ 0 \end{bmatrix} \begin{bmatrix} 12 \\ 15 \end{bmatrix} \begin{bmatrix} 11 \\ 4 \end{bmatrix}$

$C = KP \bmod 26$

$\Rightarrow \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \begin{bmatrix} 18 \\ 7 \end{bmatrix}$

$\Rightarrow \begin{bmatrix} 182 \\ 275 \end{bmatrix} \% 26$

$\Rightarrow \begin{bmatrix} 0 \\ 15 \end{bmatrix} \Rightarrow \begin{bmatrix} A \\ P \end{bmatrix}$

$\Rightarrow \begin{bmatrix} A \\ P \end{bmatrix} \begin{bmatrix} A \\ D \end{bmatrix} \begin{bmatrix} J \\ T \end{bmatrix} \begin{bmatrix} F \\ T \end{bmatrix} \begin{bmatrix} W \\ L \end{bmatrix} \begin{bmatrix} F \\ J \end{bmatrix}$

⇒ C: APADJTFTWLFJ

Rain fence Technique:

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

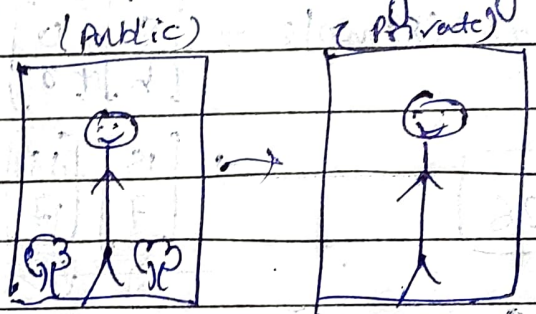
Ciphar: ttna aptm tsuo .....

V-22

Steganography:

→ covered / secrete writing

- LSB, Audio/video steganography, still imagery

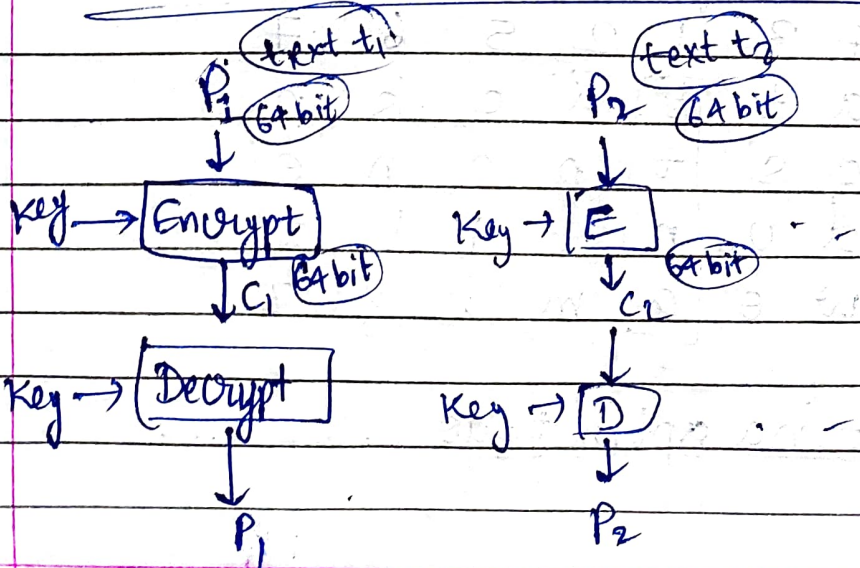


(Tree is missing
∴ Reciever will understand

⇒ Steganalyst.
(Those who try to crack the algo)

V-23 **Block cipher mode:**

① **Electronic CodeBook (ECB) mode:**



Drawback

If text t_1 & t_2 are same then C_1 & C_2 will be same. So cryptanalyst will find the word.

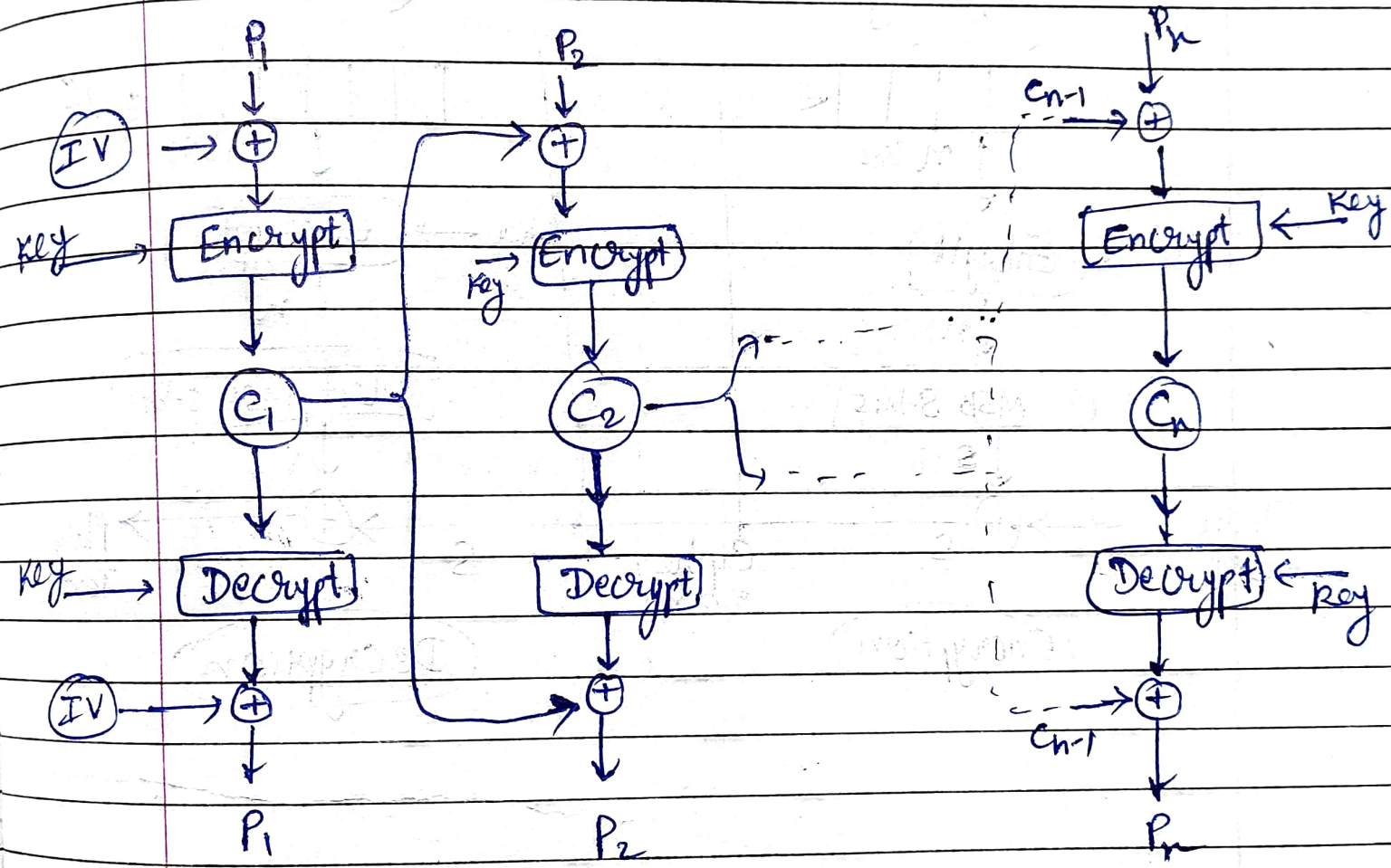
IV = Initialisation vector

⊕ = XOR.

FULLSCAPE PAGE NO.: DATE

v-24

② Cipher Block chaining mode (CBC)

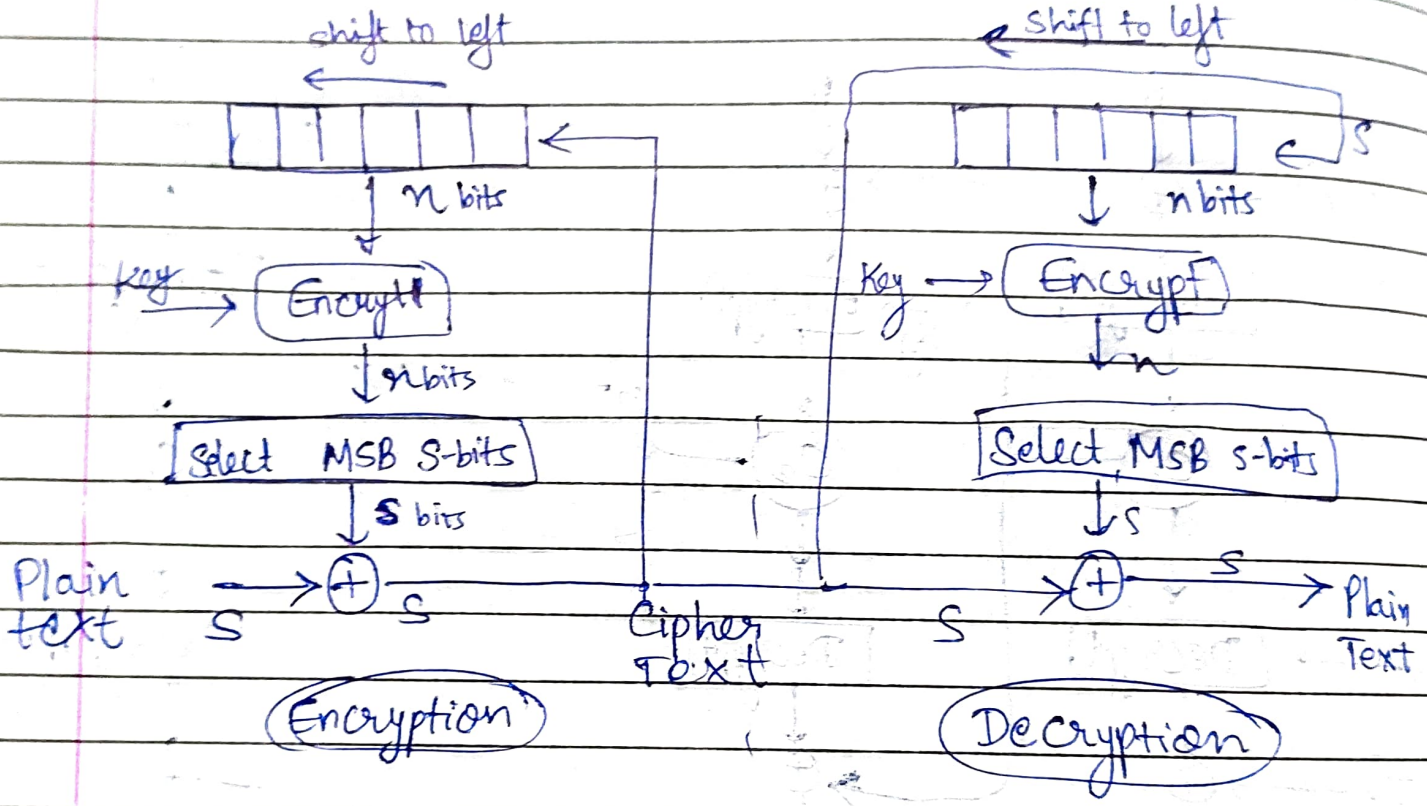


V-25

FULLSCAPE
PAGE NO.: DATE

③ Cipher Feedback mode: (CFB)

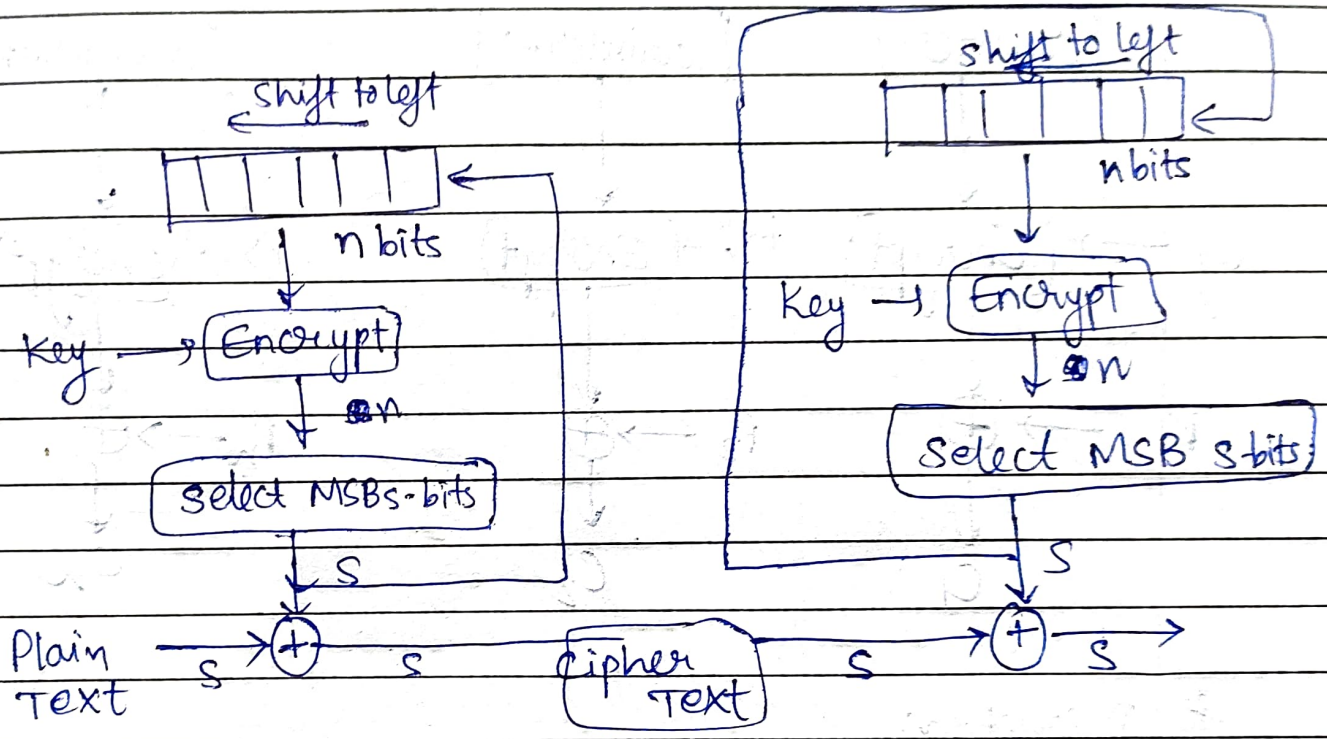
$1 < s < n$



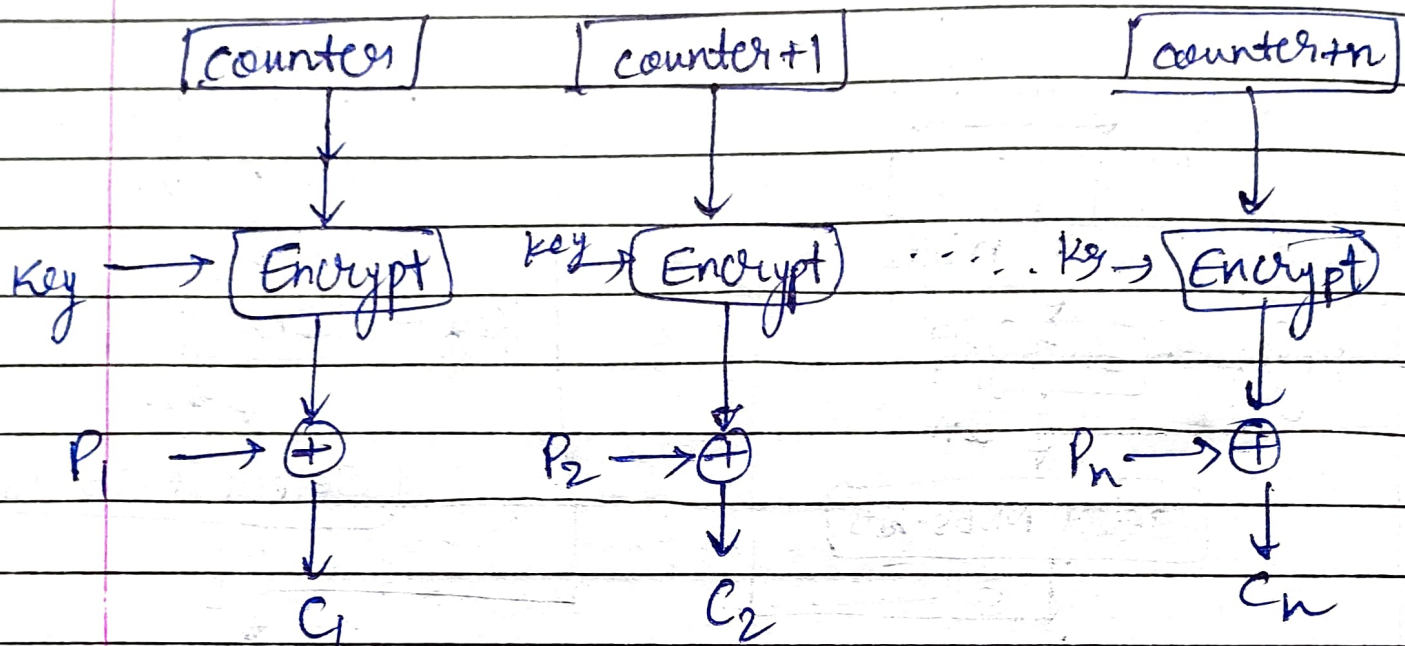
FULLSCAPE
PAGE NO.: DATE

(4) Output feedback mode : (OFB)

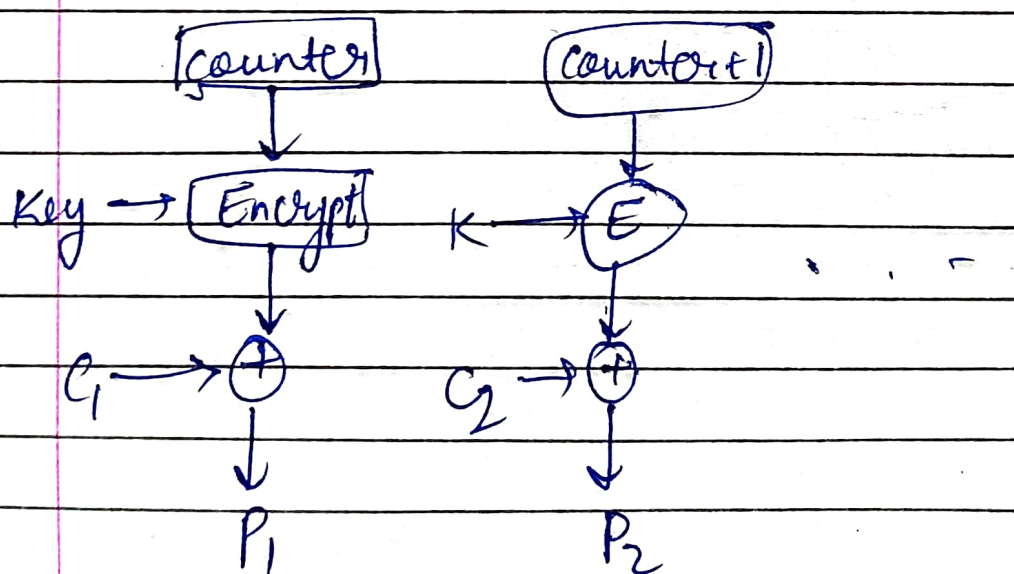
$1 < s < n$



(5) Counter mode (CTR):

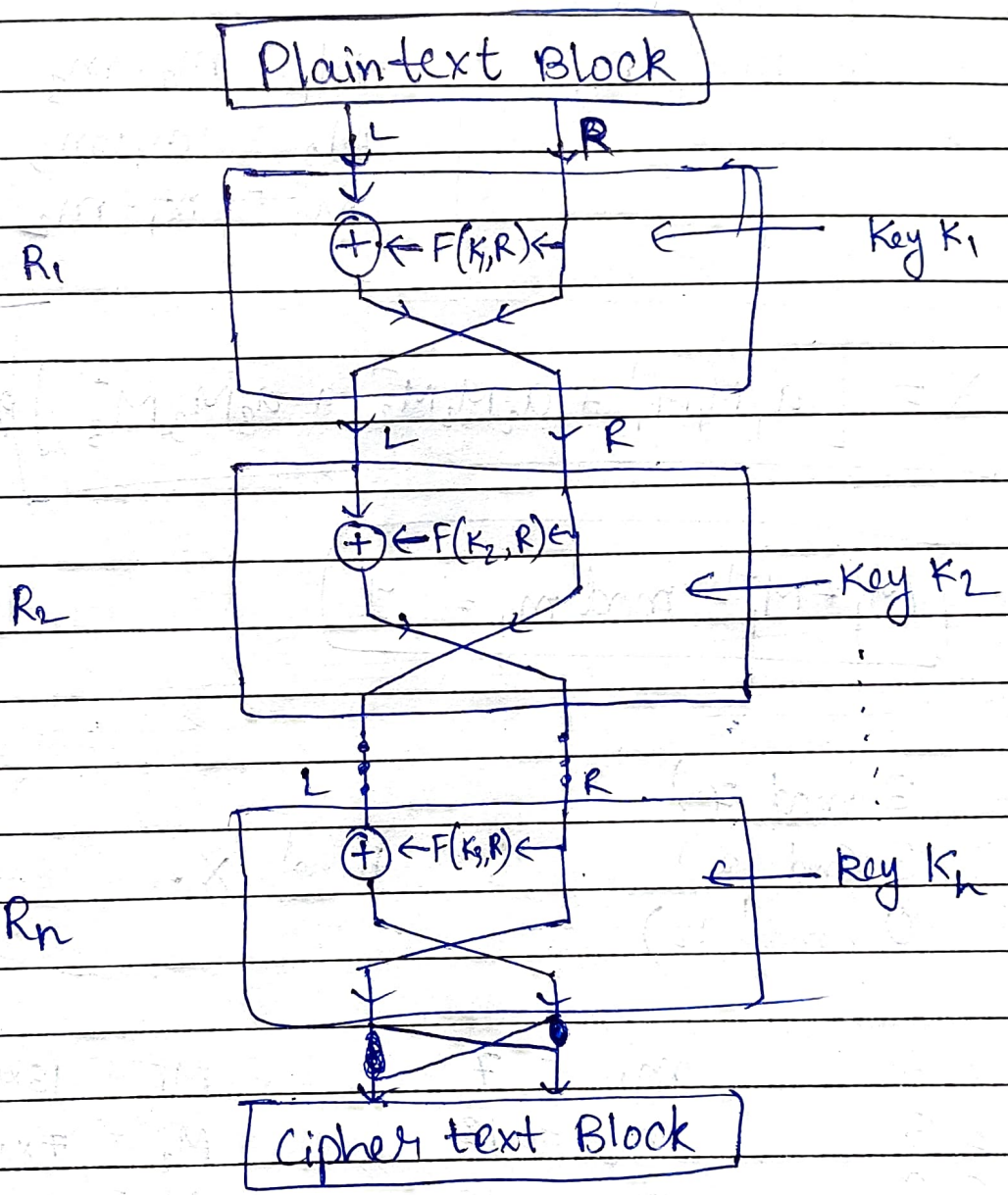


(6) Decryption:



V-28.

Feistel Cipher -



* Chinese Remainder Theorem (CRT)

FULLSCAPE PAGE NO.: DATE

$X \equiv a_1 \bmod m_1$
$X \equiv a_2 \bmod m_2$
$X \equiv a_3 \bmod m_3$

$M = m_1 \cdot m_2 \cdot m_3$

$M_1 = m_2 \cdot m_3$
$M_2 = m_1 \cdot m_3$
$M_3 = m_1 \cdot m_2$

$$X = \left[a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1} \right] \% M$$

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

Q.) $X \equiv 3 \pmod 7$
$X \equiv 3 \pmod{13}$
$X \equiv 0 \pmod{12}$

Find X.

ans:

$a_1 = 3$ $m_1 = 7$ $M_1 = 13 \times 12 = 156$
$a_2 = 3$ $m_2 = 13$ $M_2 = 7 \times 12 = 84$
$a_3 = 0$ $m_3 = 12$ $M_3 = 7 \times 13 = 91$

$M = 7 \times 13 \times 12 = 1092$

$M_1 * M_1^{-1} \bmod m_1 = 1$
$156 * M_1^{-1} \bmod 7 = 1$

let, M_1^{-1} ⇒
$156 \times 1 \,\%\, 7 = 2$ ✗ ($M_1^{-1} = 1$)
$312 \,\%\, 7 = 0$ ✗ ($M_1^{-1} = 2$)
$468 \,\%\, 7 = 6$ ✗
$624 \,\%\, 7 = 1$ ✓ ($M_1^{-1} = 4$) ✓

$84 * M_2^{-1} \% m_2 = 1$
① $84 \,\%\, 13 = 6$ ✗
② $168 \,\%\, 13 = 1$ ✓ ($M_2^{-1} = 2$)
✗
✗
⑪ ✓ ($M_2^{-1} = 11$)

FULLSCAPE
PAGE NO.: DATE

$$\therefore X = \left(3\times(156\times 4) + 3\times(84\times 11) + 0(\quad)\right) \div M$$

$$= (1872 + 2772) \div 1092$$

$$= (4644) \div 1092$$

$$= 276$$

$$\boxed{X = 276}$$

* Inverse of Matrix:

Q:) $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ $\quad A^{-1}$?

ans: $A^{-1} = \frac{1}{|A|}\, adjA$

$$|A| = \begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix} = 1(4) - 2(3)$$

$$= 4 - 6$$

$$= (-2)$$

$$adjA = C^T = \begin{bmatrix} 4 & -3 \\ -2 & 1 \end{bmatrix}^T$$

$$= \begin{bmatrix} 4 & -2 \\ -3 & 1 \end{bmatrix}$$

$$\therefore A^{-1} = \frac{-1}{2} \cdot \begin{bmatrix} 4 & -2 \\ -3 & 1 \end{bmatrix}$$

Multiplicative inverse of (-2) =>

$$(-2 \times x) \bmod 26 = 1$$

$x = 1$ $\quad -2 \bmod 26 = 24 \neq 1$

$\vdots$

$x = 12$ $\quad -24 \bmod 26 =$

(Q.) Find $11^7 \bmod 13$

ans:

$11 \bmod 13 = 11$

$11^2 \bmod 13 = 121 \bmod 13 = 4$

$11^4 \bmod 13 = (11^2) \bmod 13 = (4)^2 \bmod 13 = 3$

$\therefore 11^7 \bmod 13 = (11 \cdot 11^2 \cdot 11^4) \bmod 13$

$= (11 \cdot 4 \cdot 3) \bmod 13$

$= 132 \bmod 13$

$= 2$

V-29

Modular Arithmetic:

① $x \equiv y \bmod n$ (If both x & y have same reminder when divided by 'n')

↓ (congruent)

eg: $36 = 24 \bmod 12$

② $x \equiv y \bmod n$ (If n divides $(x-y)$)

eg: $20 = 3 \bmod 17$ [17 divides $(20-3=17)$]

③ If $x \equiv y \bmod n$ & $a \equiv b \bmod n$, Then

$(x+a) \equiv (y+b) \bmod n$

eg: $17 \equiv 4 \bmod 13$ & $42 \equiv 3 \bmod 13$

$\therefore 59 \equiv 7 \bmod 13$

④ If $x \equiv y \bmod n$ & $a \equiv b \bmod n$, Then

$(x-a) \equiv (y-b) \bmod n$

eg: $42 \equiv 3 \bmod 13$ & $14 = 1 \bmod 13$

$\therefore 28 \equiv 2 \bmod 13$

V-30

⑤ If $x \equiv y \bmod n$ & $a \equiv b \bmod n$, Then

$$(x * a) \equiv (y * b) \bmod n$$

eg: $6 \equiv 1 \bmod 5$, $7 \equiv 2 \bmod 5$ $\Rightarrow 42 \equiv 2 \bmod 5$

⑥ If $x \equiv (y \times z) \bmod n$ then $x \equiv (y \bmod n \times z \bmod n) \bmod n$

eg: $7 \equiv (12 \times 11) \bmod 5$

$7 \equiv (12 \bmod 5 \times 11 \bmod 5) \bmod 5$

$7 \equiv (2 \times 1) \bmod 5$

$\Rightarrow 7 \equiv 2 \bmod 5$ ✓

y & z are very large

⑦ $x \equiv (y + z) \bmod n$ then,

$x \equiv (y \bmod n + z \bmod n) \bmod n$

eg: $8 \equiv (11 + 12) \bmod 5$

$\equiv (11 \bmod 5 + 12 \bmod 5) \bmod 5$

$\equiv (1 + 2) \bmod 5$

$\Rightarrow 8 \equiv 3 \bmod 5$ ✓

By- Pathik455

FULLSCAPE PAGE NO.: DATE

V-31

Euler's Totient function:

- $\phi(n)$ for $(n \geq 1)$ is defined as the number of +ve integer less than 'n' that are co-prime to 'n'

  ↓ gcd = 1 (lowest common factor)

  $\phi(5) = \{1, 2, 3, 4\} = 4$

  $\phi(4) = \{1, 3\} = 2$

- When 'n' is a prime number

  $\phi(n) = n - 1$; eg: $\phi(23) = 22$

- $\phi(a * b) = \phi(a) * \phi(b)$ [a & b are co-prime]

  a, b should be prime no.

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

  $= \phi(7) * \phi(5)$ ($\because \gcd(7, 5) = 1$)

  $= 6 * 4$

  $\phi(35) = 24$

V-32

Multiplicative Inverse:

$x \not\equiv 0 \bmod n$ (n is prime)

$x \cdot y = 1 \bmod n$ ['y' is multiplicative inverse of 'x']

$y = x^{-1} \bmod n$

V-31

Euler's Totient function:

- $\phi(n)$ for $(n \geq 1)$ is defined as the number of +ve integer less than 'n' that are co-prime to 'n'

  co-prime → gcd = 1 (lowest common factor)

$\phi(5) = \{1, 2, 3, 4\} = 4$

$\phi(4) = \{1, 3\} = 2$

- When 'n' is a prime number

  $\phi(n) = n - 1$; eg: $\phi(23) = 22$

- $\phi(a * b) = \phi(a) * \phi(b)$ [a & b are co-prime]

  a, b should be prime no.

  eg: $\phi(35) = \phi(7 * 5)$ ($\because$ gcd(7, 5) = 1)

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

  $= 6 * 4$

  $\phi(35) = 24$

V-32

Multiplicative Inverse:

$x \neq 0 \bmod n$ (n is prime)

$x \cdot y = 1 \bmod n$ ['y' is multiplicative inverse of 'x']

$y = x^{-1} \bmod n$

Q) Find Multiplicative inverse of 15 or 15^{-1} or $\frac{1}{15}$

Ans: $(15 * x) \% 26 = 1$

$x = 1 \quad 15 \% 26 \neq 15 \neq 1$

$x = 2 \quad 30 \% 26 = 4 \neq 1$

$\vdots$

$x = 7 \Rightarrow 105 \% 26 = 1 = 1$

$\therefore$ Multiplicative inverse $= 7$

V-33 Euler's Theorem:

$$x^{\phi(n)} = 1 \bmod n \quad \text{or} \quad x^{\phi(n)*a} = 1 \bmod n$$

Q) $x = 4$

$n = 165$

$\therefore (4)^{\phi(165)} = 1 \bmod 165$

$$\phi(165) = \phi(15) \times \phi(11)$$
$$= \phi(3) \times \phi(5) \times \phi(11)$$
$$= 2 \times 4 \times 10$$
$$= 80$$

$\therefore \boxed{4^{80} = 1 \bmod 165}$

On dividing 4^{80} with 165 it will give remainder 1.

V.39

Fermat's Theorem:

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

$\phi(n) = n-1$

① * n = prime

② * x is not divisible by n

$$x \not\equiv 0 \bmod n$$

eg: $x = 3$

$n = 5$ (prime ✓, x is not divisible by 5 ✓)

$$3^{5-1} \equiv 1 \bmod 5$$

$$\therefore \boxed{81 \equiv 1 \bmod 5}$$

$$\Rightarrow \boxed{x^{\phi(n)} = 1 \bmod n}$$ Euler's

$$\Downarrow$$

$$\boxed{x^{n-1} = 1 \bmod n}$$ Fermat's

also,

$$x \cdot (x^{n-1}) = x \cdot (1 \bmod n)$$

$$\boxed{x^n = x \bmod n}$$ fermat's

↳ only if $\boxed{\gcd(x, n) = 1}$ *

$$\boxed{3^5 = 3 \bmod 5}$$

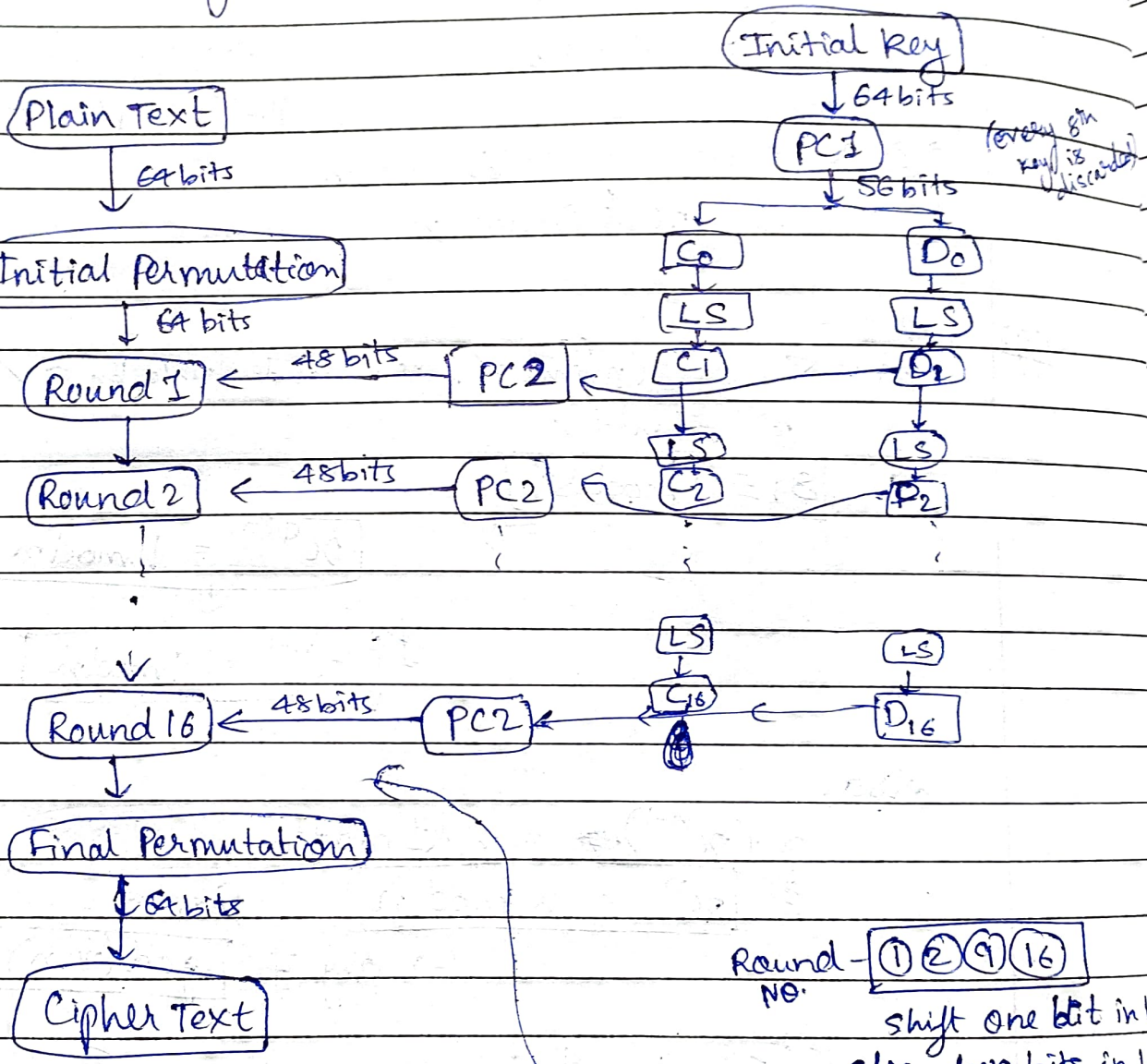
V-56

(Data Encryption Standard)
DES algorithm:

C, D = 2 half of keys

PC = Permutate choice

LS = Left shift (circular)

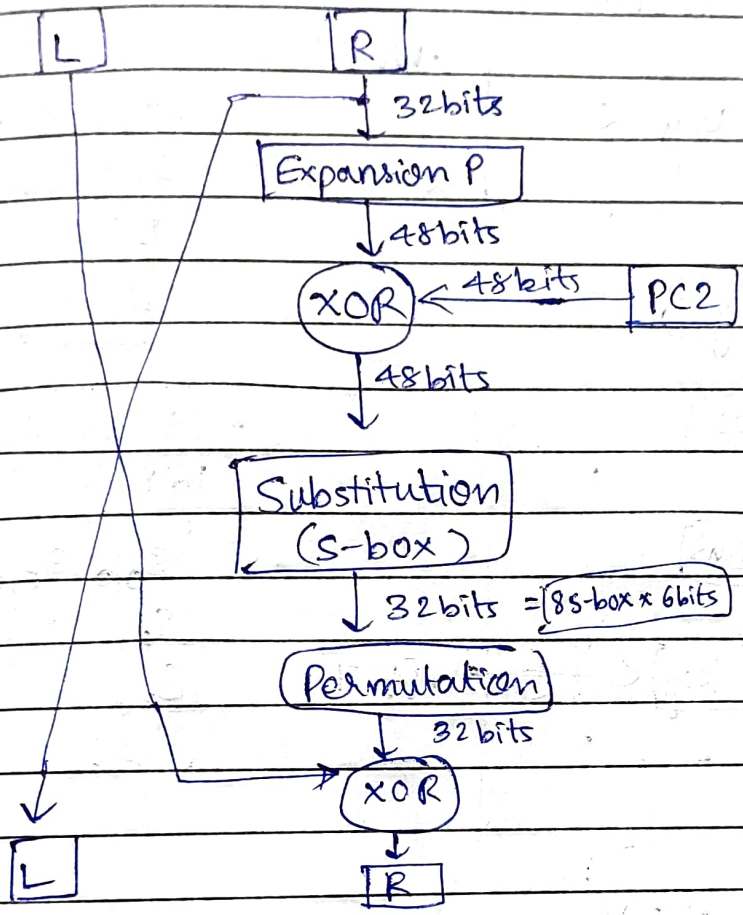


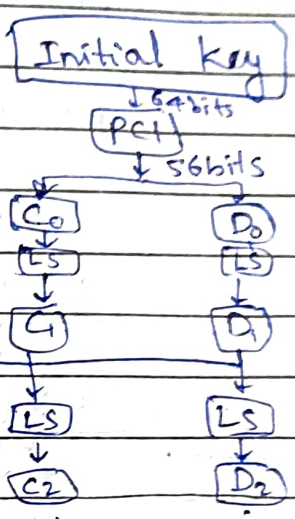
Round No.	1	2	9	16

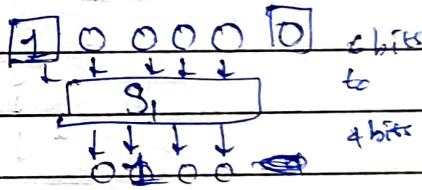
shift one bit in LS
else two bits in LS

(expansion permutation
compression permutation)

Rounds:

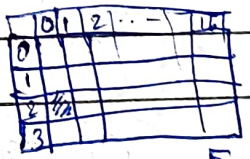




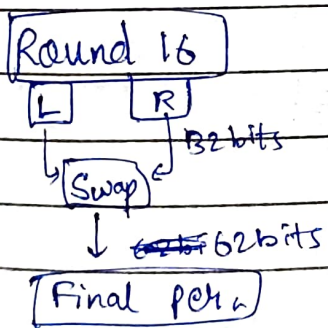


10 : 2 bits } Table.
0000 : 4 bits

∴ 2bits = 2^2 = 4rows (0,1,2,3)
4bits = 2^4 = 16columns (0,1,2,3 ... 15)

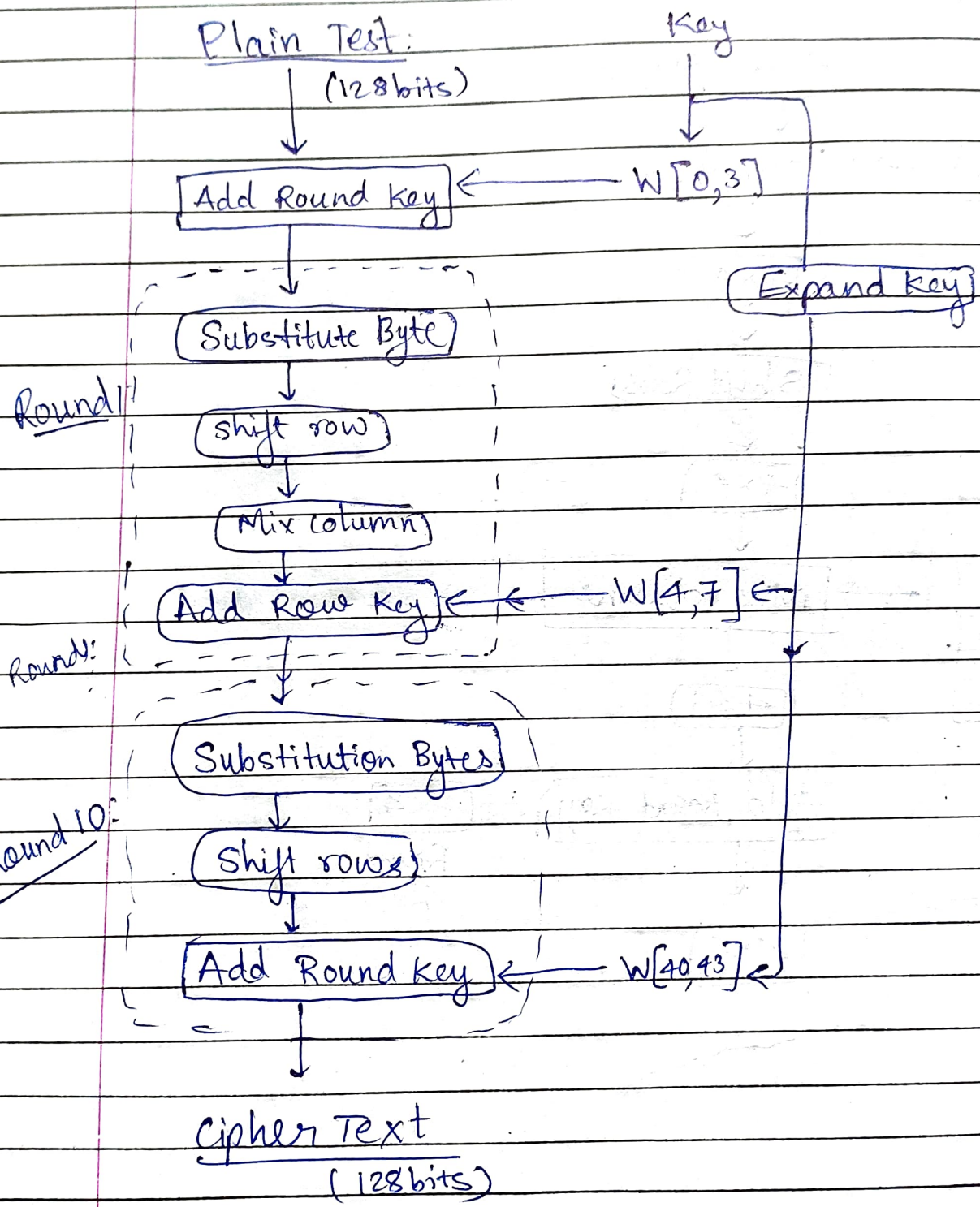


R: 10 ⇒ 2
C: 0000 ⇒ 0
eg: 4 was the value in (2,0)
∴ S_1: 0100



Cipher.

AES:



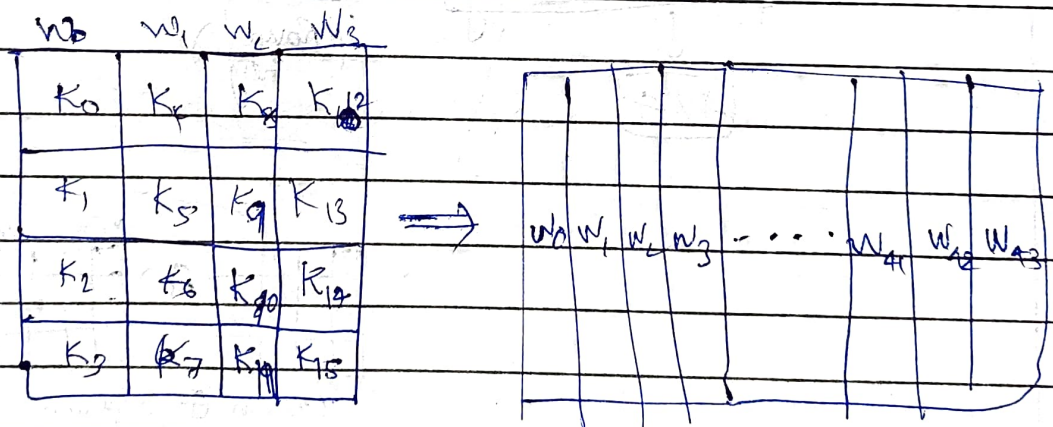
FULLSCAPE
PAGE NO.: DATE

* Input Array 128bits (4x4) = 16Bytes / 4words.

* State Array (4x4) 16Byte / 4words

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

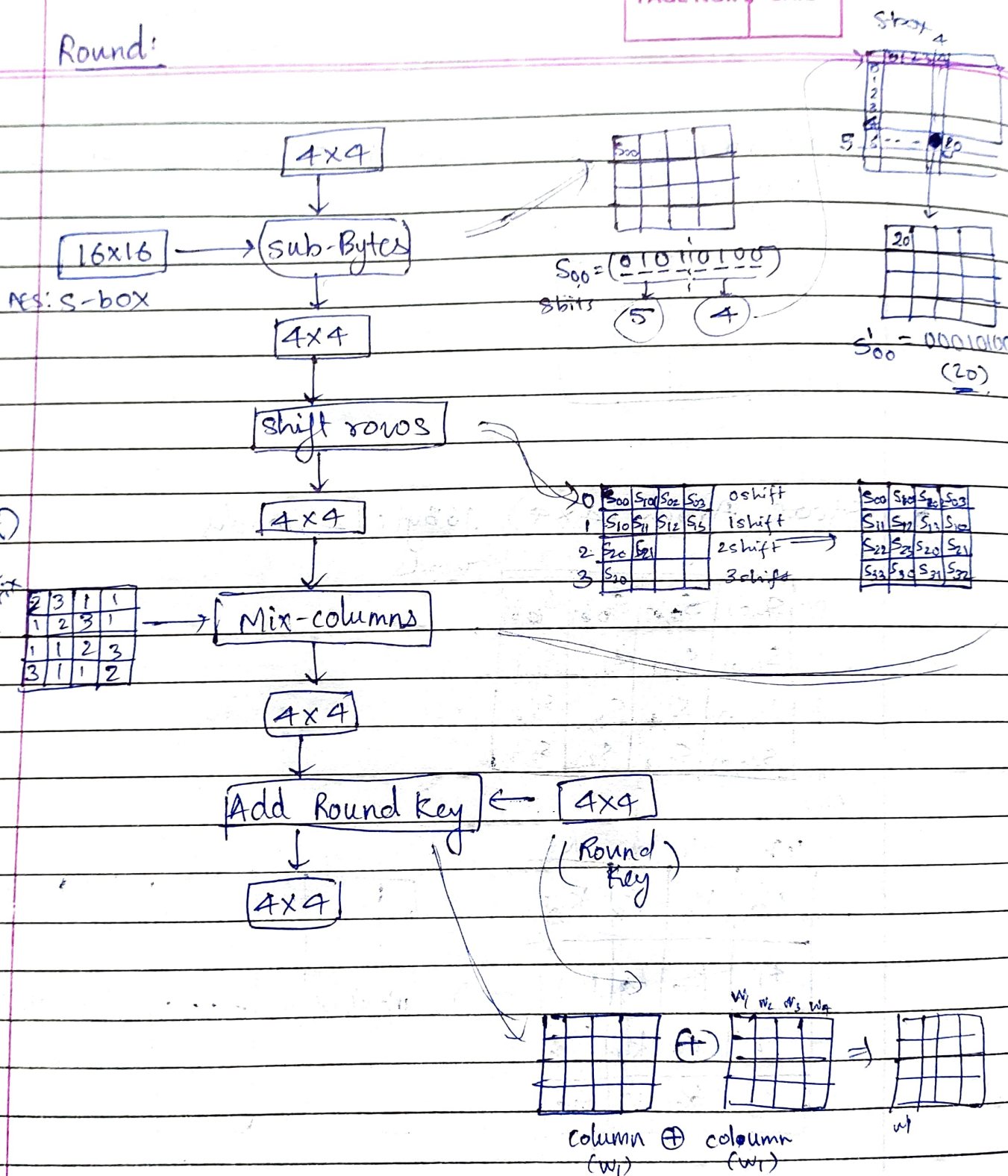
↑ Bits

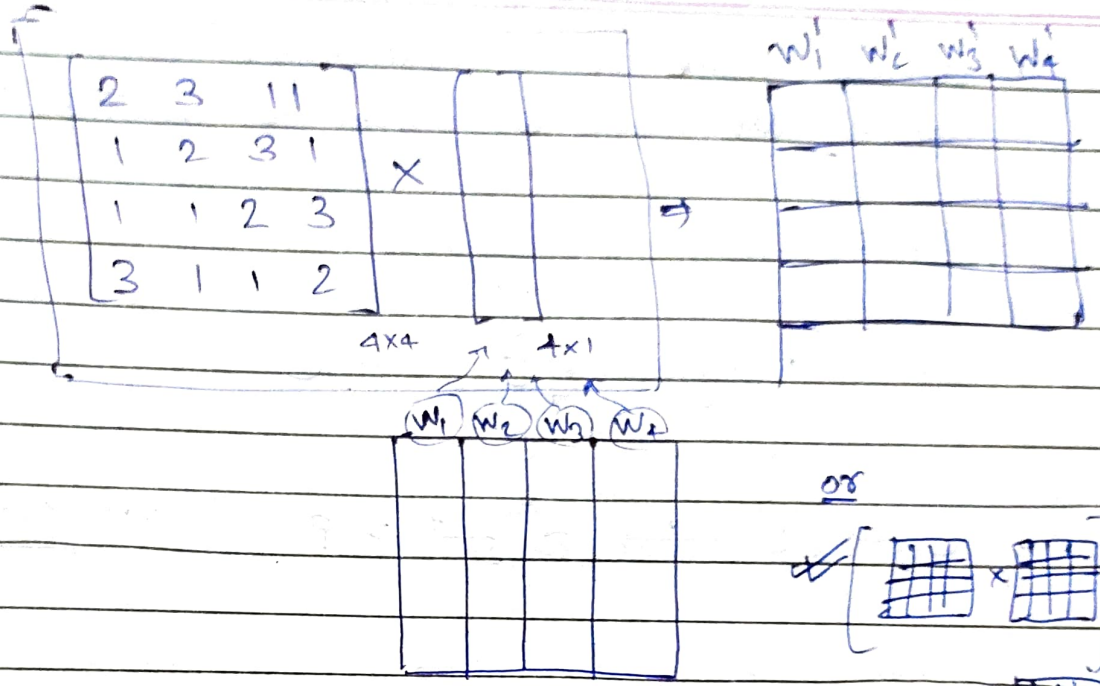


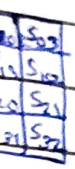
4words 44words

FULLSCAPE
PAGE NO.: DATE

Round:



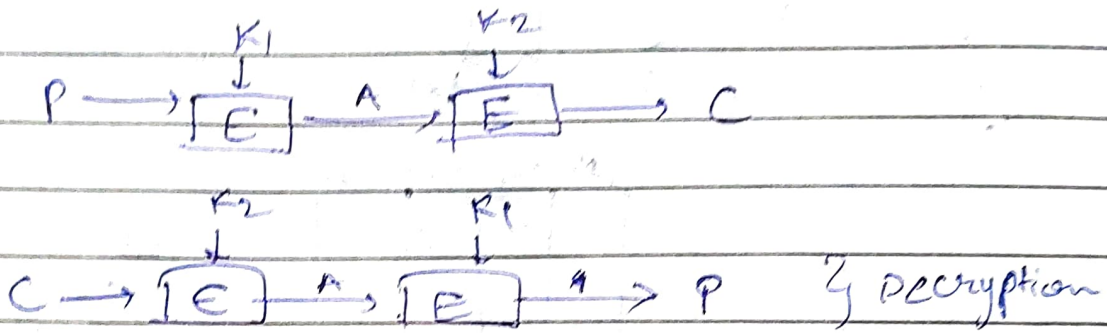




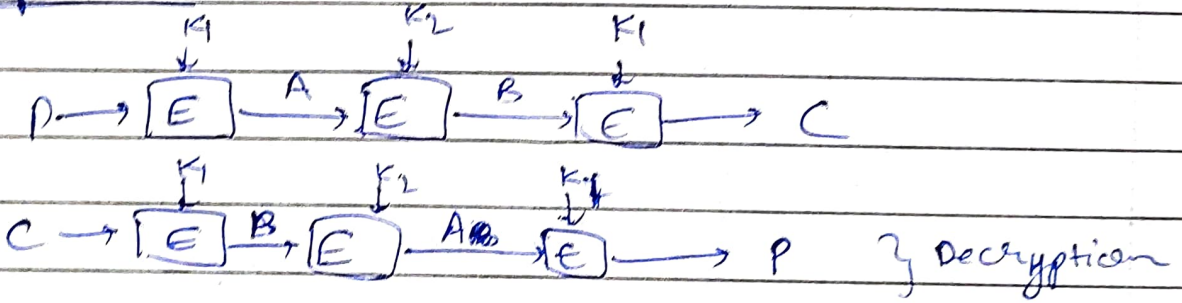
or

* DES is vernerable to brute force
so, we use AES or, Double DES or, Triple DES

Double DES:



Triple DES: (2-Key)



(3-Key) $K_1 - K_2 - K_3$ then $K_3 - K_2 - K_1$ in decryption.

FULLSCAPE PAGE NO.: DATE

RSA algorithm: (Rivest, Shamir, Adlemann)

(1) Choose 2 prime nos, p & q:
eg: p=61, q=53

(2) Compute: $n = p \times q = 61 \times 53 = 3233$
$\boxed{n = 3233}$

(3) $\phi(n) = \phi(p \times q) = \phi(p) \times \phi(q)$
$= (p-1) \times (q-1)$
$= 60 \times 52$
$\boxed{\phi(n) = 3120}$

(4) Choose 'e'; $1 < e \leq \phi(n)$ ⇒ coprime to $\phi(n)$
$\boxed{\gcd(\phi(n), e) = 1}$

$\therefore e = 17$
$\therefore (e, n) =$ public key $(17, 3233)$

(5) Determine 'd'; $\boxed{e \cdot d = 1 \bmod \phi(n)}$

$17 \times d = 1 \bmod 3120$ (d is MI of e)

$\boxed{d = 2753}$ (back page to cal. d.)

$\therefore (d, n) =$ private key $(2753, 3233)$

V-40

RSA (finding d)

$\Rightarrow \quad e \cdot d = 1 \bmod \phi(n)$

$$d = \frac{(\phi(n) \times i) + 1}{e}$$

$(i=1) \quad = \frac{(3120 \times 1) + 1}{17} = 183.58$

$(i=2) \quad = \frac{(3120 \times 2) + 1}{17} = 369.11$

$(i=3) \quad = \frac{(3120 \times 2) * 1}{17} = 550.647$

} Decimal X

$\vdots$

$(i=15) \quad = \frac{(3120 \times 15) + 1}{17} = 2753$ } integer ✓

$\therefore \boxed{(d, n) = (2753, 3233)}$

FULLSCAPE
PAGE NO.: DATE

1-41 RSA

Encryption (13, 143) — e, n

$C = P^e \bmod n$

$C = 13^{13} \bmod 143$

- $13 \bmod 143 = 13$

$13^4 \bmod 143 = 104$

$13^8 \bmod 143 = (104)^2 \bmod 143$

$= 91$

$\therefore C = [(13^8 \bmod 143) \cdot (13^4 \bmod 143) \cdot (13 \bmod 143)] \bmod 143$

$= (13 \times 104 \times 91) \bmod 143$

$C = 52$

Decryption: (37, 143) — d, n

$P = C^d \bmod n$

$= 52^{37} \bmod 143$

- $52 \bmod 143 = 52$

$52^4 \bmod 143 = 26$

$52^{32} \bmod 143 = (52^4)^8 \bmod 143$

$= (26)^8 \bmod 143$

$= 130$

$\therefore P = [(52 \bmod 143) \cdot (52^4 \bmod 143) \cdot (52^{32} \bmod 43)] \cdot \bmod 143$

$= [130 \times 26 \wedge 52] \bmod 143$

$P = 13$

* Attacking RSA algorithm
  - Brute-force Attack
  - Mathematical attack
  - Timing attack

PAGE NO.: DATE

~~Secure Hash Value is (SHA-1)~~

Elgamal: (Asymmetric key)

① Key Generation:

prime no. $P = 11$

Decryption key $d = 3$
(Private)

encryption key $e_1 = 2$ $\quad e_2 = e_1^d \bmod p$

$e_2 = 2^3 \bmod 11 = 8$

$e_2 = 8$

P, d, e_1, e_2

Public key = $(e_1, e_2, P) = (2, 8, 11)$

② Encryption:

random Integer (R) $\quad R = 4$

$C_1 = e_1^R \bmod p = 2^4 \bmod 11 = 5$

$C_1 = 5$

$C_2 = (P_T \times e_2^R) \bmod p$

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

$C_2 = 6$

P_T = Plain Text.

$P_T = 7$ Assume

FULLSCAPE
PAGE NO.: DATE

Cipher Text $(C_1, C_2) = (5, 6)$

③ Decryption:

$$P_T = \left[C_2 \times \left((C_1)^d \right)^{-1} \right] \bmod P$$

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

$$= 6 \times (125)^{-1} \bmod 11$$

~~$= 6 \times (125 \times x \bmod 11 = 1)$~~

~~$= 6 \times (375 \bmod 11 = 1)$~~
~~$x = 3$~~

If $x = 3$
$375 - 1 \cdot 11 = 1$

~~$= 6 \times 3 \bmod 11$~~

$x = 3$

$$= 6 \bmod 11 \times (125)^{-1} \bmod 11$$

$$= 6 \times (3 \bmod 11)$$

$$= 18 \bmod 11$$

$P_T = 7$

Diffi-Hellman Key Exchange:

Agent X (Private ~~channel~~ Area)	enemy (Public channel)	Agent Y (Private ~~channel~~ Area)
Select $X_A < p$	step 1: Prime Number (p) = 13	Select $Y_A < p$
Private key: (X_A & Y_A) eg: $X_A = 3$	Generator (g) = 2 (g = primitive root of p)	eg: $Y_A = 7$
$A = g^{X_A} \bmod p$		$B = g^{Y_A} \bmod p$
$A = 2^3 \bmod 13$		$B = 2^7 \bmod 13$
$A = 8$ →		$B = 11$
	$B = 11$ ← $A = 8$	
$S1 = B^{X_A} \bmod p$		$S2 = A^{Y_A} \bmod p$
$S1 = 11^3 \bmod 13$	enemy knows $A = g^{X'_A} \bmod p$	$S2 = 8^7 \bmod 13$
$S1 = 5$ ✓	$8 = 2^{X'_A} \bmod 13$	$S2 = 5$ ✓
Secret Key	(X'_A & Y'_A are too big it could not be found)	Secret Key

$S1 = S2$

Man-in-Middle Attack-

FULLSCAPE
PAGE NO.: DATE

Digital Signature:

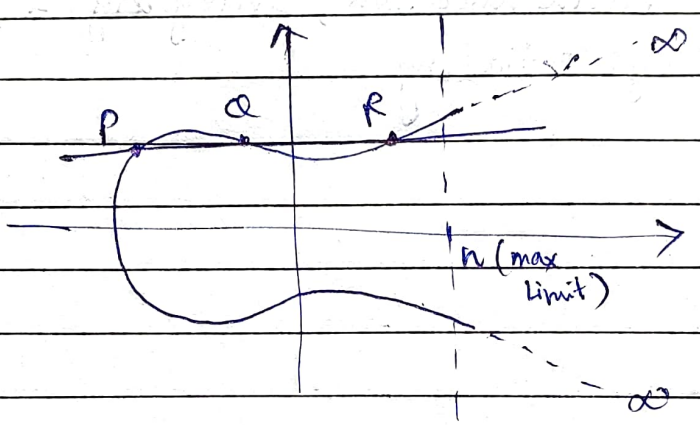
→ Imp. role in E-commerce, online trans., etc.
→ based on Asymm. key cryptography.
Encryp. = Private key
Decryp = Public key
→ Used for Authentication, Integrety & non-repudiation.
→ Not for confidentiality.

FULLSCAPE
PAGE NO.: DATE

ECC: (Elliptic Curve Cryptography)

* Asymmetric
* Small key size / High security
* Elliptic curve

$y^2 = x^3 + x + C$ (degree = 3)



- Symmetric to X-axis
- If we draw line it will touch atmost 3 points

* Trapdoor fn: A → B easy
A ← B (hard !!)
But A ← B easy if we have (trapdoor key)

* $Q = KP$ If we have Q, P we can't find K key.
If we have K, P we can find Q easily.

Discrete logarithm problem.

(1) Key Generation:

Global Public elements → $E_q(a,b)$: elliptic curve with parameter (a,b) (q = prime / 2^m)

G_1: Point on the curve / elliptic curve where $> n$

User A	User B
Private Key = n_A	Private Key = n_B
Public Key $P_A = n_A \times G_1$	Public Key $P_B = n_B \times G_1$
Calculate Secret Key $K = n_A \times P_B$	Calculate Secret Key $K = n_B \times P_A$

(2) Encryption:

→ First encode the msg to a point P_m on the eliptic curve.

chose random positive integer K,

$\therefore C_m = (KG_1, P_m + KP_B)$

↳ cipher text for encryption of publickey B.

(3) Decryption:

multiply private key of B (n_B) ⇒ for decryption

$KG_1 * n_B$

Substract 2nd point,

i.e. $P_m + KP_B - KG_1 * n_B$

we know $P_B = n_B \times G_1$

$P_m + K(n_B \times G_1) - KG_1 n_B = P_m$ ← Got original point.

FULLSCAPE PAGE NO.: DATE

RSA

→ p, q prime
→ $n = p \times q$
→ $\phi(n) = (p-1)\cdot(q-1)$
→ $e = 1 < e < \phi(n)$ (Assume e)
$\gcd(\phi(n), e) = 1$
→ $e \cdot d = 1 \bmod \phi(n)$

Finding $d = \left(\frac{\phi(n) \times x + 1}{e}\right)$

(e, n) Public key
(d, n) = Private key

Cipher text: $C = P^e \bmod n$
Plain Text: $P = C^d \bmod n$

Elgamal:

Prime P
encryption key e_1
decryption key $d \rightarrow$ (Private)
encrypt $e_2 = e_1^d \bmod P$
Public → $E(e_1, e_2, P)$ key

encry: $C_1 = e_1^R \bmod P$ (R = Random no.)
$C_2 = (P_T \cdot e_2^R) \bmod P$
(C_1, C_2) ciphers

Decry: $P_T = (C_2 \times (C_1^d)^{-1}) \bmod P$

D-H.

Prime no. $P = 13$
Generator $g = 2$ (Primitive root)

A user	B user
Private key $X_A = 3$	$X_B = 7$ $< P$
$A = g^{X_A} \bmod P$	$B = g^{X_B} \bmod P$
(Public key A, B) B → A, A → B	
$S_1 = B^{X_A} \bmod P$	$S_2 = A^{X_A} \bmod P$

$S_1 = S_2$ Always
Secret Key

ECC

$E_q(a,b)$ q = prime / 2^m
G = point > n.

A user	B user
Private key n_A	n_B
Public key $P_A = n_A \cdot G$	$P_B = n_B \cdot G$
Secret Key $K = n_A \cdot P_B$	Se. K. $K = n_B \cdot P_A$

E: $C_m = (KG, P_m + KP_B)$

D: $(P_m + KP_B) - (K \cdot G_1 * n_B)$ ($P_B = n_B \cdot G$)

P_m