Information Security

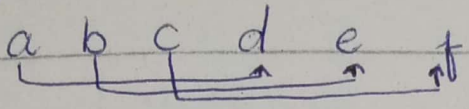
10 domains of IS

Ceasar Cipher:

Plain text : meet me after toga party

Cipher text : PHHW PH DIWHU WRJD SDUWB

→ Replacement w.r.t defined place



For decryption, move backward.

Using Modulo Math:

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

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

Ceasar Cipher (ROT-13) Rotation - 13

A	B	C	D	E	....	M
↕	↕	↕	↕	↕		↕
N	O	P	Q	R	....	Z

Plain ⇒ H E L L O

Cipher ⇒ U R Y Y B

Problem with Ceasar cipher

→ Brute force attack ⇒ try all possible combination

→ In case of ceasar cipher they are only 25. So encrypted message will be easily decrypted.

Substitution (Mono Alphabetic):

→ Decide yourself to replace a particular letter with other one

A → B k = +1

B → V k = +20

C → G k = +4

D → Q k = +13

Don't replace two letters with same

With keyword:

keyword = KEYWORD

P.L ⇒	A	B	C	D	E	F	G	H	I	J
	K	E	Y	W	O	R	D	A	B	C

K	L	M	N	O	P	Q	R	S	T	
F	G	H	I	J	L	M	N	P	Q	
U	V	W	X	Y	Z					
S	T	U	V	~~X~~	Z					

P.t = a L K i n d i

C.t = K G F B I W B

Homophone cipher:

A	B	C	D	E	F	G	H	I	J
D 9	X	S	F	Z 7 2 1	E	H	C	V 3	I

K	L	M	N	O	P	Q	R	S	T
T	P	G	A 5	Q 0	L	K	J	R 4	U 6

U	V	W	X	Y	Z
O	W	M	Y	B	N

M9PP

Cipher - F7E25F UC2 1DR6 ↑ ØE SD4UP1

WALL

Plain = DEFEND THE EAST ↓ OF CASTLE

Playfair cipher:

→ Digraph Substitution cipher

keyword = MONARCHY

→ Matrix 5x5

→ I/J replacement

→ Repeating letter → (x)

↑

M	O	N	A	R
C	H	X	B	D
E	F	G	I	J
K	L	P	Q	S

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

Keyword : Monarchy

Hello Plaintext : Instrumentsx

Helxlo GATLMZCLRQXA

HS → With same row or column
↓ replace with next letter
BP
EA → IM → with diagonals/non-dia → see in corresponding in rows.

30-01-24

Hill Cipher :

Msg : act → column vector

key : gybnqkurp (3)

Encryption :

$$C = KP \bmod 26$$

$$= \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} \bmod 26 \Rightarrow \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix}$$

C.T = POH

Decryption:

$$P = K^{-1}C \bmod 26$$

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}^{-1} = \begin{bmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{bmatrix} \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} = \begin{bmatrix} 260 \\ 574 \\ 539 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 0 \\ 2 \\ 19 \end{bmatrix} \Rightarrow \text{P.T} = \text{Act}$$

(Example)

✓ Plaint text P.T = Short Example

Key = Hill n=2

Cipher text = APADJTFTWLFJ

$C = KP \bmod 26$

$$C_1 = \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \begin{bmatrix} 18 \\ 7 \end{bmatrix} \bmod 26$$

(2)

$$= \begin{bmatrix} 126+56 \\ 198+77 \end{bmatrix} \bmod 26 \Rightarrow \begin{bmatrix} 182 \\ 275 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 0 \\ 15 \end{bmatrix} \Rightarrow \text{AP}$$

$C_2 = 0$

$$C_2 = KP \bmod 26$$

$$= \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \begin{bmatrix} 14 \\ 17 \end{bmatrix} \bmod 26 \Rightarrow \begin{bmatrix} 234 \\ 341 \end{bmatrix} \bmod 26 \Rightarrow \begin{bmatrix} 0 \\ 3 \end{bmatrix}$$

AD

= TE

$C_3 = KP \bmod 26$

$= \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \begin{bmatrix} 19 \\ 4 \end{bmatrix} \bmod 26 \Rightarrow \begin{bmatrix} 165 \\ 253 \end{bmatrix} \bmod 26 = \begin{bmatrix} 9 \\ 19 \end{bmatrix}$

C.T = J T

$C_4 = KP \bmod 26$ XA

$= \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \begin{bmatrix} 23 \\ 0 \end{bmatrix} \bmod 26 \Rightarrow \begin{bmatrix} 161 \\ 253 \end{bmatrix} \bmod 26 = \begin{bmatrix} 5 \\ 19 \end{bmatrix}$

C.T = F T

$C_5 = KP \bmod 26$ MP

$= \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \begin{bmatrix} 12 \\ 15 \end{bmatrix} \bmod 26 = \begin{bmatrix} 204 \\ 297 \end{bmatrix} \bmod 26 = \begin{bmatrix} 22 \\ 11 \end{bmatrix}$

C.T = W L

$C_6 = KP \bmod 26$ LE

$= \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \begin{bmatrix} 11 \\ 4 \end{bmatrix} \bmod 26 = \begin{bmatrix} 109 \\ 165 \end{bmatrix} \bmod 26 = \begin{bmatrix} 5 \\ 9 \end{bmatrix}$

C.T = F J

P.t = Short Example

C.t = APADJTFTWLFJ

Decryption : Assignment

Vigenere Cipher:

* Vigenere Table / Square

plain ↑	A	B	C	D	Z → key
A	A	B	C	D	Z
B	B	C	D	E	A
C	C	D	E	F	B
D	D	E	F	G	C
:	:	:	:	....	:
Z	Z	A	B	C	Y

Encryption :

P.T = geekforgeeks

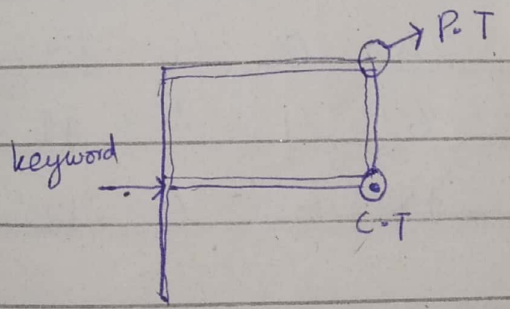
Key = xyz

x	y	z	x	y	z	x	y	z	x	y	z
G	e	e	k	F	o	r	G	e	e	k	s

Decryption

keyword ——,

C.T ——→



Keyword = UET

C.T = orbpikmmms

	U	E	T	U	E	T	U	E	T	U
=	o	r	b	p	i	k	m	m	m	s

= UNIVERSITY

Vernam Cipher

Encryption

P.T →	r	a	m	s	w	a	m	i
P.NO →	17	0	12	18	22	0	12	8
key →	r	a	n	g	e	e	l	a
K.NO →	17	0	13	6	4	4	11	0
J = P.NO + K.NO	034	0	25	24	26	4	23	8
if (J > 25)	- 26				- 26			
mod 26	8	0	25	24	0	4	23	8

C.T I A Z Y A E X I

DECRYPTION

C.T - K

8	0	25	24	0	4	23	8
- 17	0	13	6	4	4	11	0
- 9.	0	12	18	-4	0	12	8
mod 26							
17	0	12	18	22	0	12	8

R A M S W A M I

Hill Cipher Decryption

Key = $\begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix}$ det = (7)(11) − (11)(8) = 77 − 88 = −11

$\Rightarrow -11 \bmod 26 \Rightarrow 15$

$\text{Adj}\begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} = \begin{bmatrix} 11 & -8 \\ -11 & 7 \end{bmatrix}$

$K^{-1} = \frac{\begin{bmatrix} 11 & -8 \\ -11 & 7 \end{bmatrix}}{15}$

$\frac{1}{15} = 15^{-1}$

$(15)(x) \bmod 26 = 1$

$(15)(7) \bmod 26 = 1$

$105 \bmod 26 = 1$

$1 \bmod 26 = 1$

$P.T = K^{-1} C \bmod 26$

$= 7 \begin{bmatrix} 11 & 18 \\ 15 & 7 \end{bmatrix} [$

VIC Cipher:

→ Straddling Checkerboard

→ Top Row → [0–9]

→ Second Row → Popular letter in any order

ESTONIAR

	0	1	2	3	4	5	6	7	8	9
	E	T	X	A	O	N	X	R	I	S
2	B	C	D	F	G	H	J	K	L	M
6	P	Q	/	U	V	W	X	Y	Z	.

Encryption:

P.T ⇒ M A R Y Q U E E N O F

29 3 7 67 61 63 0 0 5 4 23

S C O T S

9 21 4 1 9

3 3 7 15 9 11 00 5 4 23

~~A A R~~

9 ~~21~~ 4 1 9

→ ~~D D H P J L A A F E X J V E B J~~

Step 1 → Number

Step 2 → Break 2 digits into Single digit

Step 3 → Add Key 1542 (result mod 10)

Step 4 → Pairing the result digit if their appears

2	9	3	7	6	7	6	1	6	3
1	5	4	2	1	5	4	2	1	5
3	14 mod 10	7	9	7	12	10	3	7	8
③	④	⑦	⑨	⑦	②	⓪	③	⑦	⑧
0	0	5	4	2	3	9	2	1	4
4	2	1	5	4	2	1	5	4	2
4	2	6	9	6	5	10	7	5	6
④	②	⑥	⑨	⑥	⑤	⓪	⑦	⑤	⑥

1 9

1 5

2 14

② ④

3	4	7	9	7	20	3	7	8	4	26	9	65	0	7	5	62	4
A	O	R	S	R	B	A	R	I	O	J	S	W	E	R	N	/	O

AORSRBARIOJSWERN/O

Decryption

A	O	R	S	R	B
3	4	7	9	~~20~~ 7	~~0~~ 20
-1	5	4	2	1	5
2	-1	3	7		

mod 10

2	9	3	7

2 | 3 | 7

M A R

A	R	I	Q	J	S	W	E	R	N
~~3~~	~~7~~	~~9~~	~~26~~ 4	26	~~9~~	65	0	~~7~~	5
4	2	1	5	4	2	1	5	4	2

1 0

62 4

Decryption

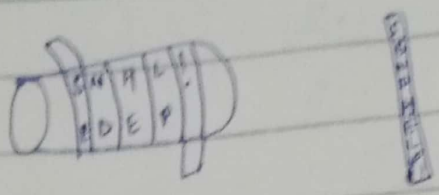
A	O	R	S	R	B	A	R	I	O
3	4	7	9	7	20	3	7	8	4
1	5	4	2	1	54	2	1	5	4
2	-1	11	11	8	74	5	8		

J	S	W	E	R	N	/	O
26	9	65	0	7	5	62	4
21	5	42	1	5	4	21	5

Transportation (Transposition) Permutation:

1- Scytale Ciphers:

P.T → send help!



C.T ⇒ SNHLIEDEP

2- Rail Fence Cipher:

Depth → 2

P.T → Meet me after class

M		E		M		A		T		R		L		S	
	E		T		E		F		E		C		A		S

C.T = MEMATRLSETEFECAS

3- Route Cipher:

key = 6

P.T ⇒ I am going to School

I	A	M	G	O	I
N	G	T	O	S	C
H	O	O	L	X	X

→ Clockwise

→ Anticlockwise

C.T ⇒ ICXXLOOHNIAMGOSOTG

③ Route cipher Decryption

↓ Insert from here

I	A	M	G	O	I
N	G	T	O	S	C
H	O	O	L	X	X

Read from here →

I am GOING TO SCHOOL xx

② Rail Fence Decryption

Depth = 2

C.T = MEMATRLSETEFECAS

2 X 16

→ Fill from left to right

M		E		M		A		T		R		L		S	
	E		T		E		F		E		C		A		S

Read zig-zag.

MEET ME AFTER CLASS

① Scytale Cipher Decryption

Every ~~second~~ fifth element write.

C.T ⇒ SNHL!EDEP

SEND HELP!

13-02-24

Number Theory

→ Division Algo:

if 'a' & 'b' → integers

$b \geq 1$

then $a = qb + r$

Modular Form

$a \equiv r \bmod b$

$r \equiv a \bmod b$

→ Divisor & GCD

integers a, b, c

$c|a$, $c|b$ → c is common divisor

GCD(a, b) → largest common divisor

→ coprime / relatively prime if their GCD is 1.

→ Congruences:-

If 'a' and 'b' are integers the 'a' is said to be congurrent to "b mod m" if $m|a-b$

m → modulus of congurence

Ex:

$24 \equiv 9 \bmod 5$ as $5 \mid 24-9$

$-8 \equiv 5 \bmod 13$ as $13 \mid -8-5$

Properties

1- $a \equiv b \bmod n$ if $n \mid a-b$

2- $a \equiv b \bmod n$ implies $b \equiv a \bmod n$

3- if $a \equiv b \bmod n$ and $b \equiv c \bmod n$ then $a \equiv c \bmod n$

1- $(a \overset{*}{\pm} b) \bmod n = [(a \bmod n) \overset{*}{\pm} (b \bmod n)] \bmod n$

$(6+8) \bmod 2$

$11^7 \bmod 13$

$= 11^{4+2+1} \bmod 13$

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

$= [(11^4 \bmod 13) \cdot (11^2 \bmod 13) \cdot (11 \bmod 13)] \bmod 13$

$= [(11^2)^2 \bmod 13 \cdot (11^2 \bmod 13) \cdot (11 \bmod 13)] \bmod 13$

$= ((4)^{2 \bmod 13} \cdot 4 \cdot 11) \bmod 13$

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

$= 132 \bmod 13 \Rightarrow 2$

Multiplicative inverse

Let $a \in Z_n$ then $\bar{a}' \bmod n$ is an integer $x \in n$

$a \cdot x \bmod n = 1 \bmod n$ (iff $\gcd(a,n) =$

$a \in Z_n$ is invertable

Calculating Multiplicative Inverse:

Euclidean Algorithm

If "a" and "b" are positive integers with $a > b$ then

$GCD(a, b) = GCD(b, a \bmod b)$

→ Calculate GCD of 4864 & 3458

$4864 = 1 \cdot 3458 + 1406$

$3458 = 2 \cdot 1406 + 646$ ✓

$1406 = 2 \cdot 646 + 114$ ✓

$646 = 5 \cdot 114 + 76$ ✓

$114 = 1 \cdot 76 + 38$

$76 = 2 \cdot 38 + 0$

$GCD = 38$

Extended Euclidean Algorithm

$$ax + by = d$$

$$4864(x) + 3458(y) = 38$$

$$38 = 114 \cdot 1 - 76 \cdot 1$$

$$38 = 114 \cdot 1 - [646 \cdot 1 - 114 \cdot 5] \cdot 1$$

$$= 114 \cdot 1 - 646 \cdot 1 + 114 \cdot 5$$

$$= 114 \cdot 6 - 646 \cdot 1$$

$$= [1406 - 646 \cdot 2] \cdot 6 - 646 \cdot 1$$

$$= 1406 \cdot 6 - 646 \cdot 12 - 646 \cdot 1$$

$$= 1406 \cdot 6 - 646 \cdot 13$$

$$= 1406 \cdot 6 - [3458 - 1406 \cdot 2] \cdot 13$$

$$= 1406 \cdot 6 - 3458 \cdot 13 + 1406 \cdot 26$$

$$= 1406 \cdot 32 - 3458 \cdot 13$$

$$= (4864 - 3458) \cdot 32 - 3458 \cdot 13$$

$$= 4864 \cdot 32 - 3458 \cdot 32 - 3458 \cdot 13$$

$$= 4864 \cdot 32 - 3458 \cdot 45$$

$$x = 32 \qquad y = -45$$

GCD(1025, 35)

1025 = 35·29 + 10

35 = 10·3 + 5

10 = 5·2 + 0

5 = GCD

45x + 130y = 5

G.CD =

130 = 45·2 + 40

45 = 40·1 + 5

40 = 5·8 + 0

GCD = 5

~~5 = 40 - 5·8~~

5 = 45 - 40·1

5 = 45 - (130 - 45·2)·1

5 = 45 - 130·1 + 45·2

5 = 45·3 + 130·(-1)

x = 3

y = -1

$513(x) + 144(y) = 9$

G.C.D

$513 = 144 \cdot 3 + 81$

$144 = 81 \cdot 1 + 63$

$81 = 63 \cdot 1 + 18$

$63 = 18 \cdot 3 + 9$

$18 = 9 \cdot 2 + 0$

G.C.D = 9

Extended Eucledean

$9 = 63 - 18 \cdot 3$

$9 = 63 - (81 - 63) \cdot 3$

$9 = 63 - 81 \cdot 3 + 63 \cdot 3$

$9 = 63 \cdot 4 - 81 \cdot 3$

$9 = (144 - 81 \cdot 1) \cdot 4 - 81 \cdot 3$

$9 = 144 \cdot 4 - 81 \cdot 4 - 81 \cdot 3$

$9 = 144 \cdot 4 - 81 \cdot 7$

$9 = 144 \cdot 4 - (513 - 144 \cdot 3) \cdot 7$

$9 = 144 \cdot 4 - 513 \cdot 7 + 144 \cdot 21$

$9 = -513 \cdot 7 + 144 \cdot 25$

$9 = 513 \cdot (-7) + 144 \cdot 25$

~~$x = 8$~~ $x = -7$

~~$y = 29$~~ $y = 25$

Affine Cipher:

→ Mono-Alphabetic substitution cipher.
→ Each letter encrypts to one letter and back again.
→ Working in mod 'm' → length of alphabets used
→ letters are mapped to integers in the range of [0-(m-1)].
→ key consist of two numbers 'a' and 'b'.
→ For 26 alphabets 'a' must be relatively prime to 'm'.

Encryption:

$C = (ap + b) \bmod m$

$b \rightarrow 1 \leq b \leq m$

$a \rightarrow 1 \leq a \leq m$,

$\gcd(a, m) = 1$ → to find multiplicative Inverse in decryption

Decryption:

$P = a^{-1}(C - b) \bmod m$

msg = I am a secret

m = 26

a = 15

b = 7

Encryption

$C = (ap + b) \bmod m$

$I = (15 \cdot 8 + 7) \bmod 26$

$= 120 + 7 \bmod 26$

$= 127 \bmod 26$

$= 23 \Rightarrow X$

$A = (15 \cdot 0 + 7) \bmod 26$

$= 7 \bmod 26$

$= 7 = H$

$M = (15 \cdot 12 + 7) \bmod 26$

$= 187 \bmod 26$

$= 53 \bmod 26$

$= 5 \Rightarrow F$

$S = (15 \cdot 18 + 7) \bmod 26$

$= 277 \bmod 26$

$= 17 \bmod 26$

$= R$

E = (15.4 + 7) mod 26

= 67 mod 26

= 15 mod 26

= 15 ⇒ P

C = (15.2 + 7) mod 26

= 37 mod 26

= 11 ⇒ L

R = (15.17 + 7) mod 26

= (255 + 7) mod 26

= 262 mod 26

= 2 ⇒ C

T = (15.19 + 7) mod 26

= (285 + 7) mod 26

= 292 mod 26

= 6 ⇒ G

XHFHRPLCPG

Decryption

$15^{-1} \bmod 26$

$\Rightarrow 15 \cdot x = 1 \bmod 26$

$\Rightarrow 26 = 15 \cdot 1 + 11$

$15 = 11 + 4$

$11 = 4 \cdot 2 + 3$

$4 = 3 + 1$

$3 = 1 \cdot 3 + 0$

G.C.D = 1

$1 = 4 - 3$

$= 4 - (11 - 4 \cdot 2)$

$= 4 - 11 \cdot 1 + 4 \cdot 2$

A

$= 4 \cdot 3 - 11 \cdot 1$

$= (15-11) \cdot 3 - 11 \cdot 1$

$= 15 \cdot 3 - 11 \cdot 3 - 11 \cdot 1$

$= 15 \cdot 3 - 11 \cdot 4$

$= 15 \cdot 3 - (26-15) \cdot 4$

$= 15 \cdot 3 - 26 \cdot 4 + 15 \cdot 4$

$= 15 \cdot 7 - 26 \cdot 4$

$\rightarrow$ $1 \bmod 26 = 15 \cdot 7 \bmod 26 - 26 \cdot 4 \bmod 26$

$1 = 15 \cdot 7 \bmod 26 = 0$

$x = 7$

$\rightarrow$ $15^{-1} \bmod 26 = 7$

$\rightarrow$

$P = a^{-1}(c-b) \bmod m$

$P_X = 7(23-7) \bmod 26$

E $= 112 \bmod 26$

$= 8 \bmod 26$

$= 8 \Rightarrow I$

$P_H = 7(7-7) \bmod 26$

$= 0 \bmod 26 \Rightarrow A$

$P_F = 7(5-7) \bmod 26$

$= -14 \bmod 26$

$= 12 \Rightarrow M$

$P_R = 7(17-7) \bmod 26$

$= 70 \bmod 26$

$= 18 \Rightarrow S$

$P_P = 7(15-7) \bmod 26$

$= 56 \bmod 26$

$= 4 \Rightarrow E$

$P_L = 7(11-7) \bmod 26$

$= 28 \bmod 26$

$= 2 \Rightarrow C$

$P_C = 7(2-7) \bmod 26$

$= -35 \bmod 26$

$= -9 \bmod 26$

$= 17 \Rightarrow R$

$P_Q = 7(6-7) \bmod 26$

$= 7(-1) \bmod 26$

$= -7 \bmod 26$

$= 19 \Rightarrow T$

Plain text:

I AM SECRET

$13^{-1} \bmod 15$

$13 \cdot x \bmod 15 = 1 \bmod 15$

$15 = 13 + 2$

$13 = 2 \cdot 6 + 1$

$2 = 1 \cdot 2 + 0$

G.C.D = 1

$1 = 13 - 2 \cdot 6$

$1 = 13 - (15 - 13) \cdot 6$

$1 = 13 + 13 \cdot 6 - 15 \cdot 6$

$1 = 13 \cdot 7 - 15 \cdot 6$

$1 \bmod 15 = 13 \cdot 7 \bmod 15 - 15 \cdot 6 \bmod 15$

$1 \bmod 15 = (7) \cdot 13 \bmod 15 - 0$

$13 \cdot x \bmod 15$

$13 \cdot 7 \bmod 15$

$x = 7$

$13^{-1} \bmod 15 = 7$

Crypto - Dimensions

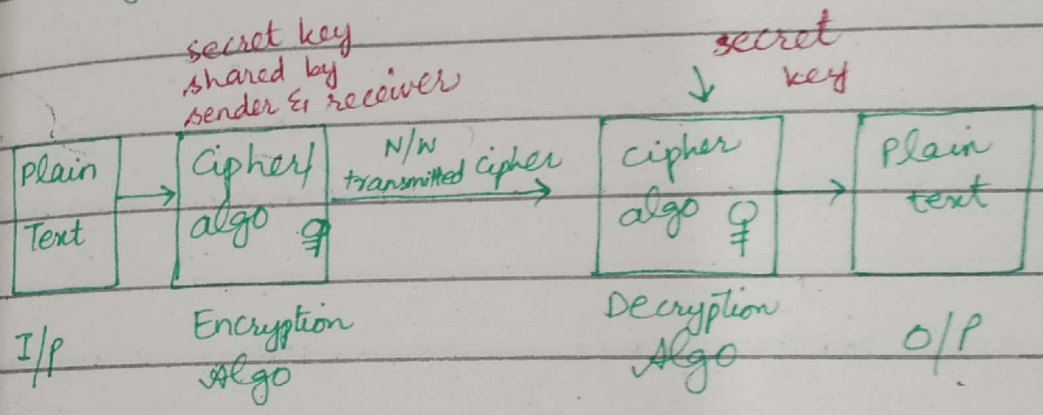
→ Types of Operation
- i- Substitution
- ii- Transposition

→ Number of keys
- i- Symmetric key
- ii- Asymmetric key

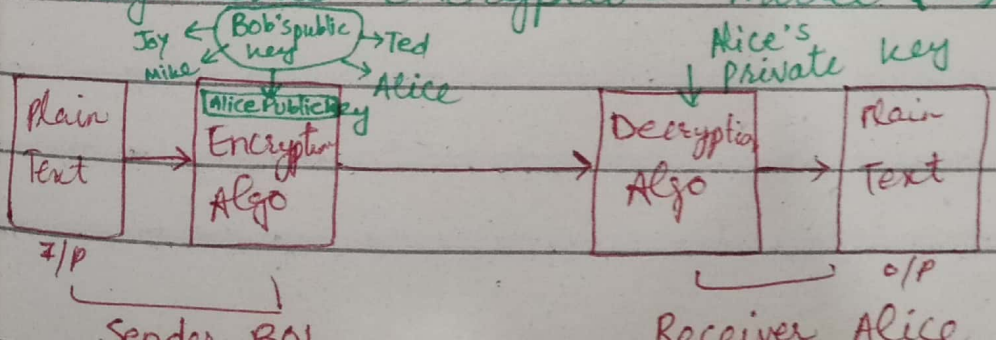
→ Processing ways
- i- Block Cipher
- ii- Stream Cipher

Basic Encryption Models:

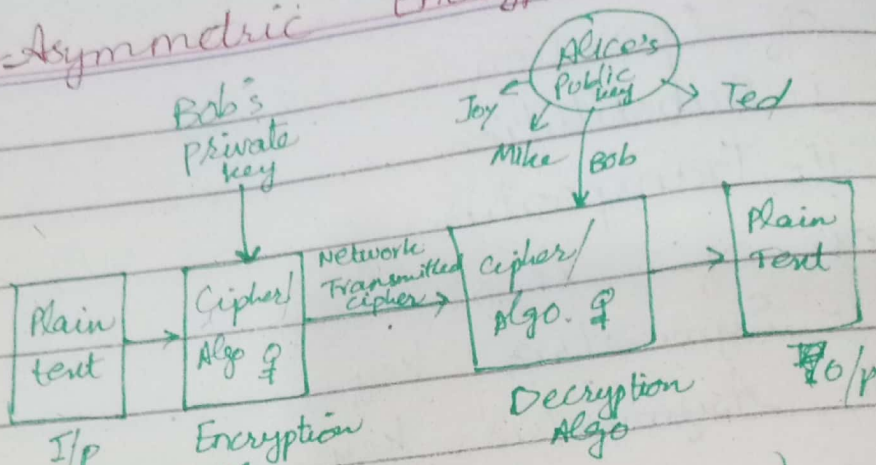
1- Symmetric Encryption Model:



2- Asymmetric Encryption Model (1):



Asymmetric Encryption Model (2)

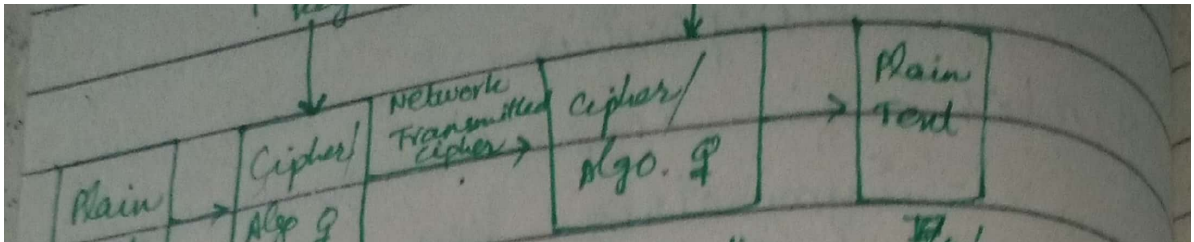


Bob sender

Alice Receiver

→ Confidentiality ⇒ Received by valid receiver

→ Authenticity ⇒ From valid sender



Bob sender

Alice Receiver

→ Confidentiality ⇒ Received by valid receiver

→ Authenticity ⇒ From Valid Sender

20-02-2024

Secure Symmetric Encryption:

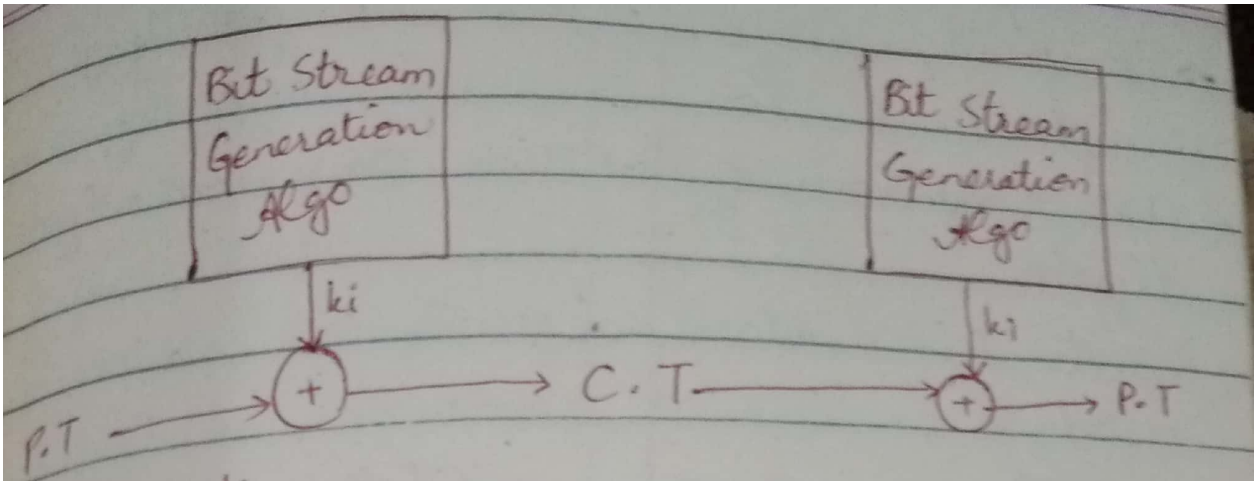
1. Strong Encryption Algo
2. Secret Key

Cryptanalytic Attacks:

1. ~~Cypher~~/Cipher text only
2. Known plain text
3. Select plain text
4. Choosen Cipher text
5. Choosen text

unconditional Security (Can not break encrypted text w

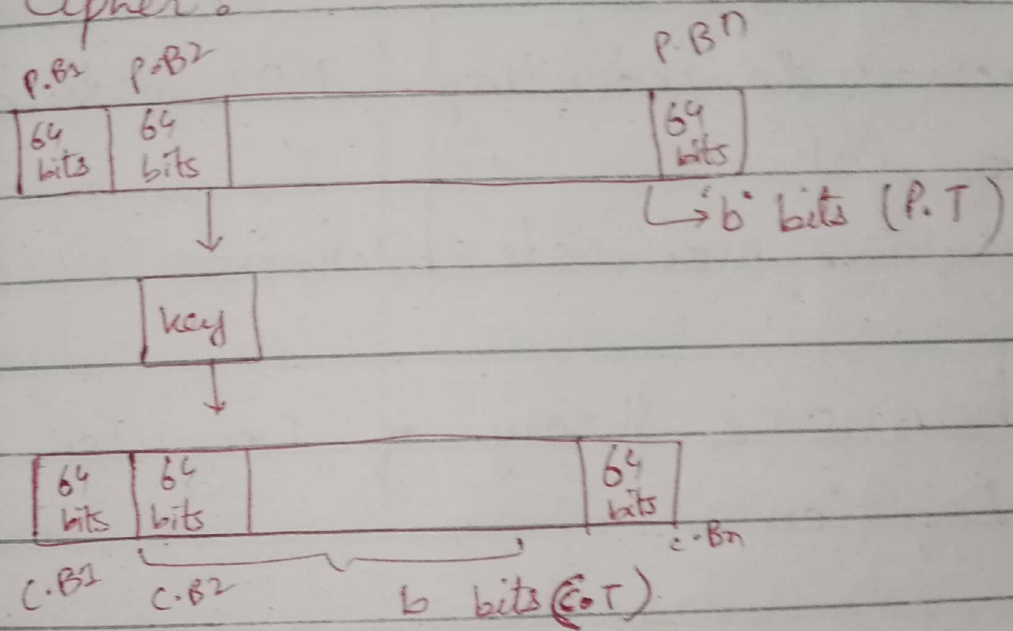
Computational Security (



Encryption :

msg	→ 1011	0110
key	→ 0101	0101
C.T	→ 1110	0011

Block Cipher :



Block Cipher :	Stream Cipher
→ P.T is grouped in blocks & then converted to C.T	→ 1 bit / 1 byte of P.T is converted into C.T
→ uses 64 or more bits	→ 8 bits are used

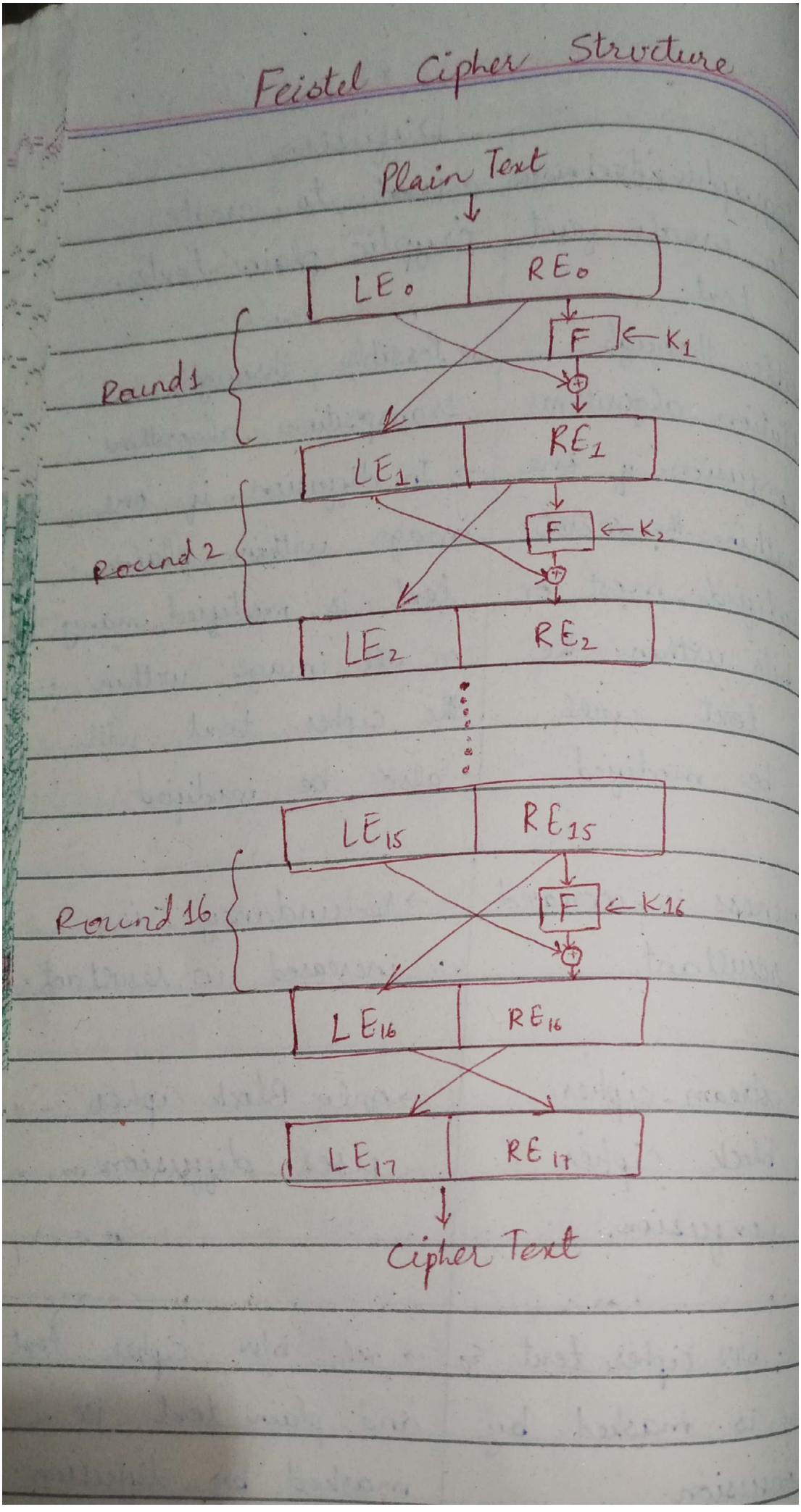
Block Cipher	Stream Cipher
→ Complexity is simple.	→ More Complex
→ Uses Confusion & diffusion	→ Uses Confusion o
→ algorithmic modes used: • ECB • CBC	→ algorithmic modes used: • CFB • OFB
→ uses transposition	→ uses substitution
→ Slower than stream cipher	→ faster
→ Increases the redundancy of P.T	→ NO redundancy
→ requires more code	→ requires less code

Shannon's theory of Confusion & Diffusion

* Diffusion → Hide the relationship b/w C.T and P.T
* Confusion → Hides the relationship b/w C.T and key

Confusion	Diffusion
cryptographic technique ed to create faint ipher text.	→ used to create cryptic plain texts.
possible through ubstitution algorithms	→ Possible through transposition algorithms
In confusion, if one t within the secret modified, most or ll bits within the ipher text will lso be modified	→ In diffusion, if one image within plain text is modified, many or all image within the cipher text will also be modified
Vagueness is increased in resultant	→ redundancy is increased in resultant.
Both stream cipher and block cipher use confusion.	→ only Block cipher uses diffusion
rel. b/w cipher text & ey is masked by confusion.	→ rel. b/w cipher text and plain text is masked by diffusion.

Feistel Cipher Structure



Block Cipher Design Principles:

- Block Size (64 bits)
- Key Size
- No. of rounds (choose optimal no.) 16
- No. of subkey
- Round Function
- Plain text divided into 2 halves.

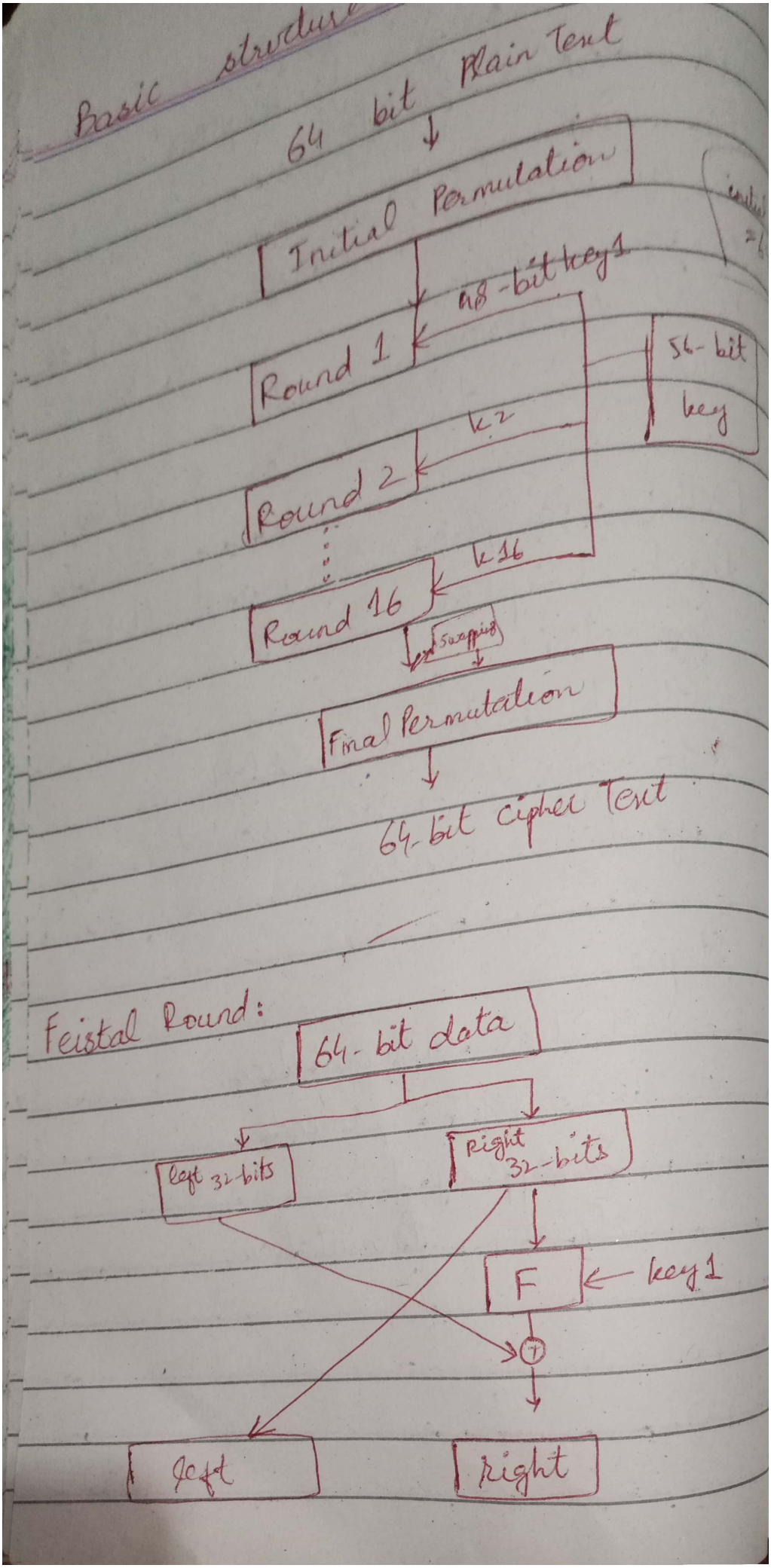
Data Encryption Standard (DES)

- Block Cipher
- Symmetric
- 64-bit Plain text block
- 16 rounds → each round is a feistal round.

4 Steps:

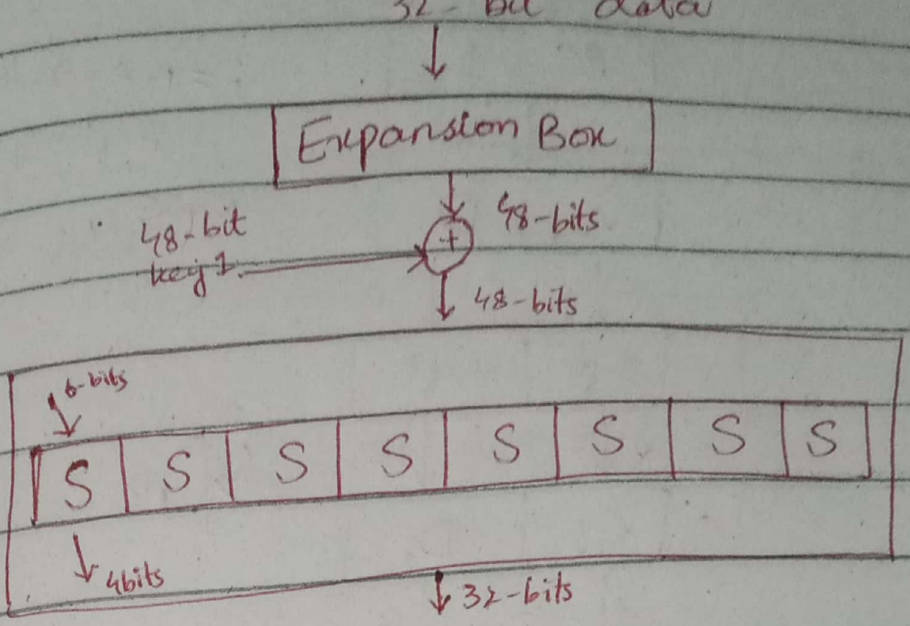
Initial Permutation
16 - feistal rounds
Swapping
Final Permutation

Basic structure



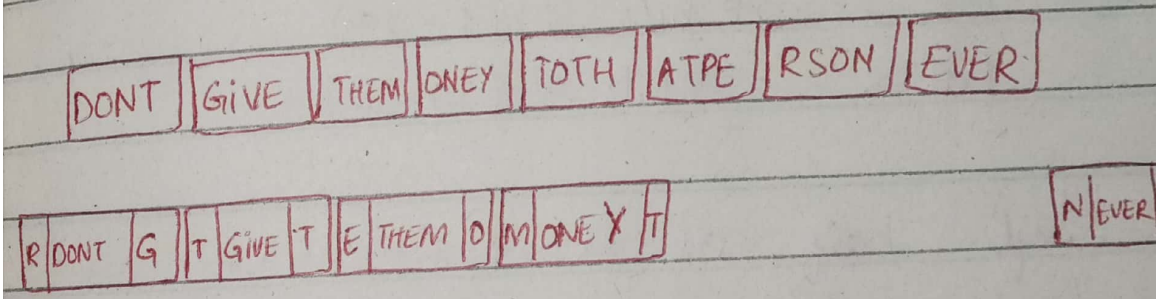
Feistal Round:

Round Function:



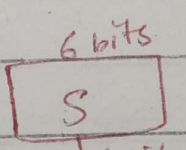
Expansion Box:

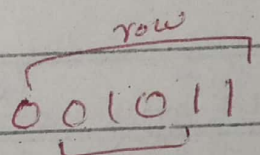
data ⇒ don't give the money to that person ever.

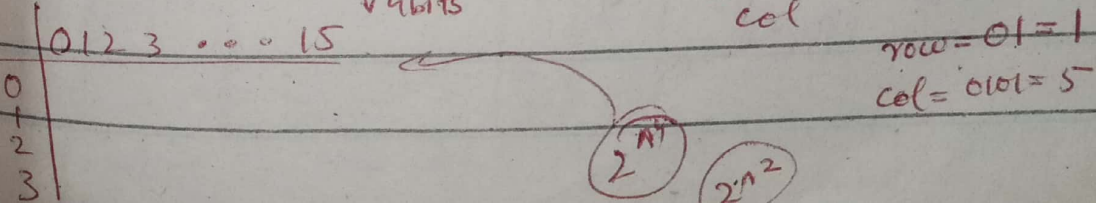


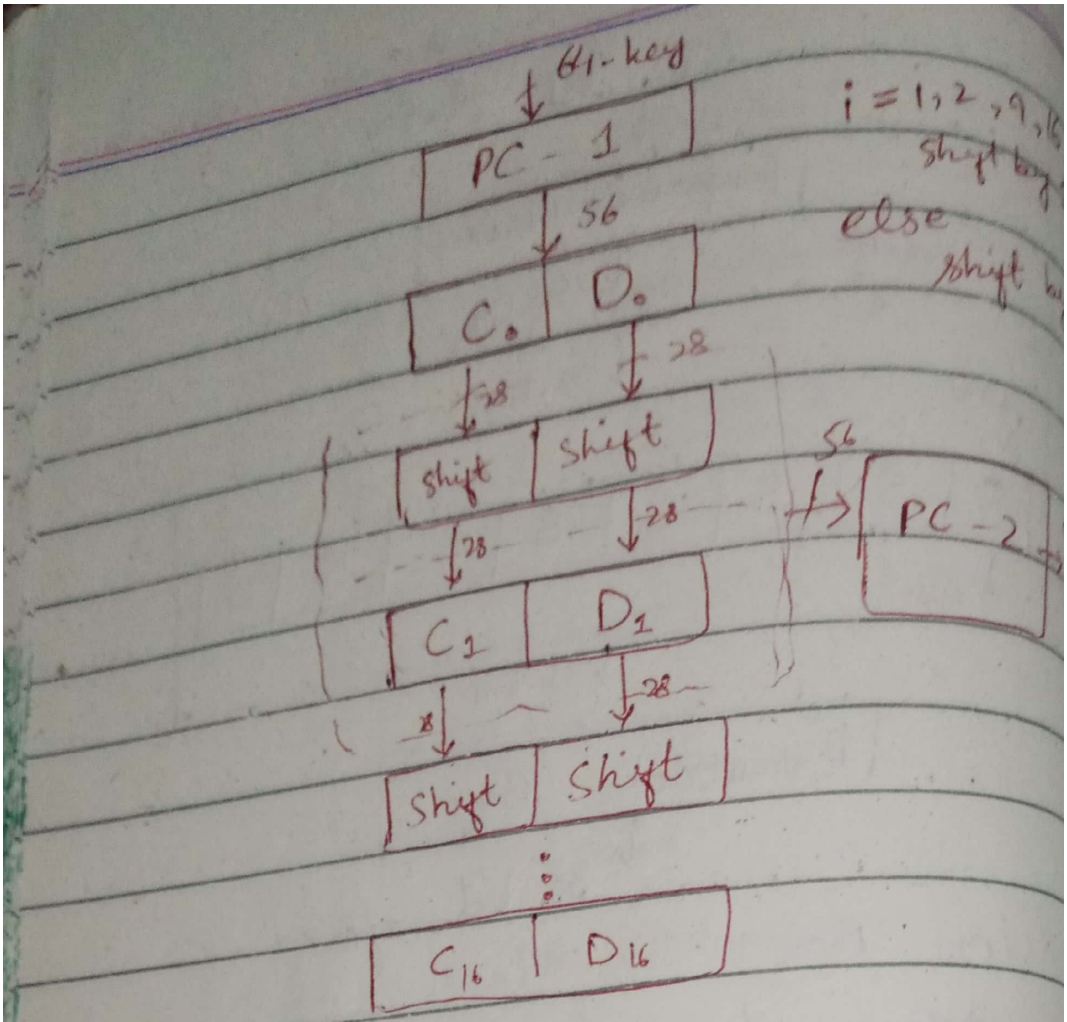
8x6 = 48

S-Box:









PC - 2 :-

56 → 48

C_1 → 28 bits → (1 - 28)

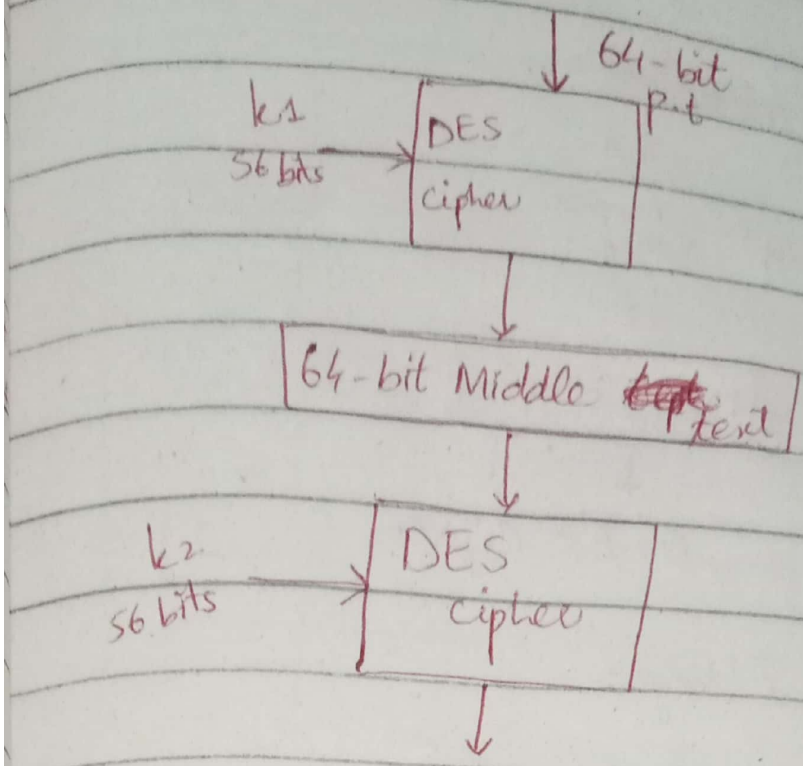
D_1 → 28 bits → (29 - 56)

left half C1 → 9, 8, 22, 25

right half C2 → 35, 38, 43, 54

Effective key length ⇒ 56_{C_2}

1- Double DES (2DES).



Encryption:

$$C.T = E(K_2, E(k_1, P))$$

Decryption:

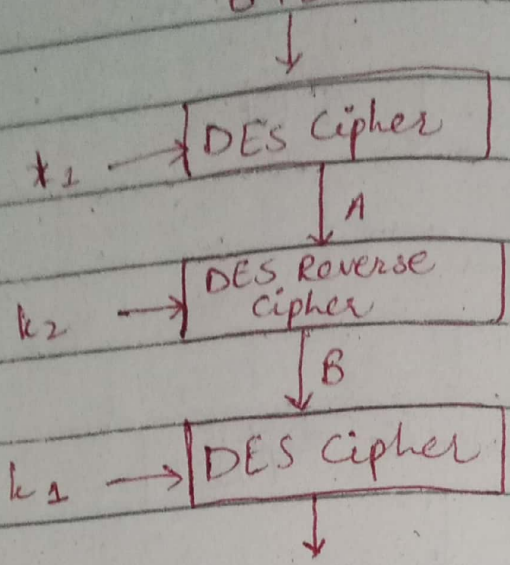
$$P.T = D(K_1, D(k_2, C))$$

Meet in the middle attack

K1				K2		
key	P.T	Middle text		key	C.T	Middle text
1				1		
2				2		
10			$k_1 = 10$	3		$k_2 = 50$
56				50		
				51		

where middle text of both table is same that will be values of k_1 and k_2.

Triple DES (3DES) using 2 keys



3DES using 3 keys:

$$C = E(k_3, D(k_2, E(k_1, P)))$$

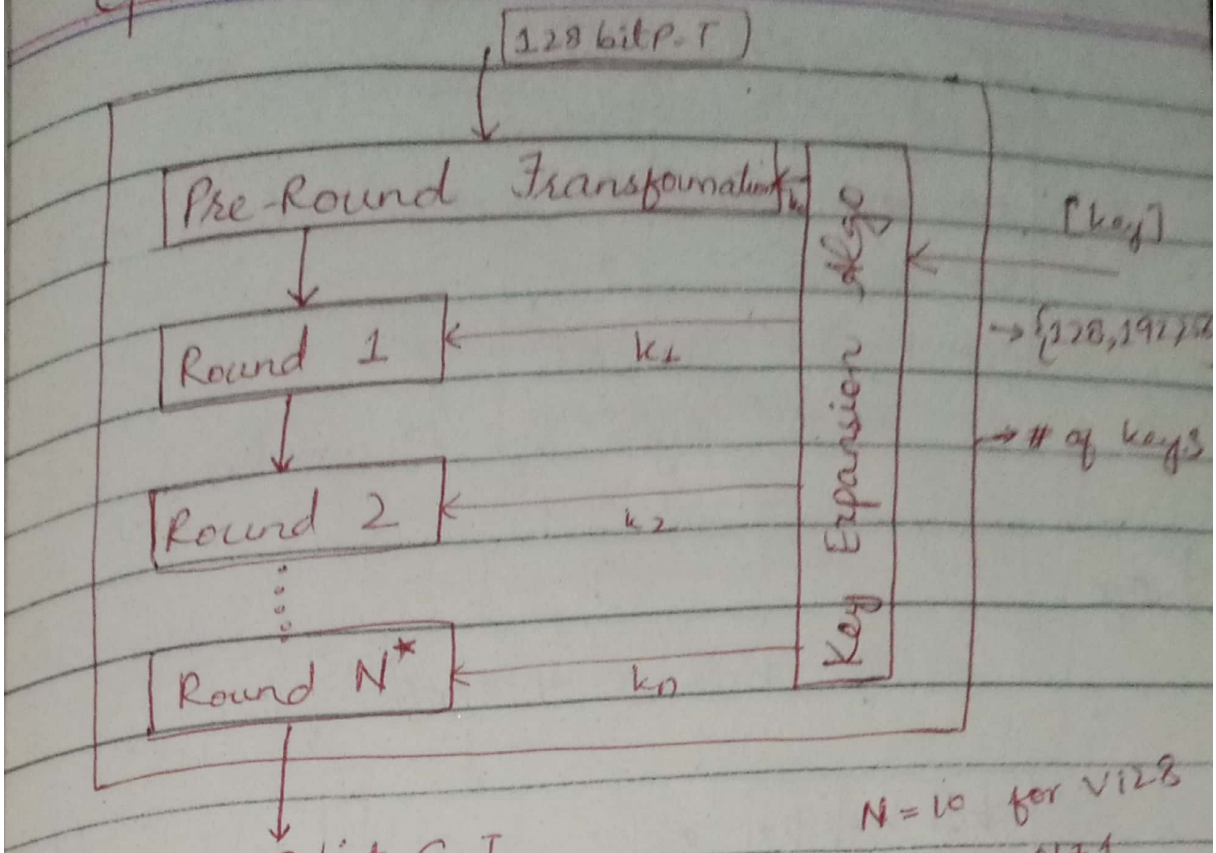
$$P = D(k_1, E(k_2, D(k_3, C)))$$

28-02-24

Advanced Encryption Standard (AES):

	Rounds	No. of bits in key
version 128	10	128
version 192	12	192
version 256	14	256

General Structure :



N = 10 for Vi128
keys = N+1

1 B = 8 bits

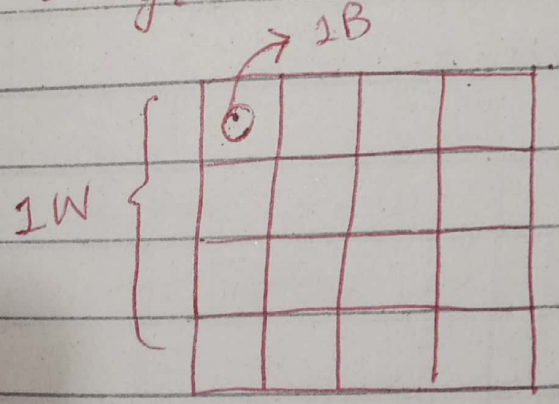
1 W = 4B = 32 bits

(State-Array) State = [4x4] matrix

~~Array~~ = 16 Bytes = 128 bits

Input Array:

W = Word



4x4 = 16B = 128 bits

State Array:

W_0	W_1	W_2	W_3
$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

→ $[W_0 W_1 W_2 W_3]$

↳ 3rd byte of 1st word

Key:

128 bits = 4 words

k_0	k_4	k_8	k_{12}
k_1	k_5	k_9	k_{13}
k_2	k_6	k_{10}	k_{14}
k_3	k_7	k_{11}	k_{15}

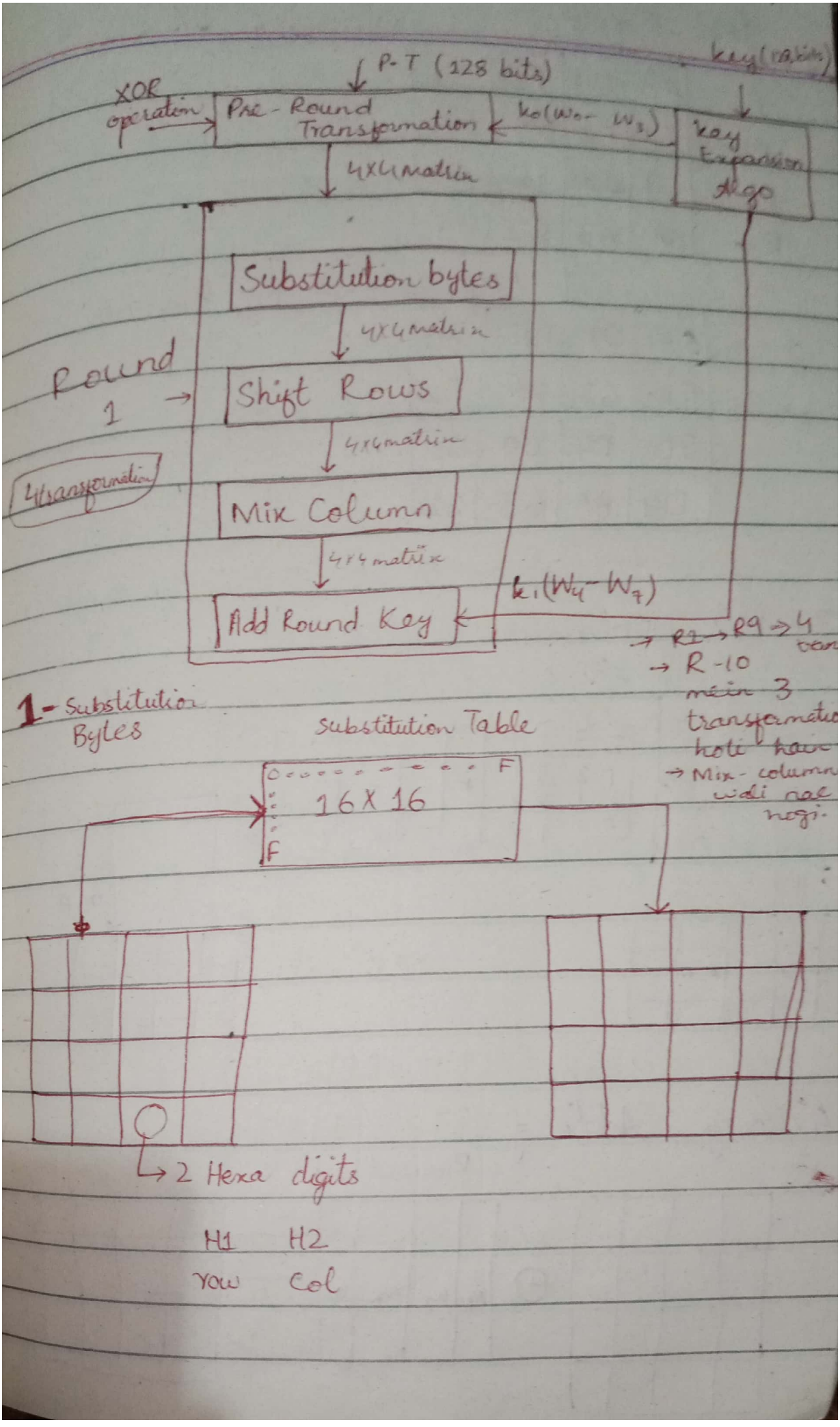
Key Expansion Algo →

44 words

→ 11 keys generated

⇒

Round Structure:


P.T (128 bits)
Key (128 bits)
XOR operation
Pre-Round Transformation
k0(W0 - W3)
Key Expansion algo
4x4 matrix
Substitution bytes
4x4 matrix
Round 1
Shift Rows
4x4 matrix
4 transformation
Mix Column
4x4 matrix
Add Round Key
k1(W4 - W7)
→ R1 → R9 → 4 con
→ R-10
mein 3 transformatio hoti hain
→ Mix-column wali nae hogi.
1- Substitution Bytes
Substitution Table
0 ... F
16 X 16
F
2 Hexa digits
H1 H2
row Col

2- Shift

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 no

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

3- Mix Column:

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}_{4\times4} * \begin{bmatrix} \quad \end{bmatrix}_{4\times1} = \begin{bmatrix} \quad \end{bmatrix}_{4\times1}$$

I/P

O/P

4- Key Adding

Round key

W_1 W_2 W_3 W_4

05-03-24

RC4

1- Key Sch

2- Key stre

3- Encryption

S[i] =

T[i]

S = [0,

key array = [

P.T. →

T [1

1 - Key

No. of

for i

do

j

S

2 - Key

RC4 Stream Cipher

1- Key Scheduling
2- Key Stream Generation
3- Encryption and Decryption

S[i] = State vector 0-255
T[i] = key vector / Temporary Array

S = [0, 1 2 3 4 5 6 7]
key array = [1 2 3 6]
P.T. → [1 2 2 2]
T [1 2 3 6 1 2 3 6]

1- Key Scheduling
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])

2- Key Stream Generation
No. of iterations = Size of key
i, j = 0

$i = (i+1) \bmod 256$

$j = (j + S[i]) \bmod 256$

Swap $[S(i), S(j)]$

$t = (S[i] + S[j]) \bmod 256$

$ki = S[t];$

3. Encryption

Encryption → P.T ⊕ New key

06-03-24

Eular's Toitent Function
(Eular Phi function)

→ $\phi(n)$

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

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
GCD(4,5) = 1

$\phi(6) = ?$

P1:

if 'n' is prime then

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

P2:

$$\phi(a * b) = \phi(a) * \phi(b)$$

P3:

$$\phi(p^n) = p^n - p^{n-1}$$

Eular's Totient Theorem:

if 'x' and 'n' are positive coprime integers then

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

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

Ex:

$x = 11$, $n = 10$

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

$$\therefore \phi(10) = \phi(2) * \phi(5)$$

$$= 1 * 4 = 4$$

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

$$1461 = 1 \bmod 10$$

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

Ex $11^{4*2} = 1 \bmod 10$

$214358881 \equiv 1 \bmod 10$

Ex. $11^{40} = 1 \bmod 10$

Ex. $4^{99} \bmod 35$

$x = 4$, $n = 35$ → coprime

By Eular's Theorem

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

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

$= 6 * 4 = 24$

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

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

$= (4^{24})^4 \bmod 35 \cdot 4^3 \bmod 35$

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

$= 64 \bmod 35$

$= 29$

Fermat's

→ Specific case of

→ If 'n' is prime and 'x' is +ve integer not divisible by 'n' then

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

Ex:

$x = 3, \quad n = 5$

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

$$3^4 \equiv 1 \bmod 5$$

$$81 = 1 \bmod 5$$

Another way

$$x^n \equiv x \bmod n$$

$$3^5 = 3 \bmod 5$$

$$243 = 3 \bmod 5$$

$\because 243 \% 5 = 3$

Ex.

$$4^{532} \bmod 11$$

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

$x = 4, \quad n = 11$

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

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

$4^{53} =$

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

$\Rightarrow 1 \bmod 11 \cdot 4^2 \bmod 11$

$\Rightarrow 16 \bmod 11$

$= 5$

RSA algo

→ Rivest - Shamir - Adleman → 1978

→ asymmetric (2 keys)

1- Key Generation:

i- Select 2 large prime numbers p, q.

ii. $n = p * q$

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

iv. Choose value of 'e'

$1 < e < \phi(n)$

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

v- Calculate

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

i.e

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

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

vi- Public key $\{e, n\}$

vii- Private key

2. Encryption:

C =

3. Decryptio

M

P = 3 ,

→ n = p

→ $\phi(n)$ =

Let

as

GC

→ d

de

7 X

7d

d =

vii- Private key {d, n}

2. Encryption:

$$C = M^e \bmod n \qquad (M < n)$$

3. Decryption:

$$M = C^d \bmod n$$

$P = 3$, $q = 11$

→ $n = P * q = 3 \times 11 = 33$

→ $\phi(n) = (P-1)(q-1) \Rightarrow (3-1)(11-1) = 2 \times 10 = 20$

Let $e = 7$

as $1 < 7 < 20$

$GCD(7, 20) = 1$

→ $d \equiv e^{-1} \bmod \phi(n)$

$de = 1 \bmod \phi(n)$

$7 \times d = 1 \bmod 20$

$7d \bmod 20 = 1$

d → multiplicative inverse of 7 = 3

Public key = $\{e, n\} = \{7, 33\}$

Private key = $\{d, n\} = \{3, 33\}$

Encryption:

Let $m = 31$

Then

$C = 31^7 \bmod 33$

$= 4$

Decryption:

$M = C^d \bmod n$

$M = 4^3 \bmod 33$

$M = 31$

$3^{302} \bmod 13$

$x = 3$ and $n = 13$ are coprime

By Euler's theorem

$$3^{\phi(13)} = 1 \bmod 13$$

$$\phi(13) = 12$$

$$3^{12} = 1 \bmod 13$$

$$3^{302} \bmod 13 \Rightarrow 3^{(12)25+2} \bmod 13$$

$$\Rightarrow 3^{(12)25} \bmod 13 \cdot 3^2 \bmod 13$$

$$= 1 \cdot 3^2 \bmod 13$$

$$= 9 \bmod 13$$

$$= 0$$