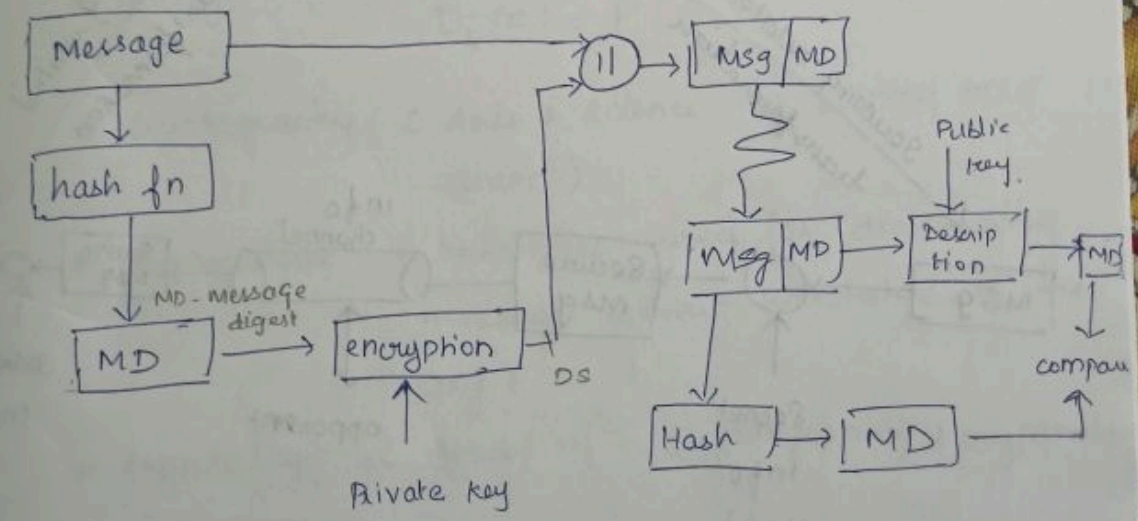
Security Mechanism

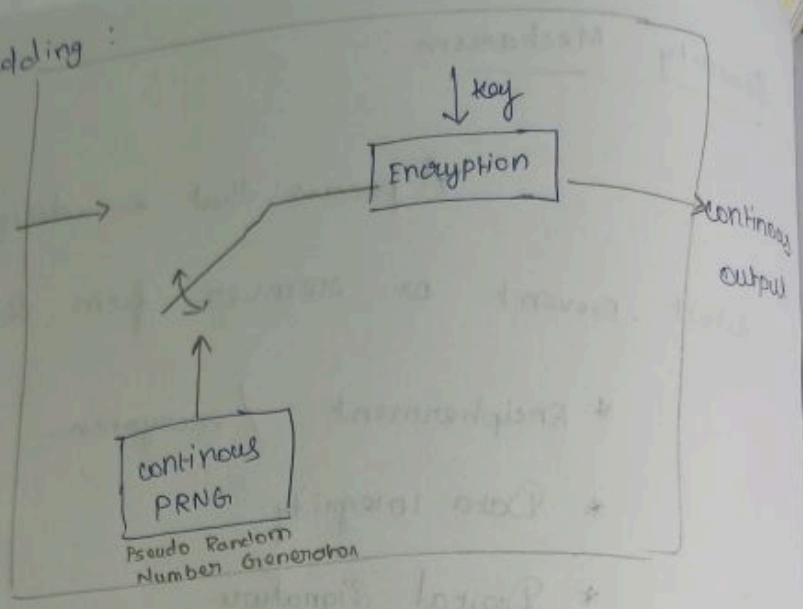
A process that is designed to detect, prevent or recover from security attack.

* Encipherment / encryption.
* Data Integrity
* Digital Signature
* Access control
* Traffic padding.

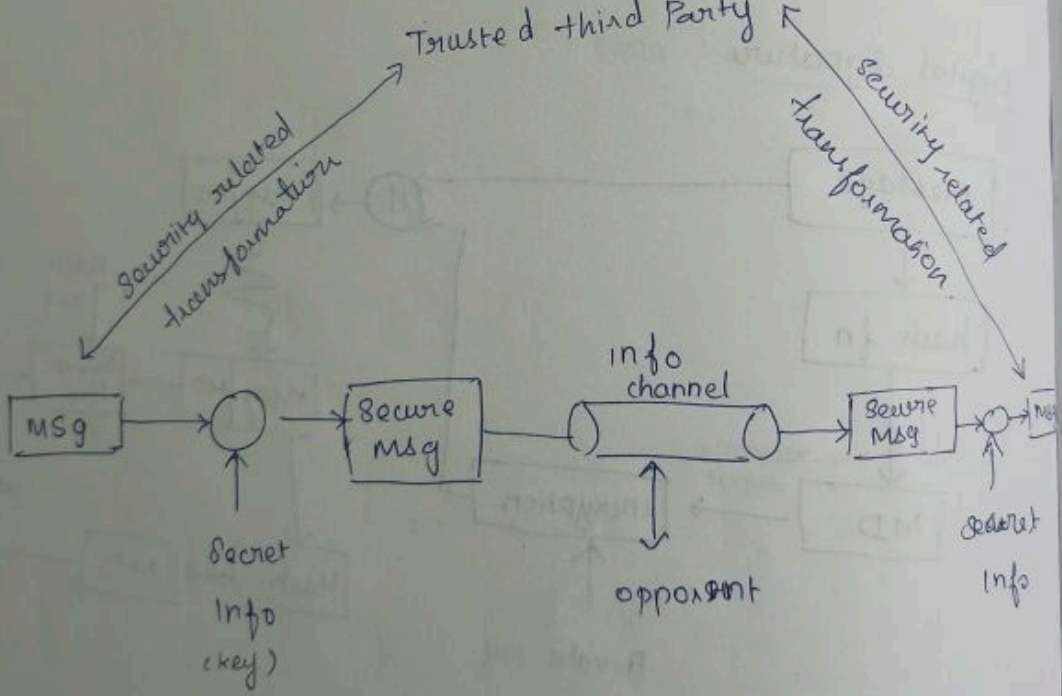
Digital Signature : (DS)



Traffic Padding :



Model for N/w security :



A tasks :

1. Design a
2. Generate
3. Develop me
   information
4. Specify H

Terms :

* plain te
* cipher te
* encrypti
* decrypti
* cryptog
* cryptan
* crypto

4 tasks:

1. Design a suitable strong encryption algorithm.
2. Generate the secret information (key)
3. Develop methods to share the security related information.
4. Specify the protocol for communication.

Terms:

* plain text (original message)
* cipher text (scrambled message / encrypted msg)
* encryption $E_k(P) = C$
* decryption. $D_k(C) = P$
* Cryptography (Arts & science of keeping msg secure)
* cryptanalysis (techniques used for deciphering message without knowledge of the key)
* cryptology (study of cryptography + cryptanalysis)

Cryptosystem

Symmetric key crypto system

→ private key / secret key / conventional cryptography

→ same key / single key.
↳ private / secret key

→ faster

→ confidentiality

Asymmetric key crypto system.

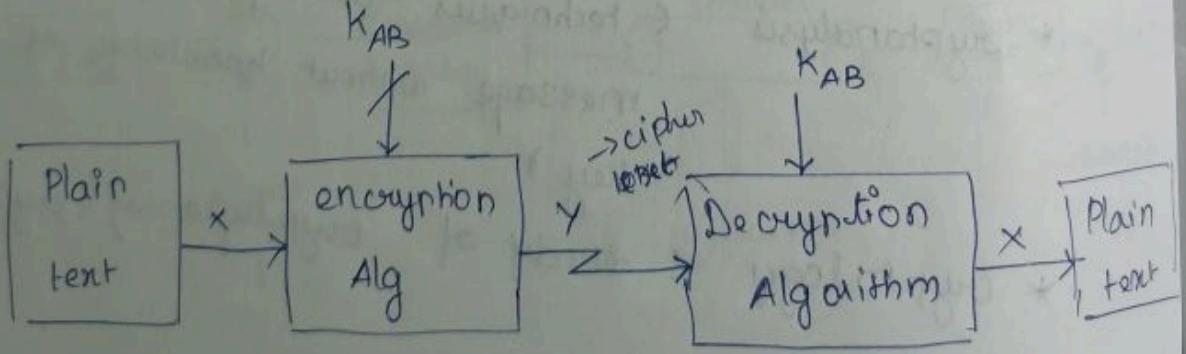
→ public key cryptography

→ a different key.
↳ 1. private key
↳ 2. public key.

→ slower.

→ confidentiality and Authentication.

Symmetric key cryptography:



5 Ingredients

① plain text
② encryption
③ decryption
④ cipher text
⑤ private key / secret key.

& Requirements of conventional cryptography System

① Need strong encryption Algorithm.
② key must be kept secret.

Symmentric key cryptography:

3 dimensions:

① type of operation used for converting PT into CT → ① Substitution technique ② transposition techniq
② No. of keys used → Block cipher, stream cipher
③ the way in which the plain text is pronounced.

Substitution technique:

In substitution technique, each character is replaced or mapped into another character.

transposition technique:

In this the position of the character is interchanged.

No. of. users	No. of. keys
2	1
3	3
4	6
5	10
⋮	⋮
N	$\frac{N(N-1)}{2}$

Block ciphers:

faster More than one byte of element @ a time

Stream cipher:

slower. process one byte / 1 bit at a time.

Substitution technique:

1. Caesar cipher
2. Monoalphabetic cipher
3. Playfair cipher
4. Hill cipher
5. Polyalphabetic cipher
6. one time pad.

Caesar cipher:

↳ developed by Julier caesar

↳ based on stream cipher.

encryption:

$$C = (P + k) \bmod 26$$

eg: P - SASTRAY

key = 4

Sol

S	A	S	T	R	A	Y
↓	↓	↓	↓	↓	↓	↓
18	0	18	19	17	0	24
+4	4	4	4	4	4	4
22	4	22	25	21	4	28 mod 26
↓	↓	↓	↓	↓	↓	↓
W	E	W	Z	V	E	C

∴ C = WEWZVEC

* Brute force attacked
* key possibility = 26
* so easily attacked

Decryption:

$$P = (C - K) \bmod 26$$

C = NE NXVE C

				V	E	C
W	E	N	X	↓	↓	↓
↓	↓	↓	↓	21	4	2
22	4	22	23	↓	↓	↓
-4	4	4	11	11	4	4

18	0	18	19	17	0	-2
↓	↓	↓	↓	↓	↓	+26
S	A	S	T	R	A	24 mod 26
						↓
						Y

P = SASTRA Y

Monoalphabetic cipher:

↳ each character maps into different random character.

↳ based on stream cipher.

1×26

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

V	W	X	Y	Z
W	X	Y	Z	A

* here possibility = 26!

Playfair cipher:

- Is multiletter encryption cipher.
- Is process 2 character at a time
- Is based on block cipher.

eg: keyword = CIPHER

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

3 rules for encryption & decryption:

- Is two plain text letters fall in the same row of the matrix are each replaced by the letter to the right with the first element of the row circularly follow the last.
  - * RD → AF
  - * RF → AR
- Is two plain text letters fall in the same column are each replaced by the letter beneath to the top element of the column circularly following the last.
  - * PK → BQ
  - * PW → BP
- Is otherwise each plain text letter in a pair is replaced by the letter that lies in its own row and column occupyed by the other plain text letter.
  - AS → DO

eg : keyword → NETWORK

combine I & J

plain text → CRYPTOGRAPHY.

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

C R Y P T O G R A P H Y

↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓

R K X Q W N D A G X Q W

x.

* Hill cipher :

encryption

Decryptio

eg : k =

* Hill cipher:

→ Multi letter encryption cipher
→ Based on Block ciphers.

encryption:

$$C = P.K \bmod 26$$

Decryption

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

eg: $K = \begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$ PT = A B cD
0 1

$$(0 \quad 1)\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix} \bmod 26$$

$$(5 \quad 7) \bmod 26$$
F H

PT AB → FH CT

$$K^{-1} = \frac{1}{|K|} \text{adj}(K) \; ; \; \text{adj}(K) = \begin{pmatrix} 7 & -4 \\ -5 & 9 \end{pmatrix}$$

$$|K| = |63 - 20| = 43$$

$$K^{-1} = \frac{1}{|43|}\begin{pmatrix} 7 & -4 \\ -5 & 9 \end{pmatrix} \bmod 26$$

$$= \frac{1}{17}\begin{pmatrix} 7 & -4 \\ -5 & 9 \end{pmatrix} \bmod 26$$

$$\simeq 17^{-1}\begin{pmatrix} 7 & -4 \\ -5 & 9 \end{pmatrix} \bmod 26$$

Extended Euclid's Alg → multiplicative Inverse.

Extended Euclid (m, b)

1. $(A_1, A_2, A_3) \leftarrow (1, 0, m)$ $(B_1, B_2, B_3) \leftarrow (0, 1, b)$
2. If $B_3 = 0$ Return $A_3 = GCD(m, b)$, No Inverse
3. If $B_3 = 1$ Return $B_3 = GCD(m, b)$, $B_2 = b^{-1} \bmod m$
4. $Q = \left[\frac{A_3}{B_3} \right]$
5. $(T_1, T_2, T_3) \leftarrow (A_1 - QB_1, A_2 - QB_2, A_3 - QB_3)$
6. $(A_1, A_2, A_3) \leftarrow (B_1, B_2, B_3)$
7. $(B_1, B_2, B_3) \leftarrow (T_1, T_2, T_3)$
8. Goto step (2)

※ $b b^{-1} \bmod m = 1$

$7 \cdot 3 \bmod 20$

$21 \bmod 20 = 1$

$T_1 = 1 - 2 \times 0$

$T_2 = 0 - 2 \times 1$

$T_3 = 20 - 2 \times 7$

eg: extended euclid (20, 7) (m = 20, b = 7) $7^{-1} \bmod 20$

Q	A_1	A_2	A_3	B_1	B_2	B_3
-	1	0	20	0	1	7
2	0	1	7	1 ($T_1 = A_1 - QB_1$)	-2	6
1	1	-2	6	-1	3	1

3 → MI

3 is the MI of 7

extended euclid (26, 17)

Q	A_1	A_2	A_3	B_1	B_2	B_3
–	1	0	26	0	1	17
1	0	1	17	1	-1	9
1	1	-1	9	-1	2	8
1	1	-1	2	8	2	[1]
					[-3] MI	

$-3 + 26 = 23$ is MI

$$K^{-1} = 17^{-1} \begin{pmatrix} 7 & -4 \\ 5 & 9 \end{pmatrix} \bmod 26$$

$$K^{-1} = 23 \begin{pmatrix} 7 & -4 \\ -5 & 9 \end{pmatrix} \bmod 26$$

$23 \times 7 \bmod 26$
$23 \times -4 \bmod 26$
$23 \times -5 \bmod 26$
$23 \times 9 \bmod 26$

$$K^{-1} = \begin{pmatrix} 5 & 12 \\ 15 & 25 \end{pmatrix}$$

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

$$= (5\ 7) \begin{pmatrix} 5 & 12 \\ 15 & 25 \end{pmatrix} \bmod 26 = (0\ 1)$$

A B

eg: $k = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$ Ans $k^{-1} = \begin{pmatrix} 11 & 9 & 15 \\ 15 & 14 & 6 \\ 11 & 0 & 17 \end{pmatrix}$

PT = CRY

Encryption

$C = P.K \mod 26$

$= (2 \quad 17 \quad 24) \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \mod 26$

$= (1139 \quad 388 \quad 823) \mod 26$

$C = (23 \quad 24 \quad 17)$

Decryption:

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

$k^{-1} = \frac{1}{|k|} adj(k)$

$|k| = -939$

$adj(k) = \begin{pmatrix} 300 & -313 & 267 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{pmatrix}$

$$K^{-1} = \frac{1}{-989}\begin{pmatrix} 300 & -313 & 267 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{pmatrix} \bmod 26$$

$$= \frac{1}{23}\begin{pmatrix} 300 & -313 & 267 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{pmatrix} \bmod 26$$

$$= 23^{-1}\begin{pmatrix} 300 & -313 & 267 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{pmatrix} \bmod 26$$

using extended euclid's algorithm:

$23^{-1} \bmod 26$

b m

Q	A_1	A_2	A_3	B_1	B_2	B_3
	1	0	26	0	1	23
—						
1	0	1	23	1	-1	3
7	1	-1	3	-7	8	2
1	-7	8	2	8	[-9]	[1]

MI

$$\equiv -9\begin{pmatrix} 300 & -313 & 267 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{pmatrix} \bmod 26$$

$$\equiv 17\begin{pmatrix} 300 & -313 & 267 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{pmatrix} \bmod 26$$

$$k^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

$$P = (28 \quad 24 \quad 17) \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \bmod 26$$

$$= (860 \quad 615 \quad 478) \bmod 26$$

$$= (2 \quad 17 \quad 24)$$

$$\downarrow \quad \downarrow \quad \downarrow$$

$$C \quad R \quad Y$$

24/3/22

Design a cryptographic system

PT → CRYP

key → EDBB by applying hill cipher substitution technique. also perform decryption using cipher text to recover the original text.

encryption:

$$C = (P.k) \bmod 26$$

$$= \begin{pmatrix} 2 & 17 \\ 24 & 15 \end{pmatrix} \begin{pmatrix} 11 & 3 \\ 1 & 1 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 25 & 23 \\ 101 & 87 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 25 & 23 \\ 23 & 9 \end{pmatrix}$$

CRYP $\longrightarrow$ Z X H J

$$K^{-1} = \frac{1}{|K|} \{ Adj(K)$$

$$K^{-1} = \frac{1}{1} \begin{pmatrix} 1 & -3 \\ -1 & 4 \end{pmatrix}$$

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

$$= \begin{pmatrix} 25 & 23 \\ 23 & 9 \end{pmatrix} \begin{pmatrix} 1 & -3 \\ -1 & 4 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 2 & 17 \\ -2 & 15 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 2 & 17 \\ 24 & 15 \end{pmatrix}$$

$$= CRYP$$

encrypt the PT → GET WELL SOON

key → CORONA

by using playfair cipher technique.

Ans:

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

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

GET WELL SOON

↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓

B F G Y F K K T R W R A

Polyalphabetic cipher: (Vignere cipher)

→ plain text

key ↑	A	B	C	D	.....	X	Y	Z
A	A	B	C	D	.....	X	Y	Z
B	B	C	D	E	.....	Y	Z	A
C	C	D	E	F	.....	Z	A	B
D								
...								
X	X	Y	Z	A	.....			
Y	Y	Z	A	B	.....			
Z	Z	A	B	C	.....			

eg: Plain text → SAETRA

Key → SRC

S A S T R A

S R C S R C (repeat key)

---

18 0 18 19 17 0

2 18 4 2 18 4

---

20 18 22 21 35 4 mod 26

↓ ↓ ↓ ↓ ↓ ↓

20 18 22 21 9 4

↓ ↓ ↓

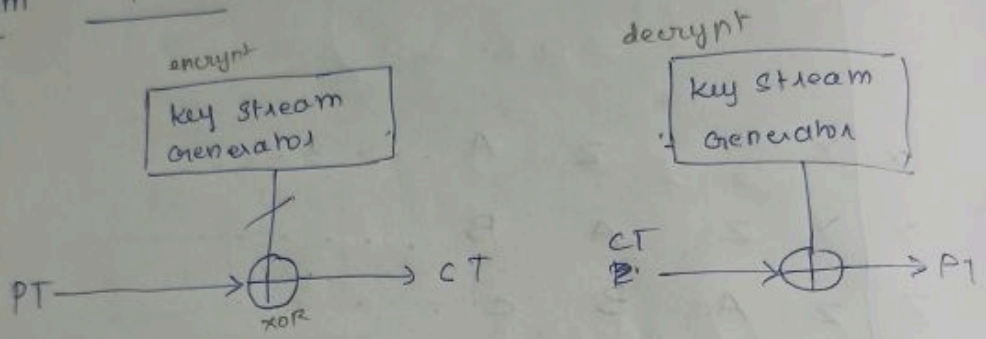
U S W

Auto key Stream Generator :

PT → S A S T R A S R C

key → C S E S A S T R A (Repeat the PT)

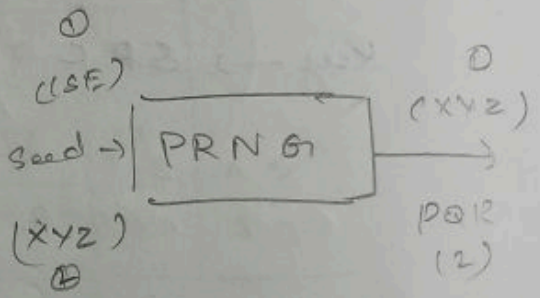
Vernam cipher :



One-time Pad :

PT : CASTIRA SRC

Key : CSEXYZ P QR



Transposition Techniques:

1. Rail fence Technique
2. single column Transposition
3. Double column transposition.

Rail fence technique:

depth = 2

PT → INFORMATION SECURITY

1 → I F R A I N E U I Y

2 → N O M T O S C R T

CT → IFRAINEUIYNOMTOSCRT

depth = 5

1 → I I

2 → N T O R T

3 → F A N U Y

4 → O M S C

5 → R E

CT → I I N T O R T F A N U Y O M S C R E

Q NO: 1 Encrypt the message "PANDEMIC IS THE WORLD WIDE SPREAD OF A NEW DISEASE" using railfence technique. depth = 3

Q NO: 2 encrypt the plaint text 15 using key 6 by appling vernam cipher

sol
1111 - 15
0110 - 6
1001 - 9

Single column transposition:

eg: encrypt
PT → NETWORK SECURITY
key → 3 1 2 3 / CSE 2

N	E	T
W	O	R
K	S	E
C	U	R
I	T	Y

filled by row
read by column

CT => EOSUTTRERYNWKCI

decrypt:

key

key^{-1}

Stream ciph

key

plaintext (Pi)

Block ciphe

key

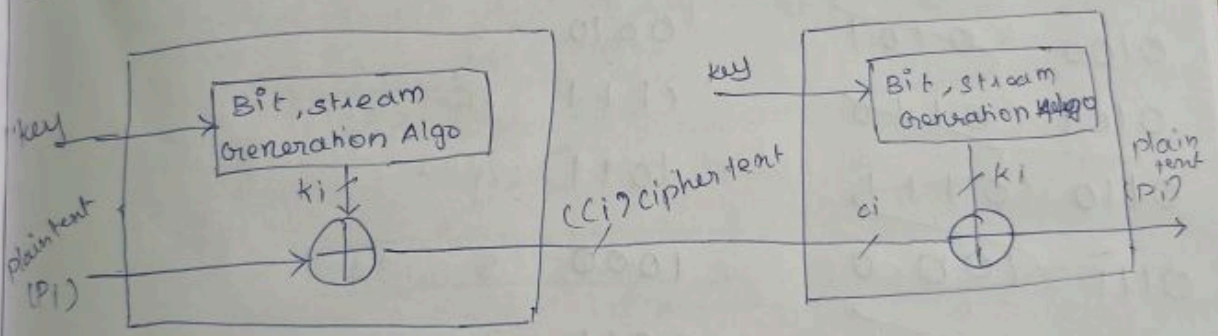
decrypt:

key → 2 1 2

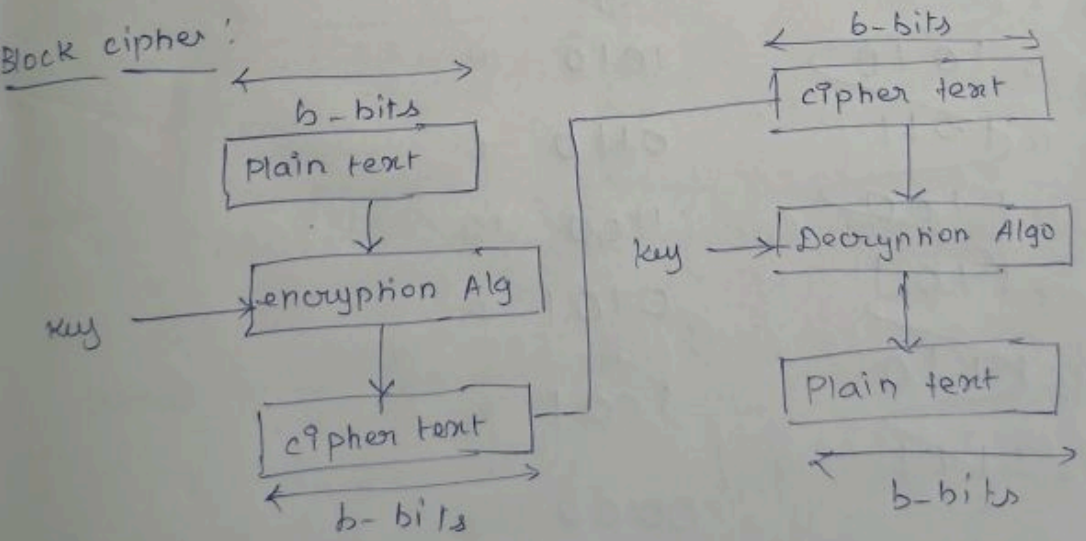
key^{-1} → 2 3 1

2	3	1
E	T	N
O	R	W
S	E	K
U	R	C
T	Y	I

Stream cipher:



Block cipher:



PT	CT
00	11
01	10
10	00
11	01

PT	CT
00	11
01	10
10	01
11	01

Ideal block cipher :

0000	0	0000
0001	1	0001
0010	2	0010
0011	3	0100
0100	4	0101
0101	5	0110
0110	6	0111
0111	7	1000
1000	8	1001
1001	9	1010
1010	10	1011
1011	11	1100
1100	12	1101
1101	13	1110
1110	14	1111
1111	15	

0000	0	1110
0001	1	0100
0010	2	1101
0011	3	0001
0100	4	0010
0101	5	1111
0110	6	1011
0111	7	1000
1000	8	0011
1001	9	1010
1010	10	0110
1011	11	1100
1100	12	0101
1101	13	1001
1110	14	0000
1111	15	0111

$y_1 =$

$y_2 =$

$y_3 =$

$y_4 =$

Feiskel

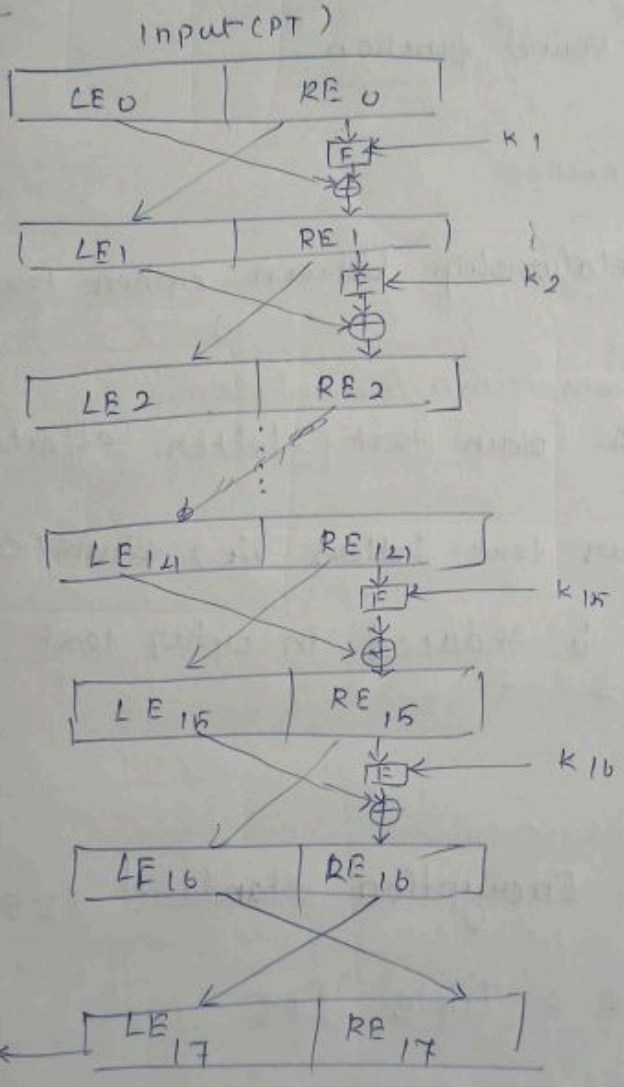
$y_1 = k_{11} x_1 \oplus k_{12} x_2 \oplus k_{13} x_3 \oplus k_{14} x_4$

$y_2 = k_{21} x_1 \oplus k_{22} x_2 \oplus k_{23} x_3 \oplus k_{24} x_4$

$y_3 = k_{31} x_1 \oplus k_{32} x_2 \oplus k_{33} x_3 \oplus k_{34} x_4$

$y_4 = k_{41} x_1 \oplus k_{42} x_2 \oplus k_{43} x_3 \oplus k_{44} x_4$

Feistel cipher:



Introduced by "claude Shanon"

father of Information theory

SPN (substitution and Permutation network):
confusion & diffusion.

Design choices:

① Block size → 64 / 128 bits
② key size → 64 / 128 "
③ No. of. Rounds → 16 Rounds.
④ Subkey Generation
⑤ Round function.

confusion: substitution

It makes relationship between cipher text and key value

Diffusion: transposition / permutation.
A plain text letter affects the value of many cipher text letters ie) statistical nature of plain text is reduced in cipher text.

① Data Encryption Standard (DES) Block size - 64 bit, key size - 56 bit
② Double & Triple DES
③ International Data Encryption Algorithm (IDEA)
④ Blow Fish Algorithm
⑤ Advanced Encryption Standard (AES)

Simplified

encryption
(Initial permutation) IP
(function using K) f_K
swapping
(inverse permutation)

encryption

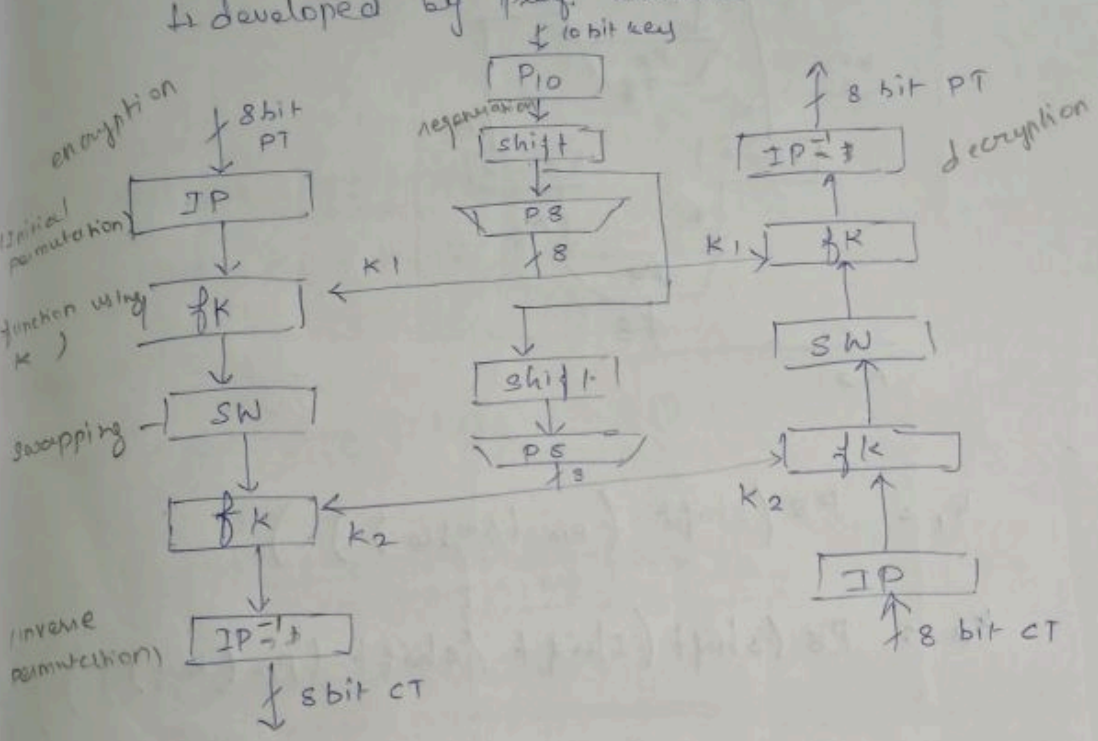
IP

Decry

① key
② enc
③ Dec

Simplified DES (S-DES)

- Block size = 8 bit
- key size = 8 bit
- developed by prof. Edward



encryption :

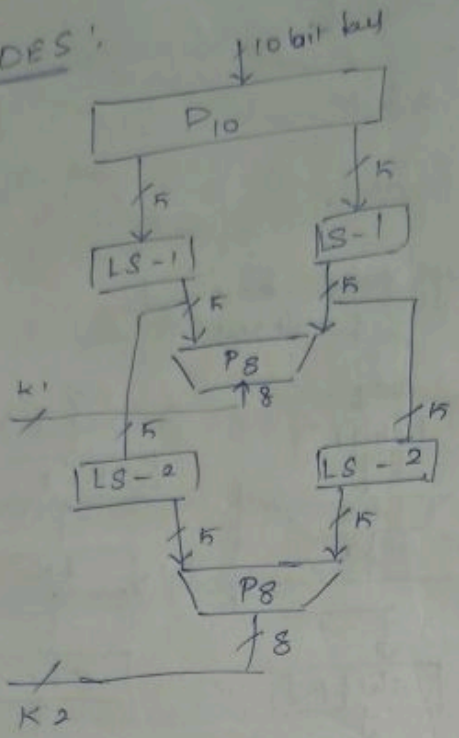
$$IP^{-1}(f_{K_2}(SW(f_{K_1}(IP(P))))) = C$$

Decryption :

$$IP^{-1}(f_{K_1}(SW(f_{K_2}(IP(C))))) = P$$

1. Key Generation
2. encryption
3. Decryption.

S-DES:



$K_1 = P8(\text{shift}(P10(\text{key}_{10})))$

$K_2 = P8(\text{shift}(\text{shift}(\text{shift}(P10(\text{key})))))$

$P_{10} = 3\ 5\ 2\ 7\ 4\ 10\ 1\ 9\ 8\ 6$

$P_8 = 6\ 3\ 7\ 4\ 8\ 5\ 10\ 9$

eg: key : 1 1 1 0 0 0 1 1 0
1 2 3 4 5 6 7 8 9 10

for K1

$P_{10} = (1\ 0\ 1\ 0\ 1\ 0\ 1\ 1\ 1\ 0)$

LS-1 = 0 1 0 1 1 1 1 0 0
1 2 3 4 5 6 7 8 9 10

$P_8 = 10111100 = K_1$

for K2

LS-1 = (01011)(11100)

LS-2 = 01101 10011
1 2 3 4 5 6 7 8 9 10

P8 = 11000111 = K2

ex:

key10 = 1100111001
1 2 3 4 5 6 7 8 9 10

find K1 + K2 = ?

for key1:

P10 = 0110011101

LS-1 = 1100011011
1 2 3 4 5 6 7 8 9 10

P8 = 10100011 = K1

for K2 :

LS-2 = 0001101111
1 2 3 4 5 6 7 8 9 10

P8 = 00111111 = K2

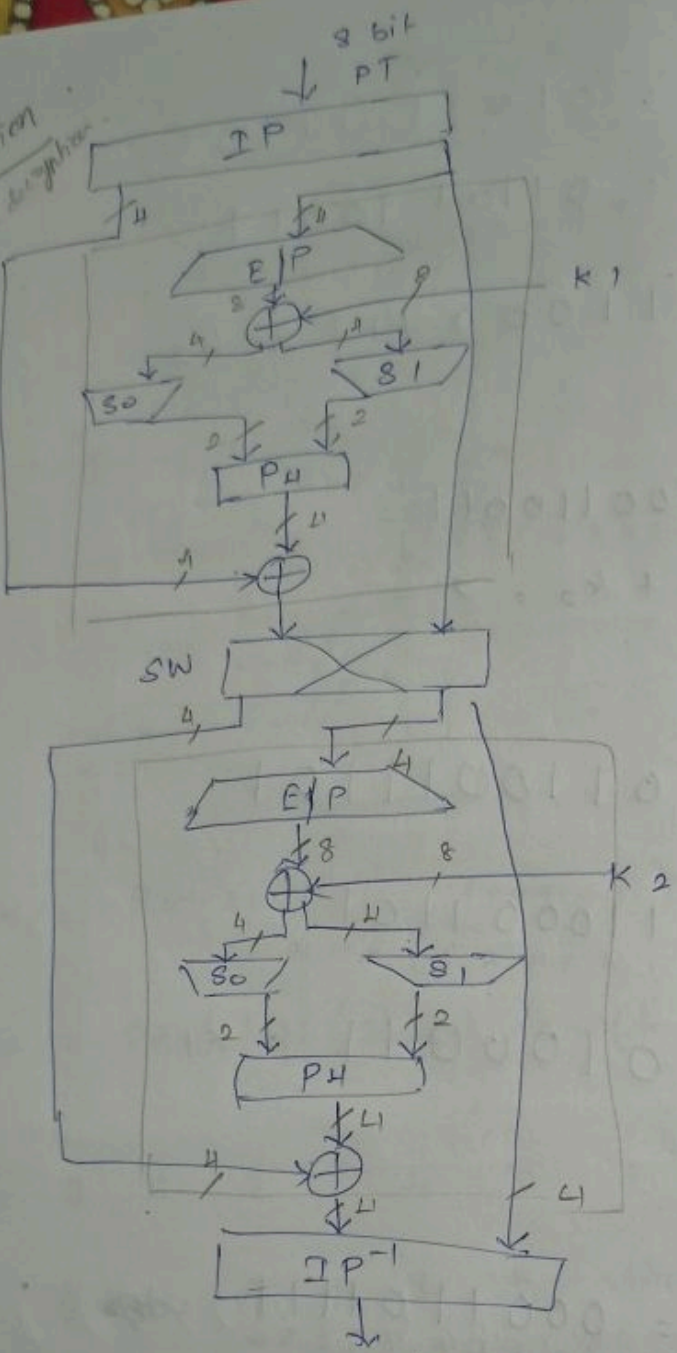
K1 = 10100011

K2 = 00111111

DES :

encryption

reverse this for decryption



E/P -> expansion & permutation

IP : 2 6 3 1 4 8 5 7
1 2 3 4 5 6 7 8

E/P : 4 1 2 3 2 3 4 1

P_4 : 2 4 3 1

IP^{-1} = 4 1 3 5 7 2 8 6

S_0 :

	0	1	2	3
0	1	0	3	2
1	3	2	1	0
2	0	2	1	3
3	3	1	3	2

S_1 :

	0	1	2	3
0	2	0	1	3
1	3	0	1	0
2	2	1	0	3

k_1 = 10100011

k_2 = 00111111

PT = 01000001
1 2 3 4 5 6 7 8

encrypt

IP = (1 0 0 0)(0 1 0 0)
L R

R = 0100

E/P : 0 0 1 0 1 0 0 0

k_1 : 1 0 1 0 0 0 1 1

⊕

1 0 0 0 1 0 1 1

S_0 S_1

S_0 = (0 0 0) → R = 10 = 2 ? — 0 → 00
R C C = 00 = 0 ?

S_1 = (1 0 1 1) → R = 11 = 3 ? — 1 → 01
C C = 01 = 1 ?

decrypt

$S_0 \& S_1 = 0001$

$P_{11} = 0100$

$\perp = 1000$

1100

$R = 0100$

$SN = 0100$

$R = 1100$

$E/P = 01101001$

$K_2 = 00111111$

01010110

$S_0 \quad S_1$

$S_0 \rightarrow 0101 \rightarrow R = 01 = 1$
$C = 10 = 2$ } $1 \rightarrow 01$

$S_1 \rightarrow 0110 \rightarrow R = 00 = 0$
$C = 11 = 3$ } $3 \rightarrow 11$

$S_0 \& S_1 = 0111$

$P_4 = 1110$

$\perp = 0100$

$1010 \quad 1100$

$IP^{-1} = 01110001 = CT$ (113 = 9)

A → 9

decryption

CT = 0 1 1 1 0 0 0 1
1 2 3 4 5 6 7 8

L R
IP = (1 0 1 0)(1 0 0)

R = 1 1 0 0
1 2 3 4

E/P = 0 1 1 0 1 0 0 1

K2 = 0 0 1 1 1 1 1 1

⊕

0 1 0 1 (0 1 1 0)

S0 S1

S0 = 0 1 0 1 → R = 01 = 1 ? 1 = 01
C = 10 = 2 ∫

S1 = 0 1 1 0 → R = 00 = 0 ? 3 = 11
C = 11 = 3 ∫

S0 & S1 = 0 1 1 1
1 2 3 4

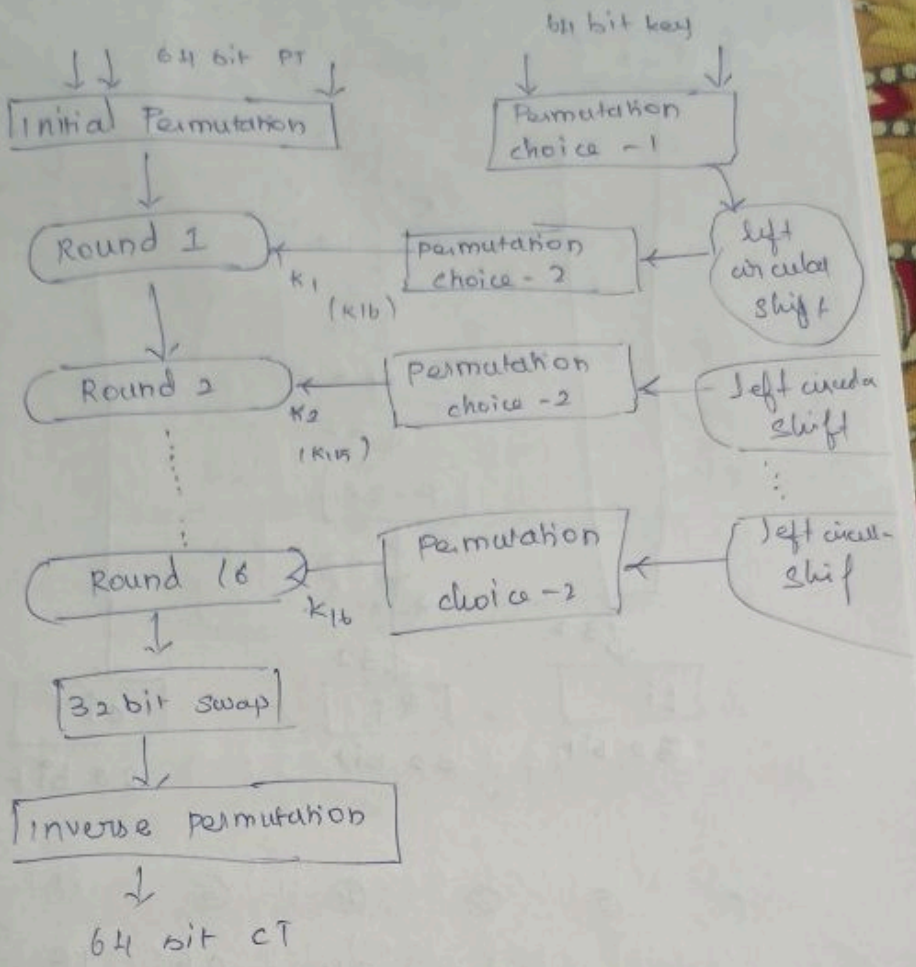
P4 = 1 1 1 0

1 0 1 0
L =

⊕

R
0 1 0 0 1 1 0 0

DES:



↳ Symmentric key Algorithm

↳ developed in 1977 by NIST

↳ Block size 64 bit

↳ key size - 56 bit

① Initial permutation

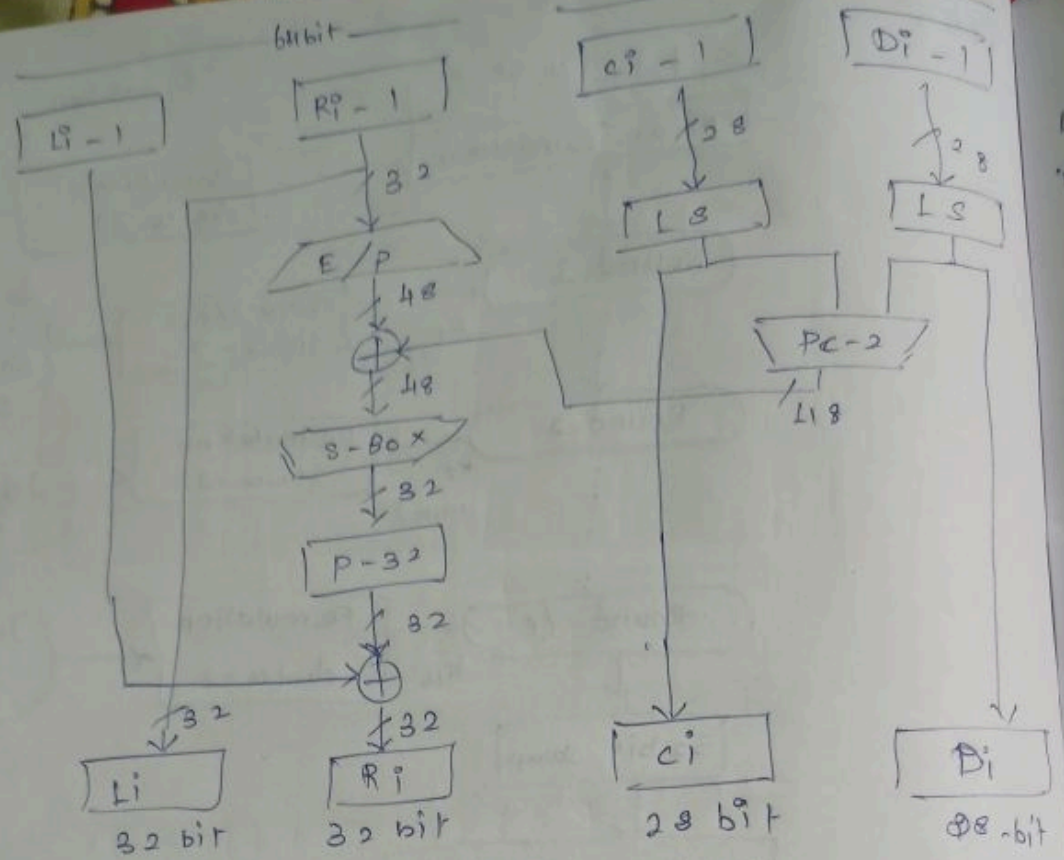
② Round function

③ Swapping

④ Inverse Permutation.

$L_i^0 = R_{i-1}$

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



write in reverse order.

IP^{-1} =

E/P =

IP =

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Inverse order.

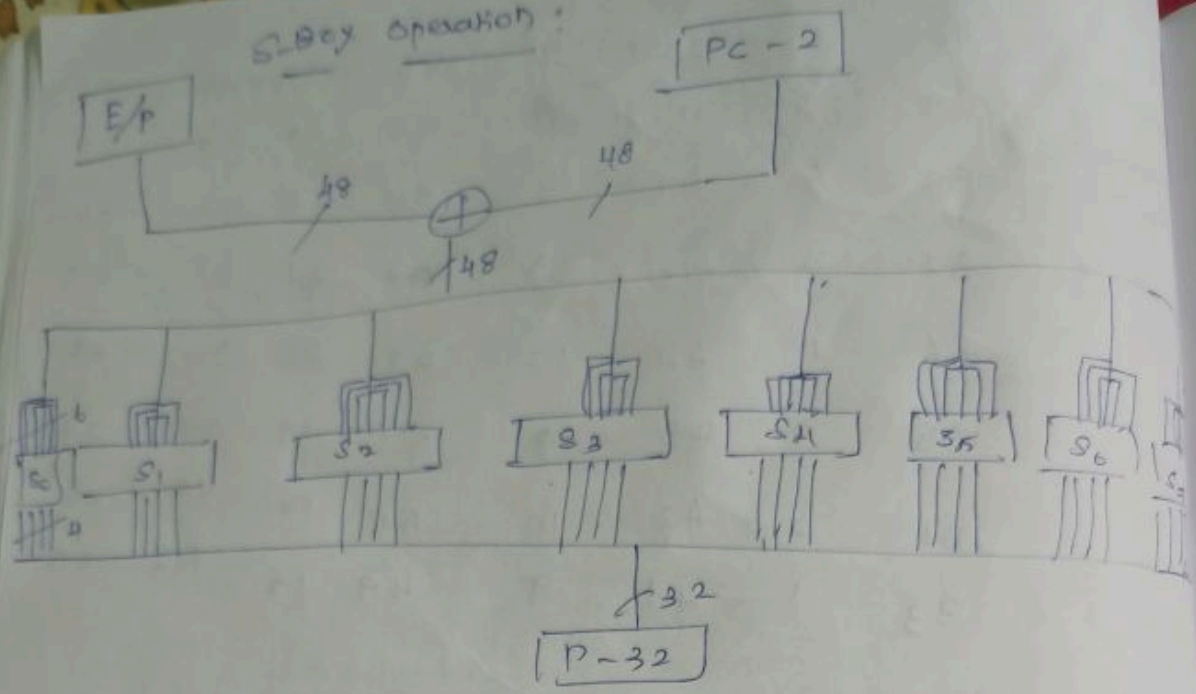
IP^{-1} =

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

E/p =

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

Subkey operation :



Key : 0F 15 71 C9 47 D9 E8 59

0000 1111 0001 0101 0111 1000 1100 1001
0100 0111 1101 1001 1110 1000 0101 1001

PC-1 =

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

PC-1 =

0	1	1	0	1	0	0
0	1	1	1	1	1	1
0	0	0	1	0	0	0
1	0	0	1	0	1	0
0	0	0	1	0	0	0
1	0	0	0	1	0	0
1	1	1	1	1	0	1
0	0	1	0	1	1	0

PC-1 = (0110100 0111111 0001000 1001010
0001000 1000100 1111101 0010110)

left shift
PC-1 = 1101000 0111111 0001000 1001010
0010000 1000100 1111101 0010110

PC-2 =

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

011110 000011 001111 000011
001000 001101 101001 110000

$k_1 = 78\ 33\ C\ 3\ 20\ D\ A\ 70$

Problem:

user A wants to send a message,
M = ABCDEF9876543210 to user B using
DES algorithm. find the output of E/p (E-box)
operation after applying initial permutation operation
on the message.

Sol:

M = 1010 1011 1100 1101 1110 1111 1001 1000
0111 0110 0101 0100 0011 0010 0001 0000

0 0 1 1 0 1 1 0
1 1 1 1 1 0 0 0
0 0 1 1 0 1 1 0
0 0 0 0 0 1 1 1
0 0 0 0 1 1 1 1
0 1 0 1 0 1 0 1
0 0 0 0 1 1 1 1
0 1 0 1 0 1 0 1

Ip =

= (0011 0110 1111 1000 0011 0110 0000 0111)

S1 (0000 1111 0101 0101 0000 1111 0101 0101)
1 4 5 8 9 12 13 16 17 20 21 24 25 28 29 32

R

E/P =

1 0 0 0 0 1
0 1 1 1 1 0
1 0 1 0 1 0
1 0 1 0 1 0
1 0 0 0 0 1
0 1 1 1 1 0
1 0 1 0 1 0
1 0 1 0 1 0

= 1000 0101 1110 1010 1010 1010

1000 0101 1110 1010 1010 1010

= 85 E A A A 85 E A A A

using
-bo a)
operation

22
000

bo b1 b9
0001 0000

Avalanche effect:

If we change single bit value either in the plain text or in the key value it will make significant changes in the cipher text.

Problem 1: using playfair cipher matrix encrypt the message "the enemy must be stopped at all costs. Do whatever is necessary". ~~to find the CT of the corresponding~~

Problem 2: to find CT of the corresponding PT "COMPUT" using hill cipher using

$$key = \begin{bmatrix} 5 & 3 & 6 \\ 2 & 11 & 7 \\ 8 & 1 & 9 \end{bmatrix}$$

Problem 1:

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

UNIT 2: Number theory:

- Divisibility & Division Algorithm
- Euclidian Algorithm
- modular arithmetic
- prime numbers.

Finite Fields:

- Groups
- rings
- fields
- finite field of the form GF(p)
- polynomial arithmetic
- Finite fields of the form GF(2^n)

AES:

- AES transformation function
- AES key expansion
- AES example
- AES implementation

Block cipher operation:

- multiple encryption and triple DES
- ECB - CBC - CFB - OFB
- counter mode
- XTS AES Mode.