9-3-2021

PAGE :
DATE : / /

UNIT : 1 CLASSICAL ENCRYPTION TECHNIQUES : SYMMETRIC CIPHER MODEL

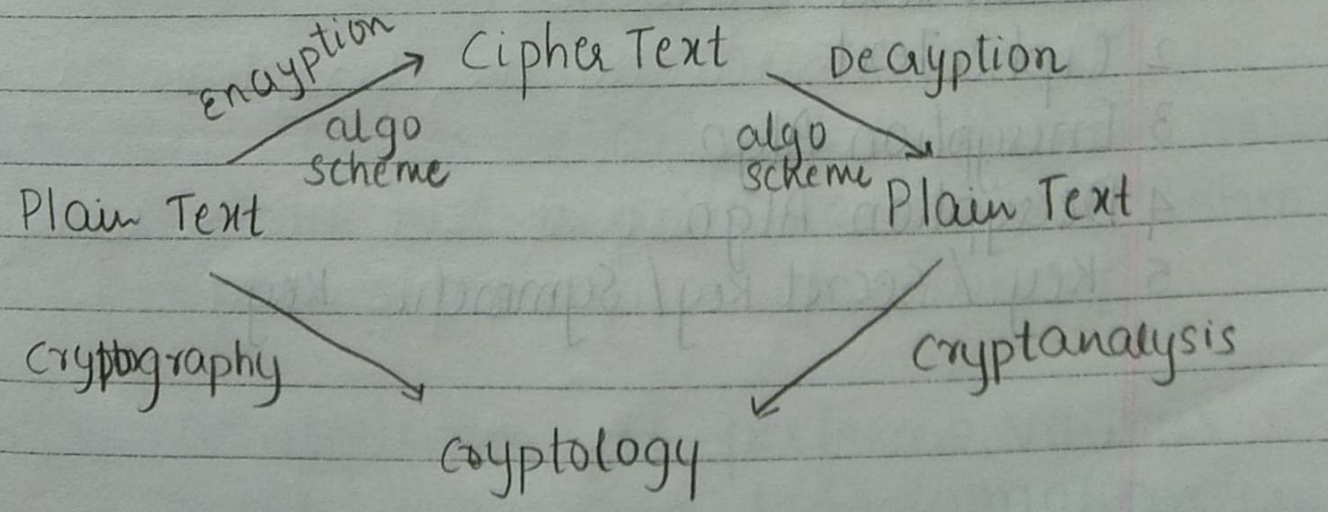
Plain Text : It is the original msg send by user

Cipher Text : It is the coded message.

Method / Process of converting plain text to cipher text is Encryption and vice-versa is decryption ← Restoring the plain text from cipher text

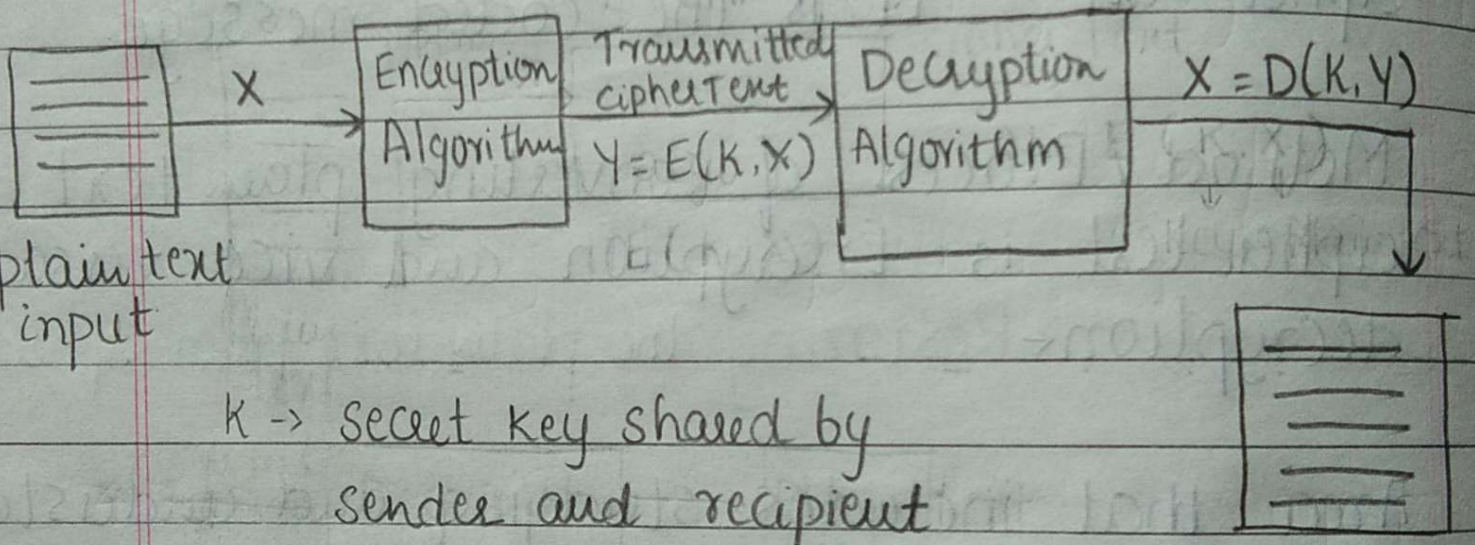
Area that includes studying and understanding algo and schemes of encryption is cryptography and of decryption is crypt analysis.

Cryptology : Cryptography + cryptanalysis



Symmetric encryption
Symmetric cipher model
- These are 5 components

1 Plain text

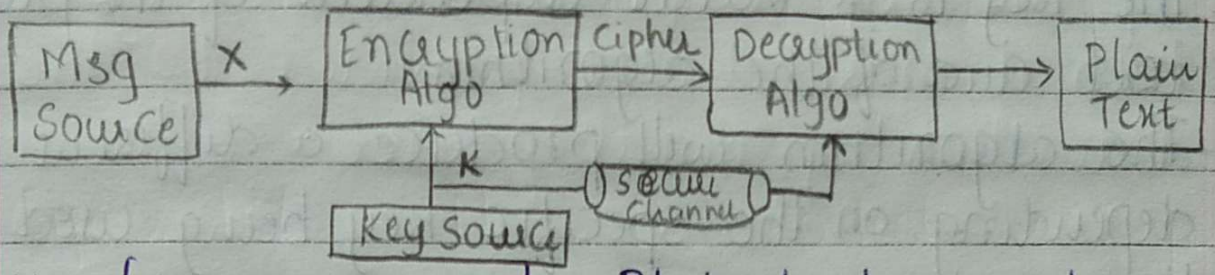


Model

1. Plain Text
2. Cipher Text
3. Encryption Algo
4. Decryption Algo
5. Key / Secret Key / Symmetric Key

~~Cryptosi~~

Essential elements of Symmetric Encryption Scheme



$X = [x_1, x_2, x_3 \ldots x_n]$: Plain text can be a word or an sentence

Key source : generates key K and send it through Secure channel

Cryptology :

The area of cryptography and cryptanalysis together are called cryptology

Symmetric Cipher model :

A symmetric encryption scheme has 5 ingredients

1 Plain Text : This is the original intelligible message or data that is fed into the algorithm as input

2 Encryption algorithm : It performs various substitutions and transformations on the plain text

-3-2021

PAGE :
DATE : / /

Characteristic of Cryptography

1 Type of operation:
2 types:
i Substitution
ii Transposition

i Substitution: in plain text
For every bit we substitute some other value or letter
eg: abc → xyz

ii Transposition:
No new value is substituted, the letters are interchanged or position of letter is changed.
eg: abc → bca or cba

2. The number of keys used secret key algo/convention
1 key algo/ symmetric algo: If same key is used for both encryption and decryption

2 key: one key for encryption, second not same but related to first key for decryption is called public key encryption/ Asymmetric

Sulekha

3 The way in which plain text is processed
2 types
1 block cipher : plain text is divided into block of some bits and each block is converted into cipher text

ii. stream cipher : plain text is processed bitwise.

How do we attack cryptography system
2 ways:
1 Deduce the key
2 Directly deduce plain text
Types of attacks
Cryptanalysis
Brute Force attack

5 types in Cryptanalysis

1 Cipher text only
2 Known plain text : attacker knows algo, cipher text
- attacker knows i. algo
ii. Cipher text
iii Plaintext - Cipher text pair

3 Chosen plain text :
attacker knows : algo, ciphertext, a pair of plaintext & ciphertext from set of PT-CT pair

4 Chosen ciphertext
5 Chosen text.
} not used in real world nowadays

Unconditionally secure system
Computationally secure system

Substitution techniques

1 ~~tea~~ Caesar cipher :
Given the plain text, every bit is substituted with next alphabet. Next is determined by key.
Eg abc K = 3
ciphertext → def.
a - z → 1 - 26.

$Y = E(K, X)$
$Y = (X + K) \bmod 26$
to get plain text back
$X = (Y - K) \bmod 26$.

Cipher text for HI HOW ARE YOU for K = 3

H → 8

Y = (8+3) mod 26

= 11 mod 26

= 11

= K

I → 9

Y = (9+3) mod 26

= 12 mod 26

= 12

= L

O → 15

Y = (15+3) mod 26

= 18 mod 26

= 18

= R

E → 5

Y = (5+3) mod 26

= 8 mod 26

= 8

= H

W → 23

→ (23+3) mod 26

= 26 mod 26

= 0

= Z

A → 1

→ (1+3) mod 26

→ 4 mod 26

4

= D

R → 18

= (18+3) mod 26

= 21 mod 26

= 21

= U

Y = 25

Y = (25+3) mod 26

= 28 mod 26

= 2

= B

HI HOW ARE YOU → KL KRZDUH'BRX

-3-2021

2 Monoalphabetic Cipher:

Some random number is substituted to letter. Some particular letter is substituted to particular letter

3 Play-Fair Cipher:

- Depends on 5x5 matrix
- Rules for Encryption:

1 Draw a 5x5 matrix and construct the matrix by filling the letters of the keyword (omitting the duplicates) from left to right and from top to bottom.

2 Fill the remaining boxes of matrix with the remaining letters of english alphabets in order.

3 Letters I and J are counted as single alphabet or one letter

4 Plain text is divided in a block of 2 bits and if it is not possible add X at the end.

5 Repeating plain text letters that are in the same pair are separated with a filler letter such as 'X' Eg: HELLO → HELXLO

6 If 2 letters fall in the same row of matrix then they are replaced by the letter to its right

7 If both letters fall in same column, then each letter is replaced by the letter beneath it

8 If both letters fall in different row and different column then letters are replaced by the letter that lies in its own row and column occupied by the other plain text letter

Eg:1 Key : SECURITY
PT : COMPUTER

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

COMPUTER
UN NL EACS

2. Key : OCCURRENCE
CT : ZCHENVUZ

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

ZCHENVUZ
WELCOMEX

16-3-2021

4 Hill Cipher

$C = P.K \bmod 26$

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

K → Key (either 2×2 matrix or 3×3 matrix).

Plain text is converted into matrix depending on key, if key → 2×2 P → 1×2

→ 3×3 P → 1×3.

Alphabets start from 0-25

Eg: P = HELP

$$K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$$

Encryption

$C = P.K \bmod 26$.

If $K \rightarrow 2 \times 2$ for PT consider first 2 elements
3×3 " " " " 3 "

$P_1 = HE = (7 \quad 4)$

$C_1 = P_1 K \bmod 26.$

$= \begin{bmatrix} 7 & 4 \end{bmatrix} \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$

$= [29 \quad 41] \bmod 26$

$= [3 \quad 15]$

$= DP$

$\frac{29}{26} = 1.1153\ldots$

Ans - whole no = Ans

Ans x 26

$P_2 = LP = (11 \quad 15)$

$C_2 = P_2 K \bmod 26$

$= \begin{bmatrix} 11 & 15 \end{bmatrix} \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$

$= [63 \quad 108] \bmod 26$

$= [11 \quad 4]$

$= L \; E$

HELP → DPLE

Decryption:

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

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

$|K| = 9$

$Adj(K) = \begin{pmatrix} 5 & -3 \\ -2 & 3 \end{pmatrix}$

$\frac{1}{|K|} = 9x = 1 \bmod 26 \quad \therefore x = 3.$

$K^{-1} = 3\begin{pmatrix} 5 & -3 \\ -2 & 3 \end{pmatrix}$

Add 26 to -ve nos

$K^{-1} = 3\begin{pmatrix} 5 & 23 \\ 24 & 3 \end{pmatrix}$

$= \begin{pmatrix} 15 & 69 \\ 72 & 9 \end{pmatrix} \bmod 26$

$K^{-1} = \begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix}$

$P_1 = (3 \quad 15)\begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \bmod 26.$

$= (345 \quad 186) \bmod 26.$

$= (7 \quad 4)$

$= HE$

$$P_2 = (11 \quad 4)\begin{pmatrix} 15 & 17 \\ 20 & 9 \end{pmatrix} \bmod 26$$

$$= (245 \quad 223) \bmod 26$$

$$= (11 \quad 15)$$

$$= LP$$

DPLE → HELP

2. $$K = \begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix}$$

PT = SCHOOL

$P_1 = SC = (18 \quad 2)$

$C_1 = P_1 K \bmod 26$

$$= (18 \quad 2)\begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix}$$

$$= (124 \quad 150) \bmod 26$$

$$= (20 \quad 20)$$

$= UU$

$P_2 = HO = (7 \quad 14)$

$C_2 = P_2 K \bmod 26$

$$= (7 \quad 14)\begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix}$$

$$= (273 \quad 98) \bmod 26$$

$$= (13 \quad 20)$$

$= NU$

$P_3 = OL = (14\ 11)$

$C_3 = P_3 K \bmod 26$

$= (14\ 11)\begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix}$

$= (257\ 145) \bmod 26$

$= (23\ 15)$

$= X\ P$

SCHOOL → UU NU XP

Decryption

$P = CK^{-1} \bmod 26$

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

$|K| = -121 \bmod 26 = 9$

$\frac{1}{|K|} = 3 \qquad Adj(K) = \begin{pmatrix} 3 & -8 \\ -17 & 5 \end{pmatrix}$

$K^{-1} = 3\begin{pmatrix} 3 & -8 \\ -17 & 5 \end{pmatrix} = 3\begin{pmatrix} 3 & 18 \\ 9 & 5 \end{pmatrix}$

$= \begin{pmatrix} 9 & 54 \\ 27 & 15 \end{pmatrix} \bmod 26$

$K^{-1} = \begin{pmatrix} 9 & 2 \\ 1 & 15 \end{pmatrix}$

$P_1 = C_1 K^{-1} \bmod 26$ $\quad C_1 \rightarrow UU\ (20\ 20)$

$= (20\ 20) \begin{pmatrix} 9 & 2 \\ 1 & 15 \end{pmatrix} \bmod 26$

$= (200\ 340) \bmod 26$

$= (18\ 2)$

$= S\ C$

$P_2 = C_2 K^{-1} \bmod 26$ $\quad C_2 = NU\ (13, 20)$

$= (13, 20) \begin{pmatrix} 9 & 2 \\ 1 & 15 \end{pmatrix} \bmod 26$

$= (137\ 326)$

$= (7\ 14)$

$= H\ O$

$P_3 = C_3 K^{-1} \bmod 26$ $\quad C_3 = XP\ (23\ 15)$

$= (23\ 15) \begin{pmatrix} 9 & 2 \\ 1 & 15 \end{pmatrix} \bmod 26$

$= (222\ 271) \bmod 26$

$= (14\ 11)$

$= O\ L$

PAGE :
DATE : / /

3×3 Encryption

1. $K = \begin{bmatrix} 17 & 7 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$ P = Pay more money

$P_1 = (15 \quad 0 \quad 24)$

$C_1 = P_1 K \bmod 26$

$= (15 \quad 0 \quad 24) \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \bmod 26$

$= (303 \quad 303 \quad 531) \bmod 26$

$= (17 \quad 17 \quad 11)$

R R L

$P_2 = MOR = (12 \quad 14 \quad 17)$

$C_2 = P_2 K \bmod 26.$

$= (12 \quad 14 \quad 17) \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \bmod 26$

$= [532 \quad 490 \quad 677] \bmod 26.$

$= [12 \quad 22 \quad 1]$

= M W B

P_3 = EMO : (4 12 14)

$C_3 = P_3 K \bmod 26$

$= (4\ 12\ 14) \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \bmod 26$

$= (348\ 312\ 538)$

$= 10\ 0\ 18$

= K A S

P_4 = NEY : (13 4 24)

$= P_4 K \bmod 26$

$= (13\ 4\ 24) \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \bmod 26$

$= (353\ 341\ 605) \bmod 26$

$= 15\ 3\ 7$

= P D H

Pay more money → RRL MWBK ASPDH

Decryption:

$|K| = 17(300) - 17($

$= -939 \bmod 26 = 23$

$$\frac{1}{|K|} = ax \equiv 1 \bmod n$$

$$23x \equiv 1 \bmod 26 = 17.$$

q	n	a	r	t_1	t_2	t	$t = t_1 - (t_2 \times q)$
	26	23	3	0	1	-1	
7	23	3	2	1	-1	8	
1	3	2	1	-1	8	-9	
2	2	1	0	8	-9	26	
	1	0		-9	26		

start with 0 1

+26 = 17.

Adj (~~A~~K) Cofactor (K) $= \begin{bmatrix} +300 & -357 & +6 \\ -313 & +313 & -0 \\ +267 & -252 & -51 \end{bmatrix}$

$$Adj(K) = \begin{bmatrix} +300 & -313 & +267 \\ -357 & +313 & -252 \\ +6 & -0 & -51 \end{bmatrix} \bmod 26$$

$$Adj(K) = \begin{bmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{bmatrix}$$

$$K^{-1} = 17 \begin{bmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 238 & 425 & 119 \\ 119 & 17 & 136 \\ 102 & 0 & 17 \end{bmatrix}$$

Sulekha

$$K^{-1} = \begin{bmatrix} 238 & 425 & 119 \\ 119 & 17 & 136 \\ 102 & 0 & 17 \end{bmatrix}$$

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

$C_1 = RRL\ (17\ \ 17\ \ 11)$

$P_1 = CK^{-1} \bmod 26$

$$= (17\ 17\ 11) \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix}$$

$= (587\ \ 442\ \ 544) \bmod 26$

$= (15\ \ 0\ \ 24)$

$=$ PAY

$C_2 = MWB\ (12\ \ 22\ \ 1)$

$$= (12\ 22\ 1) \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix}$$

$= [402\ \ 482\ \ 329]$

$= (12\ \ 14\ \ 17)$

$=$ MOR

PAGE :
DATE : / /

$C_3 = KAS = (10\ 0\ 18)$

$P_3 = C_3K^{-1} \bmod 26$

$= (10\ 0\ 18)\begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix} \bmod 26$

$= (472\ \ 90\ \ 456) \bmod 26$

$= (4\ 12\ 14)$

$= EMO$

$C_4 = PDH = (15\ 3\ 7)$

$= (15\ 3\ 7)\begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix} \bmod 26$

$= (273\ \ 186\ \ 362) \bmod 26$

$= (13\ 4\ 24)$

$= NEY$

RRLMWBKASPDH → PAY MORE MONEY.

2021

5 Polyalphabetic Ciphers

i Vigenere Ciphers:

- Keyword (n)
- Plain text (m)

$n \leq m$ $n \not> m$

if $n < m$, to make $n = m$, repeat Keyword

Eg: K → abc

PT → xyzabcd

∴ K → abcabcca

Then cipher text → x → 23 a → 0

$(23+0) \bmod 26 = 23$

∴ CT → x

Eg1. K → deceptive

PT → we are discovered save yourself

de cep tivedecept ived eceptive

d → 3	w → 22	25 mod 26 = 25 → Z
e → 4	e → 4	8 mod 26 = 8 → I
a → 0	c → 2	2 mod 26 = 2 → C
r → 17	e → 4	21 mod 26 = 21 → V
e → 4	p → 15	19 mod 26 = 19 → t
d → 3	t → 19	22 mod 26 = 22 → W
i → 8	i → 8	16 mod 26 = 16 → Q

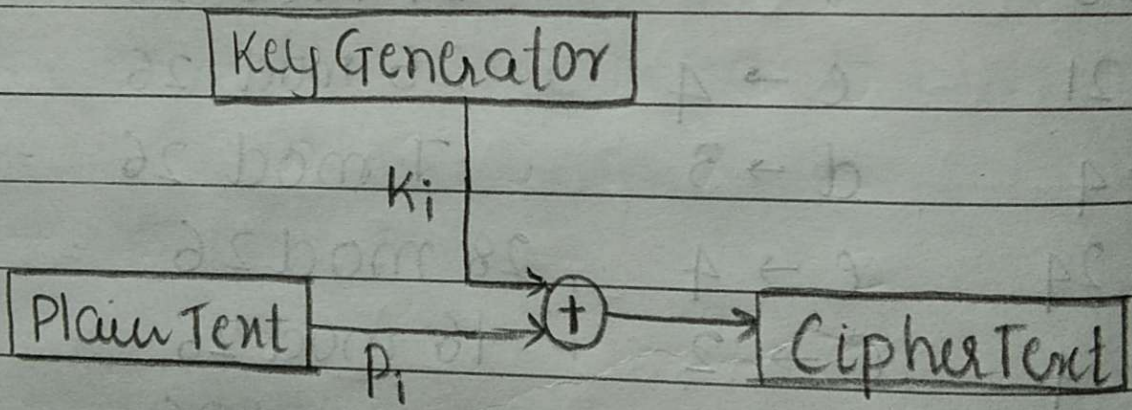
PAGE :
DATE : / /

S → 18	V → 21	439 mod 26 = 13 → N
C → 2	e → 4	6 mod 26 = 6 → g
O → 14	d → 3	17 mod 26 = 17 → r
V → 21	e → 4	25 mod 26 = 25 → z
e → 4	C → 2	6 mod 26 = 6 → g
r → 17	e → 4	21 mod 26 = 21 → v
e → 4	p → 15	19 mod 26 = 19 → t
d → 3	t → 19	22 mod 26 = 22 → w
S → 18	i → 8	26 mod 26 = 0 → a
a → 0	v → 21	21 mod 26 = 21 → v
v → 21	e → 4	25 mod 26 = 25 → z
e → 4	d → 3	7 mod 26 = 7 → h
y → 24	e → 4	28 mod 26 = 2 → c
o → 14	C → 2	16 mod 26 = 16 → q
u → 20	e → 4	24 mod 26 = 24 → y
r → 17	p → 15	32 mod 26 = 6 → g
S → 18	t → 19	37 mod 26 = 11 → l
e → 4	i → 8	12 mod 26 = 12 → m
l → 11	v → 21	32 mod 26 = 6 → g
f → 5	e → 4	9 mod 26 = 9 → j.

Sulekha

Autokey system: The repeating nature of keyword is removed.
We use/repeat the plaintext in keyword instead of using keyword itself to match the length.

ii. Vernam cipher
- deals only with binary data.
- key generated will be random



To make vernam cipher more secure we use one timepad system

DATE : / /

Transposition Technique / Columnar Cipher
- also called as Permutation.
Type : Rail Fence Cipher.

g: PT : meet me in the evening

1 Write PT diagonally:

m e m i t e v n n
e t e n h e e i g

CT : memitevnnetenheeig.
- This technique is not much secure, so we use other techniques.

Single encryption and double encryption.

: PT : attack postponed until two am
Key : 4 3 1 2 5 6 7
n: Key : 4 3 1 2 5 6 7
PT : 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

Sulekha

CT : orderwise of key

i.e. 1 2 3 4 5 6 7

ttnaaptmtsuoaodwcoixknlypetz.

- This is single transposition
- For double transposition plain text is the obtained cipher text in single transposition

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

CT : nscyauoptwltmdnaoiepaxttokz

3-3-2021

PAGE :
DATE : / /

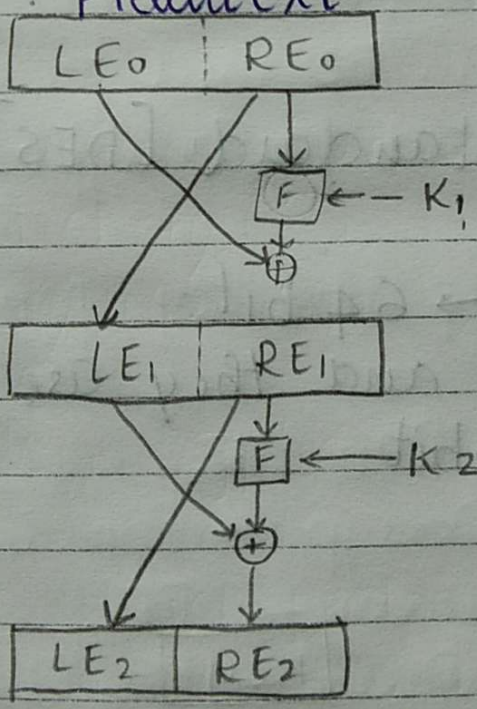
Fiestel Cipher :

- uses block cipher techniques
- PT → n bits , Key → k bits
- Combinat^n of substitution & transposition techniqu

Confusion : uses substitution
Diffusion : " transposition.

Encryption

I/P : Plaintext

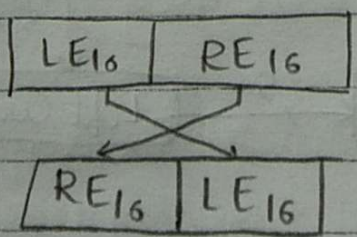


F → round function
F(K1, RE0)

Top-down Approach
n = 16
n - rounds are performed

To get cipher text swap the last RE and LE

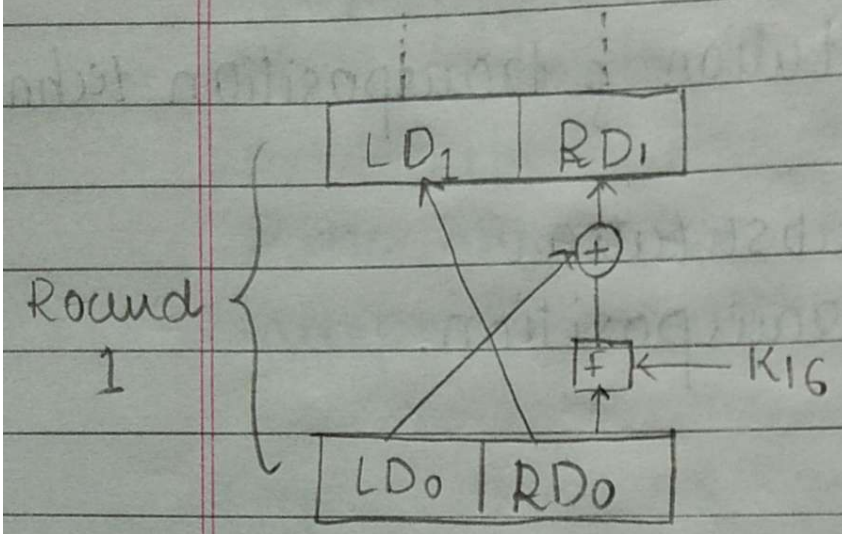
Eg:



Sulekha

Decryption:

- Bottom up approach



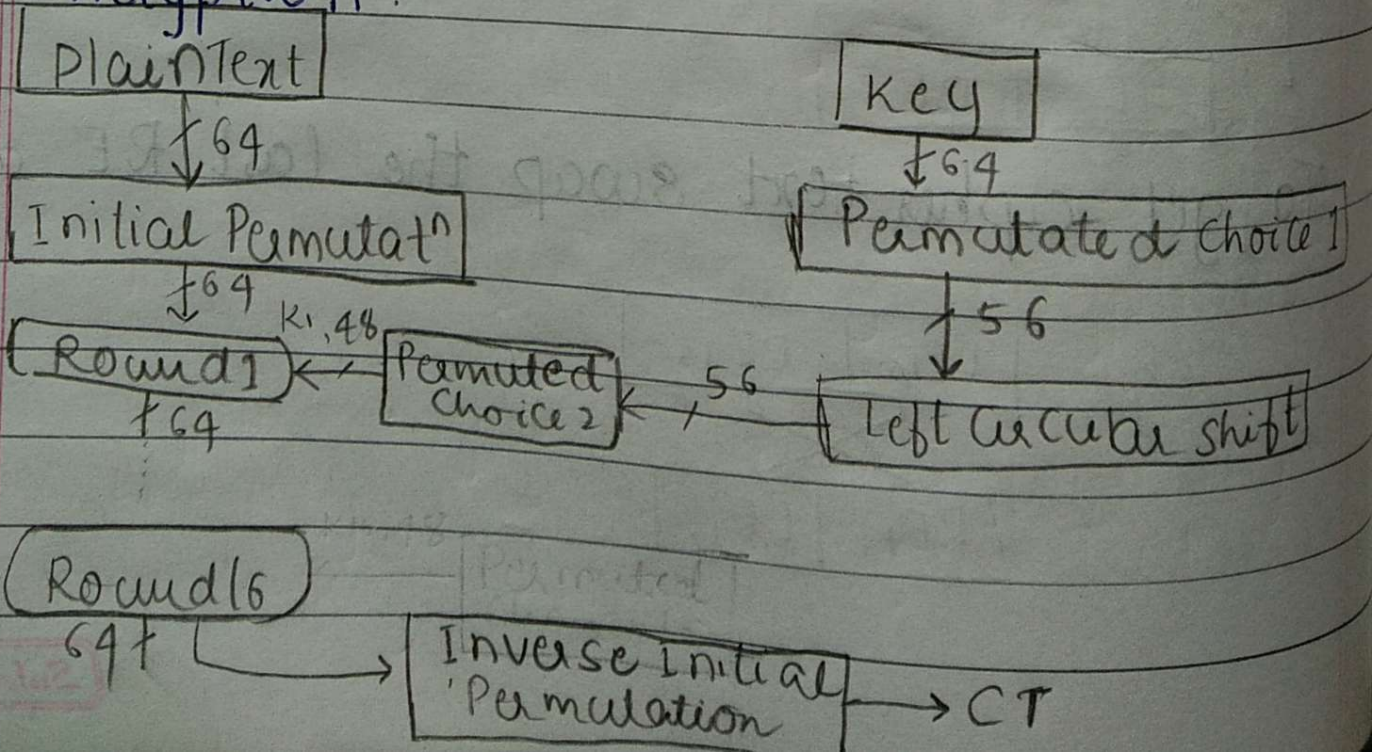
$LD_0 = RE_{16}$

$RD_0 = LE_{16}$

Data Encryption Standard [DES]

- PT → 64 bit, K → 64 bit.
- subkeys are used and they are of 48 bit, CT → 64 bit

Encryption:



PAGE :
DATE : / /

Design Principles:

1. No. of Rounds : Std no. of rounds → 16.
2. Design of function F
   - It has to be non-linear
   - It has to exhibit strong avalanche effect
     SAC - ~~sdsf~~ Strict Avalanche Criteria
     BIC - Bit Independent Criteria.
3. Design / Scheduling of subkey.