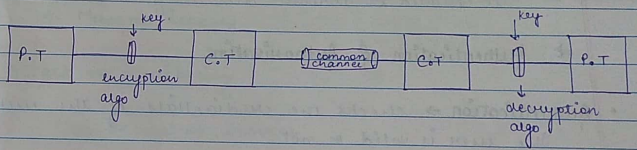
Date.
Page No.

Date.
Page No.

Cryptography & Network Security

→ Plain text (sent from sender side)

→ Cipher text (Recieved at reciever side).



Basic components of cryptography :-

→ Plain text
→ cipher text
→ encryption algo
→ decryption algo
→ key

⇒ KEY

- Symmetric key → if both keys are same
- Asymmetric key → if both keys are different

Date.
Page No.

⇒ CIA triad.

- C → confidentiality
  message is recieved by intended user only.
- I → integrity
  message when recieved from sender side it should not be altered.
- A → availability
  it should be avaible according to user's need.

⇒ Authentication & Authorization

- Authentication → checks the credientials of the user. The user is valid or not.
- Authorization → access limitations
  e.g. SAP

⇒ ATTACKS.

- Active attack → attackers not only read but also modify the data.
- Passive attack → attackers motive is to only read the data and do no modification.

⇒ Attack on Confidentiality

1. Message reception

Date.
Page No.

Attack on confidentiality

1. Reception 2. Traffic analysis

Attack on Integrity

1. Modification
2. Replaying → Sending multiple request
3. Repudiation → sender as attacker or reciever as attacker.
4. Masque Reading

Attack on availability

1. Denial of Service.

Cryptography

Symmetric key → 1 key.

Assymmetric key → 2 key. → Public, Private.

1. Caesar Cipher (Substitution Cipher).

- It works only on alphabets

→ Generalized Caesar Cipher.

Date.
Page No.

2. Play fair cipher. (also works only on letters).

PT → PLAYFAIR
KEY → CRYPTO

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

(since 25 blocks are there i, j will be taken together)

- Now pair plain text

→ (PL)(AY)(FA)(IR)

- if last one alphabet is left then add x with it.
- if two same letters are there add filler letter x.

BALLOON.
BALXLOON

if Balloon was the key.

B	A	L	O	N

Date.
Page No.

⇒ if pairing alphabets lie in same column.

e.g. E → K
K → S.

e.g. ~~S → Z~~.

S
K

S → K
Z → T

⇒ if pairing alphabets are same column

O	A	B	D	E

→ A-D → B, E

⇒ if not in same row or column.

A Q → D

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

Limitations:-
- i & j occupy same place.
- filler letter is taken as X.
- only work on alphabets

for improvement we used 7X4 play fair cipher.

26 → alphabets
other 2 → * #.
when 2 alphabets are same for pairing #.
when 1 alphabet is left at last → *.

- removal dependencies of x.
- solved ij problems
- NO numerals.

Now 6×6 came into existance.

26 → alphabets
0-9 → numerals.

→ we needed fill letter
→ no togethter use of capital & small letter.

Then final 16×16 came.

Q:- P.T → COMPUTER SCIENCE
KEY → DITU.
playfair cipher 5×5

C	O	M	P	U
T	E	R	S	C
I	N			

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

COMPUTER SCIENCEX

BP KR AU FQ PG TE KG LT

BP KR AU FQ PG TC KG LT

when attackers read the data and confidentiality is hampered.
- content specific & address specific.

2. Traffic analysis

⇒ Attack on integrity

1. modification → modification in data
2. Replaying → sending multiple request.
3. Repudation → when two

1. Caesar Cipher Algorithm [substitution cipher].

- used during World war for sending information.
- Applicable on alphabets only.
- Take reference with alphabets like

A - 0
B - 1
⋮
X - 25

cipher text = (plain text + 3) mod 26.
(3 ↑ key position)

When send A B C, sender side

CT = (PT + 3) mod 26.

A CT_1 = (0 + 3) mod 26 = 3 → D
B CT_2 = 4 → E
C CT_3 = 5 → F

Recieve D E F

:- New Modification (Generalize Caesar Cipher).

Choose random key value like

CT = (PT + K) mod 26

By hit and trial, it will also be leaked.

Reciever side :- PT = (CT - 3) mod 26 - A
- B
- C.

Date.
Page No.

Symmetric cipher — 1 key

Asymmetric cipher — 2 keys (public / private)

1. Caesar Cipher

PT, K, CT

PT - C A E S A R [K = 3]

$CT_1 = C = (2+3) \bmod 26 = 5$ - F

$CT_2 = A = (0+3) \bmod 26 = 3$ - D

$CT_3 = E = (4+3) \bmod 26 = 7$ - H

↳ Reciever at recipient side.

6.

Reciever :-

$PT_1 = (CT - 3) \bmod 26$.

→ stream cipher : when substitute one alphabet at a time (used here).

Limitation

1) Applicable on alphabet only.

2) If someone knows that the message is send using Caesar cipher then key will be find easily (b/w 0-25).

Date.
Page No.

2. Playfair Cipher [Block cipher]

Given : PT, key.

PT → PLAYFAIR

key → CRYPTO

- Work on alphabets only.
- Make 5×5 box.

Assumptions

1. I & J will occupy same place.
- There two will not occur consequently

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

Date.
Page No.

• VIGENERE CIPHER [stream cipher]

PT & key.

PT → X Y Z A B C D E F
KEY → D I T U

extend key upto plain text.

PT → X Y Z A B C D E F
KEY → D I T U D I T U D.

$C_i = (PT_i + K_i) \bmod 26$.

$C_1 = (PT_1 + K_1) \bmod 26 = (23+3) \bmod 26 = 0 = A$
$C_2 = (PT_2 + K_2) \bmod 26 = (24+10) \bmod 26 = 8 = I$
$C_3 = (PT_3 + K_3) \bmod 26 = (25+21) \bmod 26 = 20 =$
$C_4 = (PT_4 + K_4) \bmod 26 = (0+22) \bmod 26 = 22 = U.$

for decryption :-

$PT_i = (CT_i - K_i) \bmod 26$.

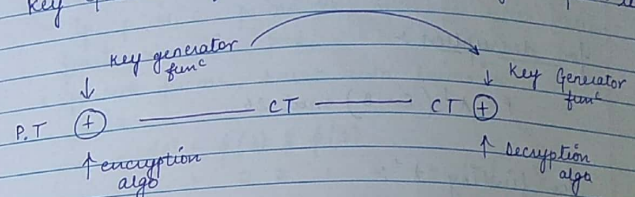
categories

- Polyalphabatic → if one character has more one occurence and both have diff. cipher text.
- Monoalphabatic → if one character has more than one occurence and both have same cipher text.

Date.
Page No.

5. VERNAM CIPHER [stream cipher]

Key Generator func^c and encryption algo on plain text.



PT	X	Y	Z	A	B	C	D	E	F	X
	1	1	1	1	1	1	1	1	1	1
	18	24	3	2	5	8	9	11	12	13

$CT = (PT + K) \bmod 26$

$PT = (CT - K) \bmod 26$.

AFFINE CIPHER

PT = PLAYFAIR

$C = (PA + B) \bmod 26$

A: multiplicative key.
B: additive key

multiplicative key should be co-prime to 26.
A = 5.
B = 8.

$P(CT_1) = (15*5+8) \bmod 26 = 83 \bmod 26 = 5 = E$

$L(CT_1) = (11*5+8) \bmod 26 = 63 \bmod 26 =$

for decryption :-

$P = A^{-1}(C-B) \bmod 26$

for finding A^{-1} :-

1. Hit and trial method

$X = \frac{1}{A} \bmod 26$

$XA = 1 \bmod 26$

$X5 = 1 \bmod 26$

find value of X such that after multiplying with 5 and further divide by 26 leaves rem = 1

Let X5 be 27 X 79 X 33 X

105 → follows

$5*21 = 1 \bmod 26$

2) EULER TOTIENT FUNCTION (ϕ)

- it works only on prime no.
- if P is a prime no. then its euler totient func^c value is $p-1$.
- if not prime, break into prime no.

Ex:- 6.

$\phi(6) = \phi(3) * \phi(2)$

$= 2 * 1 = \boxed{2}$

$\phi(P) = P-1$.

$\phi(P) = \phi(m) * \phi(n)$. } distinct prime.

$= (m-1) * (n-1)$ }

Ex:- 9. (Not distinct prime occur so

$a = 3^2$

$\phi(3^2) = 3^2 - 3^1$

$= 6$

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

Euler totient func^c tells the total relative prime numbers of the number.

$$A^{-1} \bmod m = A^{\phi(m)-1} \bmod m$$

$P = A^{-1}(C - B) \bmod 26.$

$= 5^{-1} \bmod 26.$

$\phi(26) = \phi(13) * \phi(02)$

$= 12 * 1 = 12.$

$5^{11} \bmod 26.$

$5 \bmod 26 = 5$

$5^2 \bmod 26 = 25$

$5^4 \bmod 26 = 625 \bmod 26 = 1.$

$(5^4 \bmod 26) = (5^4 \bmod 26 . 5^4 \bmod 26 . 5^2 \bmod 26).$

$= (1 * 1 * 25 * 5) \bmod 26$

$= 21.$

$A \bmod m = M - A \bmod m$

8. CT = HPCC XAQ A = 5, B = 8

using affine cipher generate PT.

$P_1 = A^{-1}(C - B) \bmod 26$

$= 5^{-1}(7 - 8) \bmod 26 = 5^{-1} - 1 \bmod 26$

$= 5 \bmod 26 =$ F

$P_2 = 5^{-1}(15 - 8) \bmod 26$

$= 21 * 7 \bmod 26$

$= 147 \bmod 26 \Rightarrow 17$ R

Date.
Page No.

6. HILL CIPHER. [Block cipher].

PT & K.

- key is in the form of matrix (Always square matrix N*N).
- Plain text is divided into blocks (NX1).

$$C = KP \mod 26$$

(K: key, P: plain text)

$$\begin{bmatrix} C_1 \\ C_2 \\ C_3 \end{bmatrix} = \begin{bmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{bmatrix}_{3\times3} \begin{bmatrix} P_1 \\ P_2 \\ P_3 \end{bmatrix}_{3\times1} \mod 26.$$

if key 3x3, organize PT in 3x1 form.

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

Suppose $K = \begin{bmatrix} 2 & 3 \\ 6 & 7 \end{bmatrix}_{2\times2}$

PT = NO ANSWER

Make pair of 2 alphabet for single alphabet use filler element.

$$CT_1 = \begin{bmatrix} 2 & 3 \\ 6 & 7 \end{bmatrix} \begin{bmatrix} N \\ O \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 2 & 3 \\ 6 & 7 \end{bmatrix} \begin{bmatrix} 13 \\ 14 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 26+42 \\ 78+98 \end{bmatrix} \mod 26 = \begin{bmatrix} 68 \\ 176 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 16 \\ 20 \end{bmatrix} = \begin{bmatrix} Q \\ U \end{bmatrix}$$

$$CT_2 = \begin{bmatrix} 2 & 3 \\ 6 & 7 \end{bmatrix} \begin{bmatrix} A \\ N \end{bmatrix} \mod 26.$$

$$= \begin{bmatrix} 2 & 3 \\ 6 & 7 \end{bmatrix} \begin{bmatrix} 0 \\ 13 \end{bmatrix} \mod 26 = \begin{bmatrix} 39 \\ 91 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 13 \\ 13 \end{bmatrix} = \begin{bmatrix} N \\ N \end{bmatrix}$$

Similarly find for all elements:

$$CT_3 = \begin{bmatrix} 2 & 3 \\ 6 & 7 \end{bmatrix} \begin{bmatrix} S \\ W \end{bmatrix} \mod 26.$$

$$= \begin{bmatrix} 2 & 3 \\ 6 & 7 \end{bmatrix} \begin{bmatrix} 18 \\ 22 \end{bmatrix} \mod 26 = \begin{bmatrix} 102 \\ 262 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 24 \\ 2 \end{bmatrix} = \begin{bmatrix} Y \\ C \end{bmatrix}$$

PT = NO ANSWER.

QU NN YC HN

Polyalphabetic cipher because one PT has different CT every time for ex: N has Q & N both.

Ques CT = QV NA VB HI

$$K = \begin{bmatrix} 2 & 3 \\ 7 & 8 \end{bmatrix}$$

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

$$K = \begin{bmatrix} 2 & 3 \\ 7 & 8 \end{bmatrix} = 16 + 21 = 37.$$

$$\begin{bmatrix} P_1 \\ P_2 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 7 & 8 \end{bmatrix}^{-1} \begin{bmatrix} Q \\ V \end{bmatrix} \bmod 26 \quad — (1)$$

Step 1:-

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

$$= \frac{1}{|A|} \times \text{Adj } A$$

↑ Transpose matrix

$$\begin{bmatrix} 2 & 3 \\ 7 & 8 \end{bmatrix} = \frac{1}{16-21} \begin{bmatrix} 8 & -3 \\ -7 & 2 \end{bmatrix}$$

$$= \frac{-1}{5} \begin{bmatrix} 8 & -3 \\ -7 & 2 \end{bmatrix} \bmod 26$$

$$= 5^{-1} \begin{bmatrix} 8 & -3 \\ -7 & 2 \end{bmatrix} \bmod 26$$

$$= 5^{-1} \begin{bmatrix} -8 & +3 \\ +7 & -2 \end{bmatrix} \bmod 26. \quad — (2)$$

$5^{-1} \bmod 26 = 5^{\phi(26)-1} \bmod 26.$

$= 5^{11} \bmod 26 = 21$

from (2) $= 21 \begin{bmatrix} -8 & 3 \\ 7 & -2 \end{bmatrix} \bmod 26.$

$$= \begin{bmatrix} -168 & 63 \\ 147 & -42 \end{bmatrix} \bmod 26.$$

$$K^{-1} = \begin{bmatrix} 14 & 7 \\ 17 & 10 \end{bmatrix}$$

Now we formula to find PT.

$$PT_1 = \begin{bmatrix} 14 & 11 \\ 17 & 10 \end{bmatrix} \begin{bmatrix} Q \\ V \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 14 & 11 \\ 17 & 10 \end{bmatrix} \begin{bmatrix} 16 \\ 21 \end{bmatrix} \bmod 26.$$

OR

$$A^{-1} = \frac{1}{|A|} \times \text{Adj } A \qquad \begin{bmatrix} 2 & 3 \\ 7 & 8 \end{bmatrix}^T$$

$$= \frac{+1}{+5} \begin{bmatrix} 2 & 7 \\ 3 & 8 \end{bmatrix} \qquad |A| = 16 - 21 = -5.$$

$$= 5^{-1} \begin{bmatrix} 2 & 7 \\ 3 & 8 \end{bmatrix} \bmod 26.$$

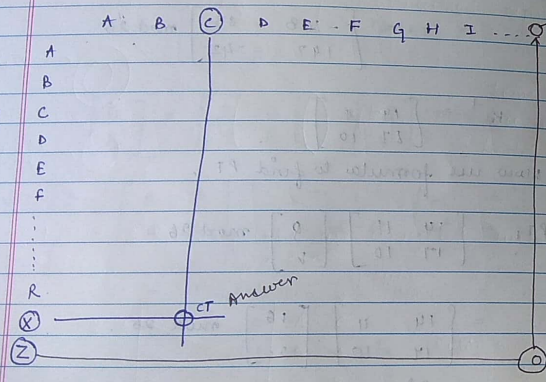
$$= 21 \begin{bmatrix} 2 & 7 \\ 3 & 8 \end{bmatrix} \bmod 26 = \begin{bmatrix} 42 & 147 \\ 63 & 168 \end{bmatrix} \bmod 26$$

Property :- $[K][K^{-1}] \bmod 26 = \text{Identity matrix } [I]$

⇓

Then only solve using hill cipher

VIGENERE CIPHER :- Vigenere Cipher



let PT = C R Y P T O (extend key).
Key = X Y Z X Y Z.

i.e. CT = (C) R Y (P) T (O)
K = (X) Y Z (X) Y (Z)

TRANSPOSITION CIPHER

1. Rail fence Cipher.

PT → we organize PT in zigzag form.

Ex:-
PT = RAIL FENCE CIPHER. depth = 2.

R A I L F E N C E C I P H E R

CT :- R I F N E I H R A L E C C P E

2. Columnar Transposition

Division in column → a entry is given → In how many col^m you divide i.e 4.

PT :- TRANSPOSITION CIPHER
fill row wise
T R A N
S P O S
I T I O
N C I P
H E R X (if empty space left).

CT :- T S I N H R P T C E A O I I R N S O P X

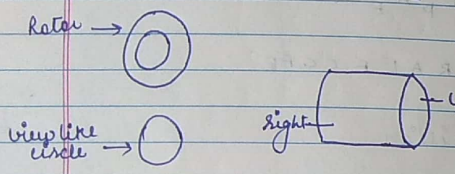
key value may or may not be given.

Read column^ wise (1st column + 2nd column + ...)

key value given : 1432 (divide into 4 column). first read 1 column then 4 column then 3 column then 2 column.

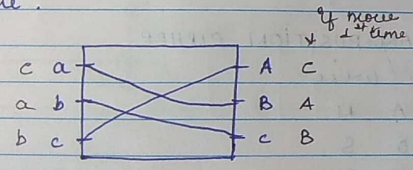
key value given : 143265 (divide into 6 column).

7- ROTOR CIPHER [substitution cipher].

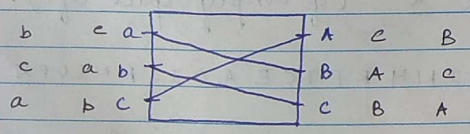


Some alphabets are written on L.H.S and R.H.S

L.H.S & R.H.S points are connected with some wire.



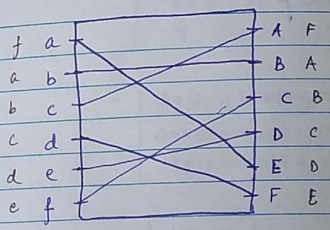
Rotor move → wire stationary.



PT → B C A.
CT → a b c.

PT → 1st alphabet → stationary position
2nd alphabet → 1st moving position
3rd alphabet → 2nd moving position

No. of rotation = Plain Text length - 1

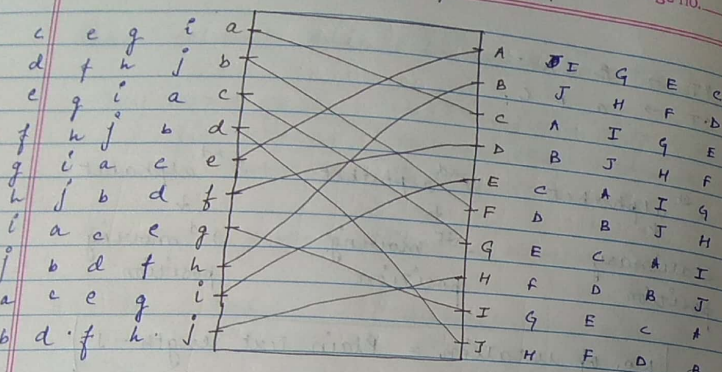


PT = B E E (rotor stationary).
CT = b a a

• if rotor moves.

PT = B E E.
CT = b C a

at time moves 2 position.



D E H I B

f a d c f.

Date.
Page No.

HILL CIPHER.

$$K = \begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix}$$

PT = CRYPTOGRAPHY

Ans:- GDAVHHGNSXRZ

PT = CRYPTOGRAPHY (15, 19, 14)

$$CT_2 = \begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix} \begin{bmatrix} 15 \\ 19 \\ 14 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 3*15 + 10*19 + 20*14 \\ 20*15 + 9*19 + 17*14 \\ 9*15 + 4*19 + 17*14 \end{bmatrix} = \begin{bmatrix} 45 + 190 + 280 \\ 300 + 171 + 323 \\ 135 + 76 + 238 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 6515 \\ 709 \\ 449 \end{bmatrix} \bmod 26 = \begin{bmatrix} 21 \\ 7 \\ 7 \end{bmatrix} \begin{matrix} V \\ H \\ H. \end{matrix}$$

$$PT_1 = [K^{-1} \times CT_1] \bmod 26$$

K^{-1} = transpose of cofactor of K.

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

$3 \bmod 26 = 3$

$3^2 \bmod 26 = 9$.

Date.
Page No.

$$|K| = 3(9*17 - 17*4) - 10(20*17 - 9*17) + 20(20*4 - 9*3)$$
$$= 255 - 1870 - 20.$$
$$= -1635$$

$$K = \begin{bmatrix} + & - & + \\ - & + & - \\ + & - & + \end{bmatrix} \begin{bmatrix} (9*17 - 17*4) & (20*17 - 9*17) & (20*4 - 9*3) \\ (10*17 - 20*4) & (3*17 - 20*9) & (3*4 - 9*10) \\ (10*17 - 20*9) & (3*17 - 20*20) & (3*9 - 20*10) \end{bmatrix}$$

$$= \frac{1}{-1635} \begin{bmatrix} 85 & -187 & -1 \\ -90 & -129 & +78 \\ -10 & +349 & -173 \end{bmatrix}$$

$$= \frac{1}{3} \Rightarrow 3^{-1} = 9.$$

$26 - 1635 \bmod 26.$

$3 \bmod 26 \Rightarrow 3.$

Date.
Page No.

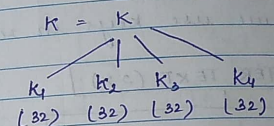
FIESTAL NETWORK (CIPHER)

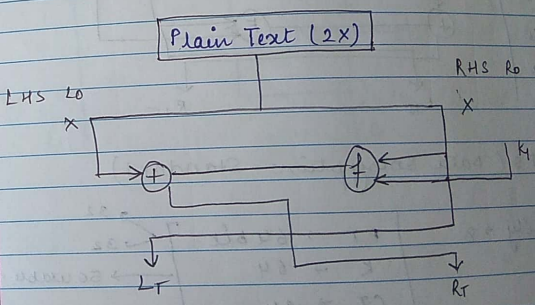
Block cipher peform operation on 32 bit or on multiple of 32.

Symmetric structure works on block cipher.

PT = 32, 64, 128 .....

CT = 16, 32, 64, ...





$L_i = R_{i-1}$

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

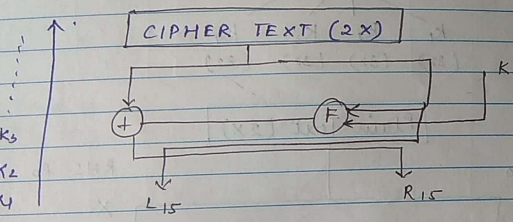
Date.
Page No.

Efficiency of algo

- secure but more time complexity
- selection of p.t
- function (should be strong)
- sub key generation algo.
- No. of rounds.

Decryption

- Same but we use keys in reverse order.



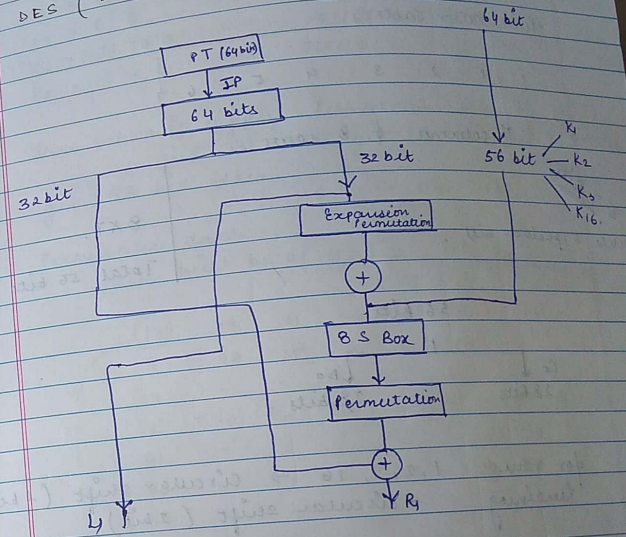
→ DES (Data Encryption Standard)

Parity → 8

PT → 64 bit
K → 64
CT → 64

→ 32
→ 32
→ 56 usable → 48 for every round.

DES (Data Encryption Standard)



K = 64 bits

• Permutation Table.

1 2 3 4 5 6 7

7 column & 8 rows.

8 × 7.

Total 56 bits

5^7 bits.

(while 57 position bit).

56 Bits

C0 → 28 Bits

D0 → 28 bits

for round 1, 2, 9, 16 → circular shift (1 bit)

Remaining → circular shift (2 bit).

K = 64 bits

↓

K⁺ = 56 bit

C0 = 1100 11 - - - - - 10.

D0 = 0101 0 - - - - - - 01

C1 = 1001 1 - - - - - 101

D1 = 1010 - - - - - - - 010.] K⁺.

Similary C2 & D2.

C2 = 0011 - - - - - - - 1011]

D2 = 010 - - - - - - - 0100.] K2⁺

C3 = 11 - - - - - - - 101100.]

D3 = 0 - - - - - - - - - 010001] K3⁺

Then we will apply Permutation Table on K1⁺, K2⁺ ..... and we will get 16 round and get 48 bit data.

Permutation Table.

table will be of 48 bits

combination of C0D0

14	17	11	24	1	5
3	28	15	6	21	10
23	-	-	-	-	-
16	-	-	-	-	-
41	-	-	-	-	-
30	-	-	-	-	-
44	-	-	-	-	-
46	-	-	-	-	-

14th bit position 17th bit position 11th 24th 1st 5th.

• S Box.

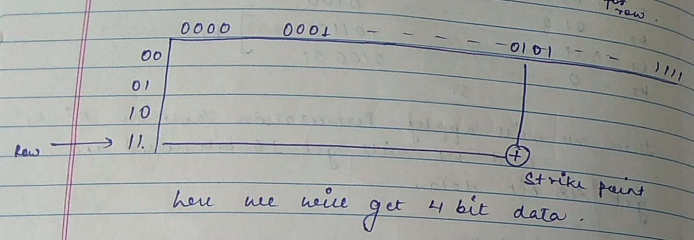
48 bit data → 1 0 1 0 1 1 | 0 1 1 1 0 1 1 - - - - - - -

S1 S2

for 1st six bit → S box 1.

Date. Page No.

Total 8 S boxes.



here we will get 4 bit data.

Total 32 bit

- Initial Permutation

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16

(8×8) 64 bit

Select even column & write in reverse order.

58 . . . . . 2 → 0
. 4
. . . . . 6.
. . . . . 8.

Date. Page No.

Then select odd column

57 . . . . . 1 → 40
. 3
. 5
. . . . . 7.

40 8 . . . .
. . . . .
. . . . .

} Check the shifted position from initial data

2 DES

Here we have 2 keys.

$$CT = E_{K_2}(E_{K_1}(P))$$

and we decrypt we use the keys in same order.

$$PT = D_{K_1}[D_{K_2}(C)]$$

- more security but more complex.

3 DES.

It works with both 2 keys & 3 keys.

$$CT = E_{K_3}\left(D_{K_2}\left(\left(E_{K_1}(P)\right)\right)\right)$$

↳ with 3 key.

$$CT = E_{K_1}\left(D_{K_2}\left(\left(E_{K_1}(P)\right)\right)\right)$$

↳ with 2 key.

Limitation :-

block size remain 64 bit always.

AES (Advance Encryption Standard).

Data block - 128 bits (PT).

Key → variable length (128 bit, 192 bit, 256 bit).

No. of round →

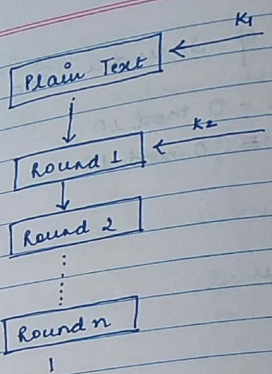
128 bit key → 10.

192 → 12.

256 → 14.

sub key / Round key = 128 bit.

Total subkey = No. of Round + 1



- Set of Residue (Z_n)

$Z_n = \{0, 1, 2 \ldots\ldots (n-1)\}$

$Z_3 = \{0, 1, 2\}$

used in modular arthimatic in generation of public key cryptography.

- Additive Inverse

If there are two no. a & b then a, b under Z_n.

$$a + b \equiv 0 \bmod n$$

$$(a+b) \bmod n = 0 \bmod n$$

Date.
Page No.

• Additive inverse of 3 under Z_{10}

$(a+b) \bmod n = 0 \bmod 10$

$3+b \equiv 0 \bmod 10$

$\downarrow$

7

• Multiplicative Inverse.

a, b, Z_n

if they follow

$\boxed{a \times b \equiv 1 \bmod n}$

$\boxed{(a \times b) \bmod 10 = 1 \bmod 10}$

⇒ for $Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

$3 \times b \equiv 1 \bmod 10$

$\Downarrow$

7

⇒ find all multiplicative inverse of 7 under Z_{10}.

$7 \times b \equiv 1 \bmod 10$

$\downarrow$

3

Date.
Page No.

Euclidean Algo

• Extended Euclidean Algorithm.

Simple Euclidean algo finds GCD of two numbers.

→ find multiplicative inverse of 13 in Z_{20}

13 Z_{20}

$\downarrow$ $\downarrow$

a n.

Step 1: $r_1 \leftarrow n$.
$r_2 \leftarrow a$

Step 2: $t_1 \leftarrow 0$, $t_2 \leftarrow 1$.

Step 3: while $(r_2 > 0)$

{

$q \leftarrow r_1 / r_2$.

$r \leftarrow r_1 - q\, r_2$

$t \leftarrow t_1 - q\, t_2$

$r_1 \leftarrow r_2$

$r_2 \leftarrow r$

$t_2 \leftarrow t$

$t_1 \leftarrow t_2$

}

q	r_1	r_2	r	t_1	t_2	t
1	20	13	7	0	1	-1
1	13	7	6	1	-1	2
1	7	6	1	-1	2	-3
6	6	1	0	2	-3	20
	1	0		-3	20	

Step 4:- $a^{-1} = t_1$

(Here $t_1 = -3$)

$-3 \bmod 20 = 20 - 3 \bmod 20 = 17$.

7 is multiplicative inverse of Z_{20}.

Verification :- $\frac{13 * 17}{20} = \frac{221}{20} = \boxed{1}$

if we divide algo into two parts

Euclidian Algo :-

q	r_1	r_2	r	t_1	t_2	t

:- find multiplicative inverse of 11 under Z_{26} using extended euclidean algo.

q	r_1	r_2	r	t_1	t_2	t
2	26	11	4	0	1	-2
2	11	4	3	1	-2	5
1	4	3	1	-2	5	-7
3	3	1	0	5	-7	26
	1	0		-7	26	
		x				

$5 - 3*1$
$5 * 21$
$-2 - 5$
$-2 - 1*5$
$26 - 2*11$
$26 - 22$
$0 - 2*1$
$11 - 2*4$
$11 - 8$
$1 - 2*(-2)$
$1 + 4$

5 mod 26 = .

$a^{-1} = 9 - 7$.

$-7 \bmod 26 = 26 - 7 \bmod 26$
$= 19 \bmod 26$

Verify :- $\frac{19 * 11}{26} = 1$ Rem

we cannot find 12 in Z_{26} (condition both should be co-prime).

• using Euler Totient.

$11^{-1} \bmod 26$.

$= 11^{\phi(26)-1} \bmod 26$.

$\phi(26) = 13 * 2$.
$= 12 * 1$

$= 11^{11} \bmod 26$

$= \{(11^4 \bmod 26) \cdot (11^4 \bmod 26) \cdot (11^2 \bmod 26) \cdot (11 \bmod 26)\} \bmod 26$

$= (9 * 17 * 11) \bmod 26$

$=$

• $29^{-1} \bmod 80$.

q	r_1	r_2	r	t_1	t_2	t
2	80	29	22	0	1	-2
1	29	22	7	1	-2	3
3	22	7	1	-2	3	-11
7	7	1	0	3	-11	80
	1	0		-11	80	

$-11 \bmod 80 = \frac{80}{26} - 11 \bmod 80$.

$= 69 \bmod 26$

$= \frac{69 * 29}{80}$

ASSIGNMENT-1

1. What are different security services and security mechanisms that ensures security?
2. Explain different types of modes of operation of block cipher.
3. Differentiated b/w :- i) cryptography and steganography
   ii) Block cipher and stream cipher
   iii) confusion and diffusion -

FERMAT'S THEOREM (fermat's little theorem)

i) p → prime no. & a → +ve integer
& p doesn't divide a
then $\boxed{a^{p-1} \equiv 1 \bmod p}$

$a^{p-1} \bmod p = 1 \bmod p$.

ii) p → prime no. & a → +ve integer.

$\boxed{a^p \equiv a \bmod p}$

iii) p - prime no. & a → +ve integer.

$\boxed{a^{p-2} = a^{-1} \bmod p}$

• $3^{10} \bmod 11$.
(a, p)

$3^{11-1} \bmod 11 = 1 \bmod 11$
$= 1$ //.

• $3^{12} \bmod 11$.
(a, p)

$3^{11} \bmod 11$

Date.
Page No.

By first condition:-

$= (3^{10} \bmod 11 \cdot 3^2 \bmod 11) \bmod 11$.

$= (1 \cdot 9) \bmod 11$

$= 9 \bmod 11 = 9$.

By second condition

$(3^{11} \bmod 11 \cdot 3 \bmod 11) \bmod 11$.

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

$= 9 \bmod 11 = 9$.

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

$= 7^{13-2} \bmod 13$

$= 7^{11} \bmod 13$.

=

Euler's Theorem

a and n are positive integers.

then $\boxed{a^{\phi(n)} \equiv 1 \bmod n}$

- Not applied on prime no.

$\boxed{a^{\phi(n)-1} \equiv a^{-1} \bmod n}$

- $6^{24} \bmod 35$

$6^{\phi(35)} \bmod 35$

$= 01$

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

$= 24$

Date.
Page No.

- $20^{62} \bmod 77$

$20^{\phi(77)} \bmod 77$

$= 20^{60} \bmod 77 \cdot 20^{2} \bmod 77$

$= 1 \cdot 400 \bmod 77$

$= 400 \bmod 77 = 15$

$\phi(77) = \phi(11) * \phi(7)$

$= 10 * 6$

$= 60$

- $7^{222} \bmod 10$

$7^{\phi(10)} \bmod 10$.

$= 7^{4} \bmod 10 \cdot 7^{218} \bmod 10$.

$= \{[7^4 \bmod 10]^{55} \quad 7^2 \bmod 10]\} \bmod 10$.

$= [7^2 \bmod 10] \bmod 10$.

$\Rightarrow 9 \bmod 10 = 9$

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

$= 4 * 1$

$= 4$

55
4 | 222
53

55 * 4 = 220

- $10^{18} \bmod 19$

$10^{\phi(19-1)}$.

$= 10^{1} \bmod 19$

$= 19 - 10 \bmod 19$

$= 9 \bmod 19 = 9$.

$= 10^{19-1} \bmod 19$.

$= 1 \bmod 19$

$= 1$