INDEX

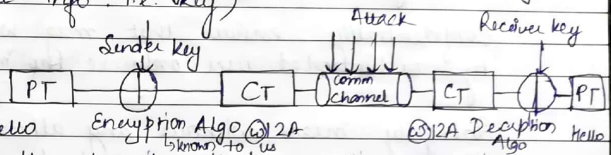
NAME: ADITI STD.: CSE SEC.: E ROLL NO.: 12 SUB.: Cryptography

S. No.	Date	Title	Page No.	Teacher's Sign / Remarks

Two types of text is used:
Plain text: Original message from the sender side.

Cipher text: Coded message.

From the sender side plain text is converted into cipher text by using some operation (i.e. adding of additional info. i.e. key)



- Most of the security attacks are via communication channel. Comm. channel is made secure by using keys & algo(s)

On the receiver side, Cipher text is received. At the receiptent end, key is added, (decription algo)
↳ known to us

Basic components of Cyptography

1. Plain Text
2. Cipher Text
3. key
4. Enkryption Algo
5. Decryption Algo

Cyptography

Every user has the public key of other users

↓

Symmetric key cyptography
→ If key 1 = key 2; i.e. key for encryption & decryption algo is same.

↓

Asymetric key cyptography
If key 1 != key 2.

CIA ~~Traid~~ Traid

→ Confidentiality
→ Integrity
→ Availability

} Balance of these will lead to a correct cryptographic mechanism.

We have to ensure them and then we provide security, when we use.

- Confidentiality ensures that msg will be received by authenticated user only. i.e. the intended user.
- Integrity means without any alteration or modification the message sent is received.
- Message availability is not affected, even if we apply key value to it or by order in which it does not affect it. It is available in the correct form whenever required.

Authentication: Whether the user logged in is valid or not. It checks user credentials.
Ex: G-mail.

Authorization: Access - limitation.
Ex: SAP → different users: faculty, librarian, student
Authorization level defined is different. Permission is granted a/c to the levels once authentication is done.

Authorization is followed by Authentication.

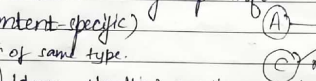
Attacks

1. Active: They read the data and modify it and then transmit it.

2. Passive: Attackers aims to gain user info. from the data. They do not modify the data. Read the data only. This is known as message reception.

Indirect: org emp info $\xrightarrow{\text{retrieve}}$ convince emp.

Attacker fetches same content ← (content-specific) or of same type.



(Address-specific): When contacted to a single user. Attacker receive data from same address

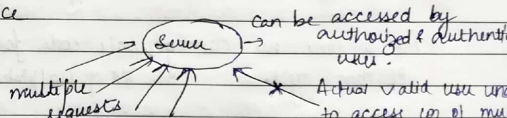
Attack

Confidentiality → message reception → Info gain.

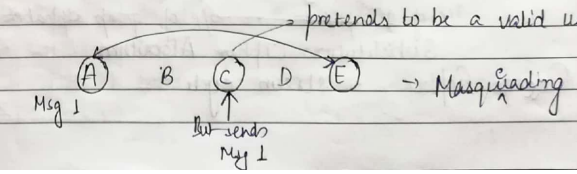
Integrity Attack
(i) Modification
(ii) Masquerading: When attacker pretends to be a valid us

Repudition: Authenticated parties are pretending as attack
Someone sends a msg & denies later → sender side
Someone receives a msg & denies later → recipient side.
To control this we have certification authority

Availability attack
Denial of Service
↳ Single user cannot access



Distributed Denial of Service Attack: When multiple users cannot access.



Before cryptography, compression of messages were done which may or may not be password protected.

- Lossly (info is lost) → no critical info
- Lossless (no info is lost) → critical info

Size depends on Algo.

- fast compression
- Multiple compression

Symmetric key Algo.

Category
1. Substitution Cipher
2. Transposition Cipher.

1. Alphabets in original message are replaced using other alphabets. This is done using key. key is mandatory.
2. In this case, shuffling of message's characters is done. key is not mandatory.

At a time, we can generate code for one alphabet → Stream-cycle. i/p of 1 alphabet → o/p of 1 alphabet

At a time, we can generate code for multiple (group) of alphabets → block-cycle.

i/p of group alphabet → o/p of group alphabet

Substitution Cipher Algorithm

1. Caesar Cipher - stream cycle

Caesar cipher was used ~~using~~ during World-War.
This is applicable only on alphabets.

We associate reference number to the Alphabets

A - 0
B - 1
⋮
Z - 25

$$CT = (PT+3) \bmod 26.$$

Encrypt:

A = $CT_1 = (0+3) \bmod 26 = 3$ - D
B = $CT_2 = (1+3) \bmod 26 = 4$ - E
C = $CT_3 = (2+3) \bmod 26 = 5$ - F

- key has to be chosen in such a way, that both parties agree to same number. But value has to be 0-25. It was easy to attack, since we can use hit & trial $CT = (PT+k) \bmod 26$; it was made generalized to overcome attack but it didn't help Decryption (∵ 0-25 hit & trials)

Decrypt → $PT_1 = CT_1 - 3 \bmod 26 = 0$ A
$PT_2 = CT_2 - 3 \bmod 26 = 1$ B
$PT_3 = CT_3 - 3 \bmod 26 = 2$ C.

Q: PT = CEASER K = 3
CT = (PT+3) mod 26 = FIDVIU Encryption

PT = (CT-3) mod 26 = CEASER Decryption

Cryptography is a mecanism through which message is sent from sender to receiver via a channel i.e. comm. channel & it has to be secure. For securing it, we have different methods.

Confidentiality : No modification of message
1. Reception 2. Traffic analysis (Address-specific)
(content specific) ↳ Competative org. contact to which org.
↳check the type of content send
Integrity : Eg msg ko bar bar send karna agar benefit ke liye
1. Modification 2. Masquerading 3. Re-playing : multiple request send karna who is authenticated
4. Repudition : Single side works as attacker.

Availability :
1. Denial of Service.

In Symmetric Cipher → key
" Assymetric Cipher → public key & private key.

To counter the attacks - we study algo(s)

2. Playfair cipher - block-cycle
• Works only on alphabets.
PT= PLAYFAIR
Key = CRYPTO

Make a block of 5 row + 5 col ~~of key~~

Start from this corner

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

• Assumption : I & J will occur at same place. (I/J)

• Now we do pairing of plain text (PLAYFAIR)
• If we have single alphabet at the end.
Ex: Y
We add filler alphabet YX.
• BALNOON BALLOON
BALXLOON
↓
filler alphabet

In PLAYFAIR CIPHER
Assumption : • I & J occur at same place
• Filler Alphabet → X
• No alphabet is repeated
Ex: key : BALLOON

B	A	L	O	N

case: Same Column
Suppose we have EK as pair
EK → KS (Next alphabet in the same col)
SZ → ZT (Next alphabet in same col)
↑ circular shift

case: Same row
AD → BE (Next alphabet in same row)
DE → EO (" ")
↑ circular shift

case : Different row & Different column

AQ – DM

for A
Move to row of A & col of Q → D (strike point)

for D
Move to row of D & col of A → M

NOW PL AY PA IR

PL → CQ
AY → BR
PA → QO
IR → GP

limitations :

1. I & J can occur together
2. X is taken as filler alphabet but it can occur as normal alphabet
3. Works only on alphabets, no numerals entry.

for improvement in Playfair cipher

- We use a block of 7 × 4
- We used * , #
  - * → for pairing with single alphabet (Y*)
  - # → filler alphabet b/w same alphabets (L#L)

→ Remove dependencies of X as filler alphabet
→ It only solved I&J problem.
→ No numerals allowed.
NOW, we used 6×6 block.

→ 26 → alphabets
→ 0–9 → numbers
→ Can use upper / lower case one at a time
→ Again same the dependency to take filler alphabet
→ No special symbol

Finally, the correct solution was 16 × 16.

Q: PT – COMPUTER SCIENCE
KEY – DITU

CO MP UT ER SC IE NC EX
BP KR AU FQ PG TC KG LT

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

Indexing

A – 0	J – 9	S – 18
B – 1	K – 10	T – 19
C – 2	L – 11	U – 20
D – 3	M – 12	V – 21
E – 4	N – 13	W – 22
F – 5	O – 14	X – 23
G – 6	P – 15	Y – 24
H – 7	Q – 16	Z – 25
I – 8	R – 17	

Q: PT - NETWORK KEY: SECURITY

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

NE TW OR KX
MC YV PU HZ

Decryption: NETWORKX

Rules for Decryption in Playfair Cipher
1. Same row: Previous alphabet in the same row
2. Same column: Previous alphabet in the same column.
3. Different: Same as encryption rule.

3. AFFINE CIPHER

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

Condition to be followed
- A and 26 has to be co-prime.
A acts as a multiplicative key
B acts a a additive key.

Q: PT = AFFINE CIPHER, A = 5, B = 8.

PT = A F F I N E C I P H E R
(0) (5) (5) (8) (13) (4) (2) (8) (15) (7) (4) (17)
(PA+B) 8 33 33 48 73 28 18 48 83 43 28 93
1 PA+B = 0×5+8 = 8
2 PA+B = 5×5+8 = 33

(PA+B) mod 26 = 8 7 7 22 21 2 18 22 5 17 2 15

cr IHHNVCSNERCP

If in Affine cipher A = 1, then it is generalized caesar cipher.

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

To find multiplicative inverse, one condition must be followed

$A \cdot A^{-1} = 1 \bmod 26$

We can use different methods :-

(i) Hit and Trial

$5 \times A^{-1} = 1 \bmod 26$
$5 \times 21 = 1 \bmod 26$
$(105) \rightarrow 86 \times 4 = 104$

(ii) Euler Totient function (ϕ)
$\phi(P) = P-1$, where P is a prime number.
$\phi(3) = 3-1 = 2$
$\phi(6) = \phi(3) \times \phi(2) = 2 \times 1 = 2$

- It should be broken into distinct prime no(s).
∴, Generalized case = $\phi(m)\phi(n) = (m-1)(n-1)$

$\phi(8) = \phi(2)^3 = 2^3 - 2^2 = 8-4 = 4$.
[Meaning there are 4 co-primes of 8 less than 8 1, 3, 5, 7]

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

$\phi(1) = 0$

Q: $\phi(120) = \phi(30) \times \phi(40) = \phi(60)$.

$120 = 8 \cdot 15 \cdot 1 = 2 \times 2 \times 5 \times 2 \times 2 \times 2 \times 5 = 2 \times 2 \times 2 \times 3 \times 5$
$\phi(120) = \phi(3) \times \phi(5)^2 \times \phi(2)^3$
$= 2 \times 4 \times (8-4) = 2 \times 4 \times 4 = 16 \times 2 = 32$

Equivalent → $A^{-1} \bmod M$
$A^{\phi(M)-1} \bmod M$

$5^{-1} \bmod 26$. [A^{-1} & M should be co-prime]

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

$\phi(26) = \phi(2) \times \phi(13) = 1 \times 12 = 12$

$5^{12-1} \bmod 26 = 5^{11} \bmod 26$. → Now to solve this we use repetative square method.

$5 \bmod 26 = 5$
$5^2 \bmod 26 = 25$
$5^4 \bmod 26 = (5^2 \bmod 26 \times 5^2 \bmod 26) \bmod 26$
$= (25 \times 25) \bmod 26 = 625 \bmod 26$
$= 1$

$5^{11} \bmod 26 = (5^4 \bmod 26 \times 5^4 \bmod 26 \times 5^2 \bmod 26 \times 5 \bmod 26) \bmod 26$

~~$= (21 \times 21 \times 25 \times 5) \bmod 26$~~
~~$= (441 \times 125)$~~

$= (1 \times 1 \times 25 \times 5) \bmod 26 = 125 \bmod 26$
$= 21.$

for I
$PT = 21\ (8-8) \bmod 26 = 0 = A$

for H
$PT = 21\ (7-8) \bmod 26 = -21 \bmod 26$
$= 26 - 21 \bmod 26$
$= 5 \bmod 26 = 5.$

$-A \bmod M \Rightarrow M - A \bmod M.$

Symmetric cipher

SUBSTITUTION CIPHER
- Caesar - Generalized caesar - Playfair - Affine
- Vigenere cipher - Vernam cipher

4. VIGENERE CIPHER - stream cycle

PT = XYZABCDEF
key = DITU

→ We expand key length to the PT length with repetation of alphabets of key.

X	Y	Z	A	B	C	D	E	F
D	I	T	U	D	I	T	U	D
CT: A	G	S	U	E	K	W	Y	I

$CT_1 = (PT_1 + K_1) \bmod 26$
$= (23 + 3) \bmod 26 = 0 = A$

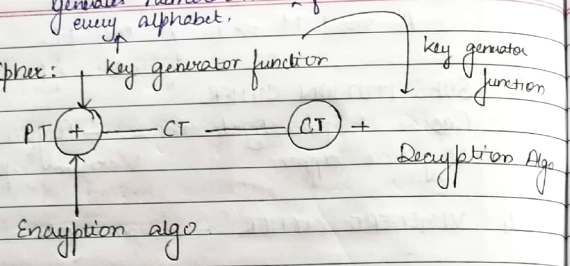
$CT_2 = (PT_2 + K_2) \bmod 26 = (24 + 8) \bmod 26 = 32 \bmod 26 = 6$
$= G$

$CT_3 = (25 + 19) \bmod 26 = 44 \bmod 26 = 18 = S$
$PT_1 = (CT_1 - K_1) \bmod 26 = (0 - 3) \bmod 26 = 23$
$CT_4 = (0 + 20) \bmod 26 = 20 = U.$

Monoalphabatic cycle: for same alphabets, the cipher text generated remains the same.
Ex: Caesar

Polyalphabatic: for same alphabets, the cipher text generated can change. For a particular alphabet, the cipher text will vary.

5. VERNAM Cipher: 'key' generates numerical value for every alphabet.



PT = X Y Z A B C D E F
24 25 26 1 2 3 4 5 6

$CT_1 = (PT + k) \bmod 26$
$= (X + 18) \bmod 26 = (23 + 18) \bmod 26 = P$

$PT_1 = (CT_1 - K) \bmod 26$

- key also work in reverse order (decryption) i.e. the same key is used.

Q: Solve using Affine Cipher.

PT = PLAYFAIR, A = 5, B = 8.
A and 26 = co-prime

	P	L	A	Y	F	A	I	R
	(15)	(11)	(0)	(24)	(5)	(0)	(8)	(17)
(PA+B)	83	63	8	128	33	8	48	93
(PA+B) mod 26	5	11	8	24	7	8	22	15
CT =	F	L	I	Y	H	I	W	P

Decryption: $I = A^{-1} (C - B) \bmod 26$,

$A^{\phi(26)-1} \bmod 26$

$\phi(26) = \phi(2) \times \phi(13) = 1 \times 12 = 12$

$5^{12-1} \bmod 26$.

$5 \bmod 26 = 5$
$5^2 \bmod 26 = 25$
$5^4 \bmod 26 = (25 \times 25) \bmod 26 = 625 \bmod 26 = 1$

$5^{11} \bmod 26 = 1 \times 1 \times 25 \times 5 = 125 \bmod 26 = 21$.

$P = 21 (C - B) \bmod 26$.

Q: Solve using Affine Cipher
CT = HPCCXAQ, A = 5, B = 8

CT = H P C C X A Q
7 15 2 2 23 0 16

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

$A^{\phi(26)-1} \bmod 26 = 21 = 5^{11} \bmod 26$.

$PT_1 = 21 (7 - 8) \bmod 26 = -21 \bmod 26 = 5$ F

$PT_2 = 21 (15 - 8) \bmod 26 = 147 \bmod 26 = 17$ R

$PT_3 = 21 (2 - 8) \bmod 26 = 4$ E
$PT_4 = 4$ E
$PT_5 = 21 (23 - 8) \bmod 26 = 315 \bmod 26 = 3$ D

$PT_6 = 21 (0 - 8) \bmod 26 = -168 \bmod 26 = 14$ O
$PT_7 = 21 (8) \bmod 26 = 12$ M

6. HILL cipher. - Block-cycle
(Used any filler)

Key is in the form of square matrix NXN.

PT has to be broken in the form NX1.

$$CT = KP \bmod 26.$$

$$\begin{bmatrix} CT_1 \\ CT_2 \\ CT_3 \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \\ P_3 \end{bmatrix} \bmod 26$$

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

Q: $K = \begin{bmatrix} 2 & 3 \\ 6 & 7 \end{bmatrix}_{2\times2}$, PT = NO ANSWER

PT = NO ANSWER

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

$$= \begin{bmatrix} 2 & 3 \\ 6 & 7 \end{bmatrix}_{2\times2} \begin{bmatrix} 13 \\ 14 \end{bmatrix}_{2\times1} \bmod 26 = \begin{bmatrix} 26+28 & 39+42 \\ 78+91 & 91+98 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 54 & 81 \\ 169 & 189 \end{bmatrix} \bmod 26 = \begin{bmatrix} 54+42 \\ 78+98 \end{bmatrix} \bmod 26 = \begin{bmatrix} 96 \\ 176 \end{bmatrix} \bmod 26$$

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

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

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

$39 - 26 = 13$

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

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

$$= \begin{bmatrix} 2 & 3 \\ 6 & 7 \end{bmatrix} \begin{bmatrix} 18 \\ 22 \end{bmatrix} \bmod 26 = \begin{bmatrix} 36+66 \\ 108+154 \end{bmatrix} = \begin{bmatrix} 102 \\ 262 \end{bmatrix} \bmod 26$$

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

$$CT_4 = \begin{bmatrix} 2 & 3 \\ 6 & 7 \end{bmatrix} \begin{bmatrix} E \\ R \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 2 & 1 \\ 6 & 7 \end{bmatrix} \begin{bmatrix} 4 \\ 17 \end{bmatrix} \bmod 26 = \begin{bmatrix} 8+51 \\ 24+119 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 59 \\ 143 \end{bmatrix} \bmod 26 = \begin{bmatrix} 7 \\ 13 \end{bmatrix} = \begin{bmatrix} H \\ N \end{bmatrix}$$

Polyalphabatic cipher cuz one PT has diffuent CT

N → Q

& N → N.

Q: CT = QV NA YQ HI

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

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

$$\begin{bmatrix} P1 \\ P2 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 7 & 8 \end{bmatrix}^{-1} \begin{bmatrix} Q \\ V \end{bmatrix} \bmod 26$$

While finding inverse,
we cannot have fractional values
we cannot have negative values

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

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

$$= \frac{1}{16-21} \begin{bmatrix} 8 & -3 \\ -7 & 2 \end{bmatrix} \begin{bmatrix} 16 \\ 21 \end{bmatrix} \bmod 26$$

$$= \frac{1}{-5} \begin{bmatrix} 8 & -3 \\ -7 & 2 \end{bmatrix} \begin{bmatrix} 16 \\ 21 \end{bmatrix} \bmod 26$$

$$= \frac{1}{-5} \begin{bmatrix} 128-63 \\ -112+42 \end{bmatrix} \bmod 26$$

$$= \frac{-1}{5} \begin{bmatrix} 65 \\ 70 \end{bmatrix} = \begin{matrix} -13 \\ -14 \end{matrix}$$

$$K^{-1} = \frac{1}{16-21} \begin{bmatrix} 8 & -3 \\ -7 & 2 \end{bmatrix} \bmod 26 = \frac{1}{-5} \begin{bmatrix} 8 & -3 \\ -7 & 2 \end{bmatrix} \bmod 26$$

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

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

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

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

$$= \begin{bmatrix} -168 & 63 \\ 147 & -42 \end{bmatrix} \bmod 26 = \begin{bmatrix} 14 & 11 \\ 17 & 10 \end{bmatrix}$$

$$-168 \bmod 26 = 26 - 168 \bmod 26 = 26 - 12 = 14$$

$$\begin{bmatrix} P1 \\ P2 \end{bmatrix} = \begin{bmatrix} 14 & 11 \\ 17 & 10 \end{bmatrix} \begin{bmatrix} 16 \\ 21 \end{bmatrix} \bmod 26.$$

Solvable only when :-
- $K \cdot K^{-1} \bmod 26 =$ Identity matrix

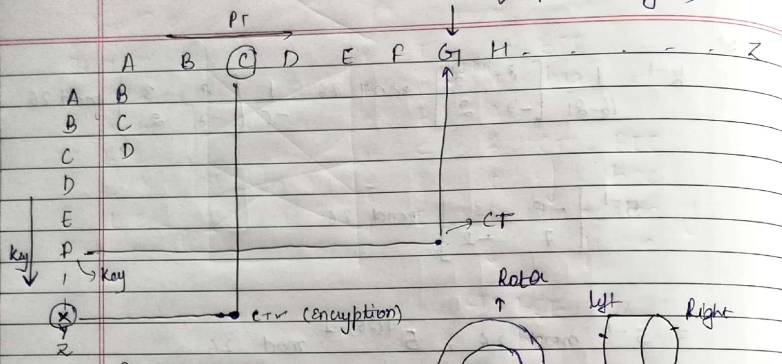
7. VIGENERE SQUARE:

A B C D . . . . Z

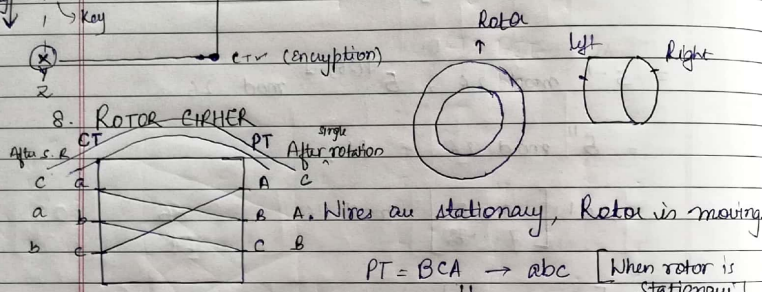
PT = CRYPTO, KEY = XYZ

XYZXYZ

Decryption case:
PT (of cipher text is given)



8. ROTOR CIPHER



A, Wires are stationary, Rotor is moving.

PT = BCA → abc [When rotor is stationary]

⇓

When rotor is moving,

1st alphabet CT will be generated from stationary position
2nd " CT " " b " single rotation
3rd " " " " c " after 2nd rotation.

Also, we have to keep in mind, how many position it is rotating.

No. of rotation = length of PT − 1.

Transposition Cipher

(i) Rail fence cipher: Plain text has to be written in zig-zag form. Depth will be given to us. → Kitne rows me plain text organize karna hai
Multiple row. Jaun

PT: RAIL FENCE CIPHER

① → R I F N E I H R
② → A L E C C P E

CT: RIFNEIHRALECCPE.

(ii) Columnar Transposition:

PT: TRANSPOSITION CIPHER

Case 1: Enter value = 4 → No. of columns used.

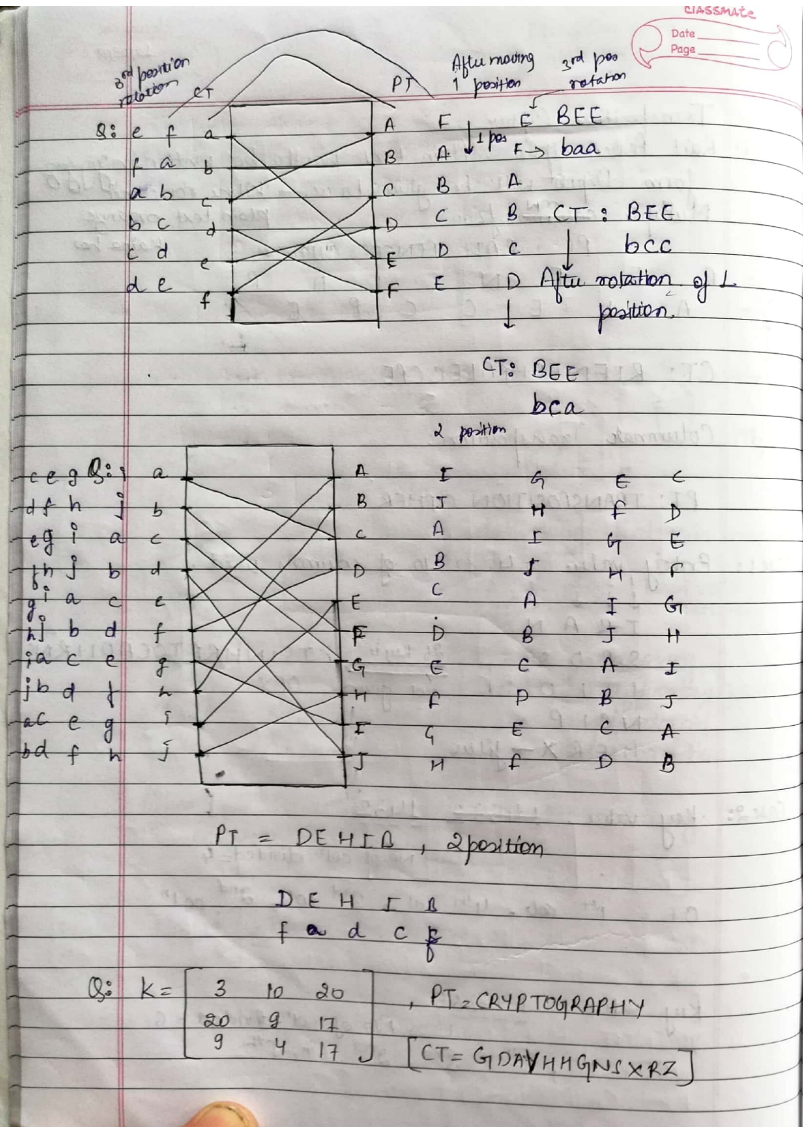
1 2 3 4
↓ ↓ ↓ ↓
T R A N
S P O S
I T I O
N C I P
H E R X → fillr

If key is not given → TSINHRPTCEAOIIRNS OPX

Case 2: Key value: 14532 (1432)
↓
No. of coln divided = 4

CT = 1st col, 4th col, 3rd col, 2nd coln.

Key value: 143265
↳ No of coln divided = 6
CT: 1st, 4th, 3rd, 2nd, 6th, 5th



PT = DEHIB , 2position

D E H I B
f a d c f

Q: $K = \begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix}$, PT = CRYPTOGRAPHY

CT = GDAVHHGNSXRZ

3×1 PT = CRY PTO GRA PHY

$CT_2 = K\ P \mod 26$

$C = \begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix}_{3\times3} \begin{bmatrix} 15 \\ 19 \\ 14 \end{bmatrix}_{3\times1} \mod 26$

$= \begin{bmatrix} 45+190+280 \\ 300+171+238 \\ 135+76+238 \end{bmatrix} \mod 26 = \begin{bmatrix} 515 \\ 709 \\ 449 \end{bmatrix} \mod 26 = \begin{bmatrix} 21 \\ 7 \\ 7 \end{bmatrix}$

$= \begin{bmatrix} V \\ H \\ H \end{bmatrix}$

$PT = [K^{-1} \times CT] \mod 26$

$K^{-1} = \frac{1}{|K|} Adj\ K$ — Adj K → create co-factor matrix → transpose it

$|K| = 3[(9\times17) - 17\times4] - 10[(20\times17 - 9\times17) + 20(20\times4 - 81)$

$= 3[153 - 68] - 10(340 - 153) + 20(80 - 81)$

$= 3[85] - 10(187) + 20(-1)$

$= 255 - 1870 - 20 = 255 - 1890 = -1635$

$= 3(153 - 68) - 10(340 - 153) + 20(-1)$

$= (3 \times 85) - 10(187) - 20 = -1870 - 20 + 255$

$= -1635$

Co-factor matrix

$$\begin{bmatrix} (9\times17-17\times4) & -(20\times17-17\times9) & +(20\times4-9\times9) \\ -(10\times17-20\times4) & -(3\times17-20\times9) & +(3\times4-9\times10) \\ +(10\times17-20\times9) & -(3\times17-20\times10) & +(3\times9-20\times10) \end{bmatrix}$$

$-1635 \mod 26$

$26 - 1635 \mod 26 = -23$

$26 - 23 \mod 26 = 3$

$$k^{-1} = \frac{1}{3}\begin{bmatrix} & & \\ & & \\ & & \end{bmatrix} = 3^{-1}\begin{bmatrix} \cdot & & \\ & & \\ & & \end{bmatrix} \mod 26$$

$3^{-1} \mod 26 = 9$ (Using Euler's totient).

$k^{-1} = 9$

FIESTAL NETWORK C CIPHER

→ Shuffling of bits.

→ Performs operation on multiple of 32 bits - 32, 64, 128 bits etc.

→ It is a symmetric structure, that works on block cipher.

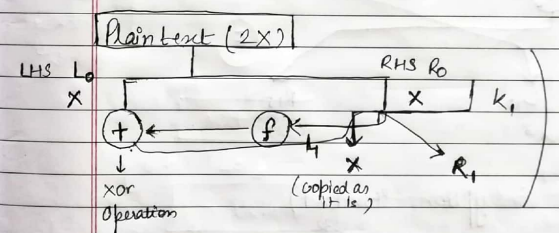
→ K is a key → we use some portion of the key in every round.

→ Fiestal network gives result in multiple rounds or iteration

PT = 32, 64, 128, ...

K = K ∴

K1 K2 K3 K4



- In DES algo → 16 rounds.

Generalized form $L_i = R_{i-1}$

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

→ Security should be provided but time complexity should not be compromised

(i) Selection of plain text (ii) Selection of function

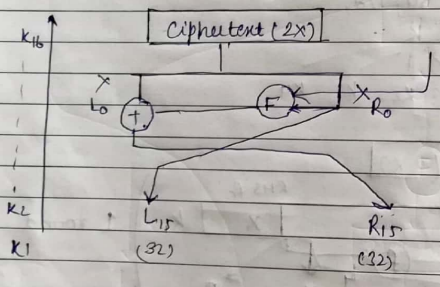
(iii) Sub-key generation algo (iv) No. of rounds

These conditions should be taken into consideration, for increasing efficiency.

Decryption:

(i) We have to use the key in reverse order.

Suppose, we iterate it for 16 rounds.



DES (Data Encryption Standard)

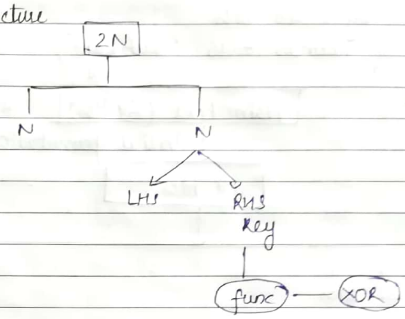
PT - 64 Bit → 32, 32

K - 64 → Parity bits: 8 → Usable: 56 → for each round: 48

CT - 64

$K_1 + K_2$ to K_{16}

Feistal Structure



More complex block size - secure structure

General form:

$R_i = L_{i-1} + f(K_i, R_{i-1})$

$L_i = R_{i-1}$

DES (Data Encryption Standard)

The DES is a block cipher, meaning a cryptographic key and algo are applied to a block of data simultaneously rather than one bit at a time.

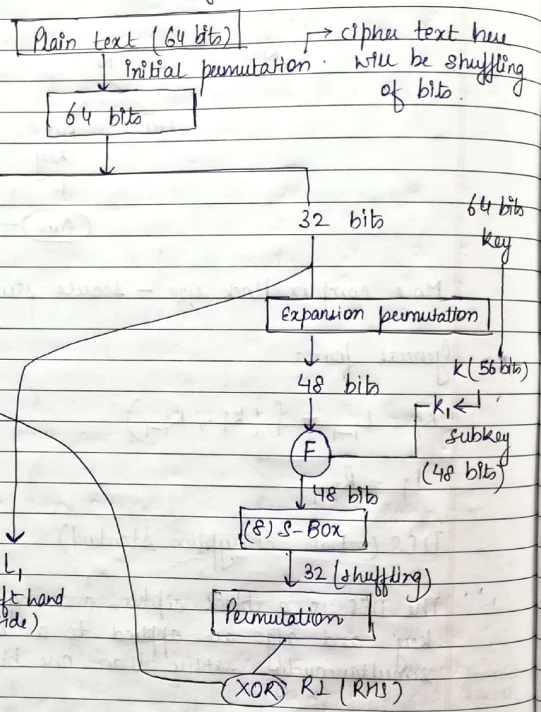
To encrypt a PT message, DES group it into 64-bit blocks.

Plain text (Block size) = 64 bits

Key = 64 bits → usable = 56 bits

(The 8 bits that are removed from 64 bits are just to disguise the attackers (parity bits)

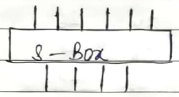
Sub-key = 48 bits
No. of rounds = 16 (subkeys)



→ cipher text here will be shuffling of bits.

We need to perform is more rounds for this.

S-Box → Substitution box it takes the 6 bit input and gives 4-bit output.



Initial permutation.

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

even bit

Bitwise the entry will be 0 or 1.

For each block, when we start with the initial permutation we will start from 1st even column starting from bottom to top.

The new table will look like:

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

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

Now that we have completed the even, we will start from the odd column again

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

final permutation is done.

Now check the bit position i.e. we will be having (0,1) bits on 58th position.

Read from the original table to new table one by one.

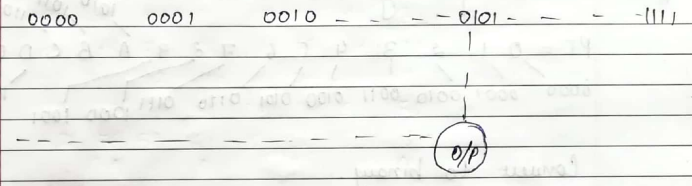
Expansion	Permutation → we are				having 32 bits, but inorder to convert to 48 we will do repetition then only expansion will occur.
32	1	2	3	4	5
4	5	6	7	8	9 (extra added at the end)
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

extra added in start

Added 8 bits in the starting and at the end.
This is a pre-defined table.
(given in exam)

S-Box (8 S-Box exists)

- 6 bit i/p
- 4 bit o/p



Ques: (1)0101(1) (Convert 6 bits to 4 bits)

outer bits will be treated as row, i.e. (11) further inner bits are 0101
Now search in the table given above, the output will be the answer in 4 bits.

Ques:

- Role of S-Box
- Definition
- Conversion

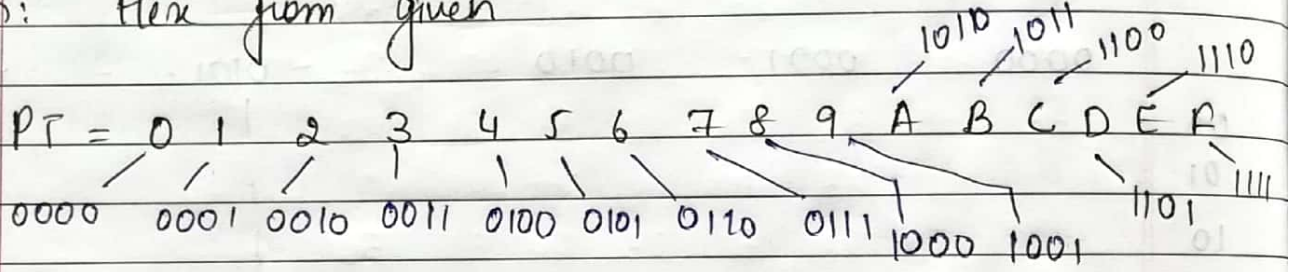
Permutation

We have got data from S-box

32 1 2 4
3 7 8 5

We will put 32 bit on the 1st position & 1st bit on the second position.

Question: Hex from given



Convert to binary.

16 x 4 = 64 bits
(each bit placed at diffent position)

Original table

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

- first even then odd from bottom.

How to identify key?

K = 64 Bits

57 1 2 3 4 5 6 7 8

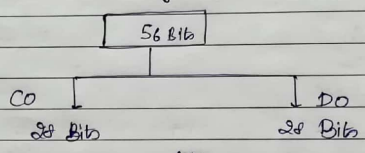
pos. no

place 5th digit from 64 bit data

8

8×7 = 56

56 bits → Round key (48 bits)



left

C0: Round 1, 2, 9, 16 : Circular shift of one bits

Rest rounds : left " " " two "

Ex: K^+ = 56 bits

↑

C_0 = 110011 - - - - - 10

D_0 = 01010 - - - - - 01

Circular shift-

K_1^+ C_1 = 10011 - - - - 101

D_1 = 1010 - - - - 010

K_2^+ C_2 = 0011 - - - - 1011

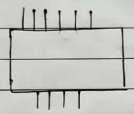
D_2 = 010 - - - - 0101

K_3^+ C_3 = 11 - - - - 101100

D_3 = 0 - - - - 010101

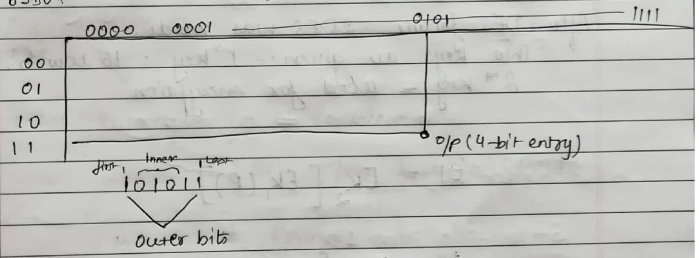
16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

S-box



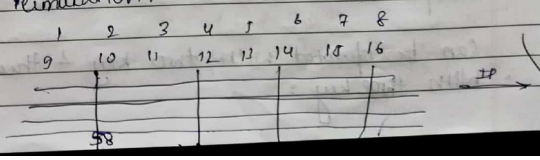
Resultant: 101011 1011 1011 =

S1 S2



- DES complete structure, how to genuate round key (table will be given), Role of sboxes, expansion, initial permutation

Initial Permutation.



Connecting column to row

2 → 2nd bit (14th pos)
4
6
8
1 → first bit (40th pos)
3
5
7

Final permutation

40 8 ____

After DES failure, 2DES was made.
Two keys are given:- 1st key : 16 rounds.
2nd key - used for encryption

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

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

Security & time complexity increases.

Triple DES

Can be operated with two key & three key
• With three key :

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

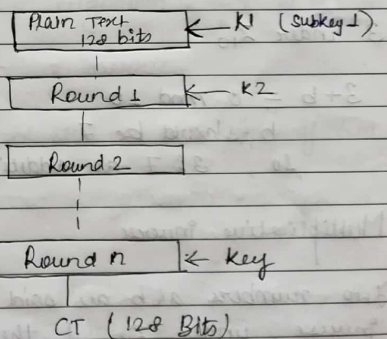
• With two key

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

Limitation of DES, 2DES & triple DES
→ The block cycle can only be of 64 bits.

AES (Advanced Encryption Standard).

→ The data block was of 128 bits. (Plain text)
→ Key = 128 bits, 192 bits, 256 bits.
→ No. of rounds : Depends on the key, if k = 128, NR = 10, k = 192 : NR = 12, k = 256 : NR = 14.
→ SUBKEY = 128 bits.
or Round Key
→ Total Subkey = No. of Rounds + 1.



key generator function is present for generating key.

Set of Residue (Z_n).

Set of some elements starting from 0.

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

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

We will use it in modular arithmatic & it is used in public cryptography.

Additive Inverse

If there exists two numbers a & b, are said to be additive inverse under Z_n, if they follow following condition

$$a+b \equiv 0 \mod n$$
$$\Rightarrow a+b \bmod n = 0 \bmod n.$$

3 under Z_{10}

$3+b = 0 \mod 10$

b should be 7

so, 3 & 7 are additive inverse under Z_{10}.

Multiplicative Inverse

Two numbers a & b are said to be multiplicative inverse under Z_n, if they follow following condition:

$a \times b = 1 \mod n$

Where b/a & n must be co-prime.

3 under Z_{10}

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

$b = 7.$

Find all multiplicative inverse of 7 under Z_{10}.

$7 \times b = 1 \mod 10$

$(7 \times b) \bmod 10 = 1$

3.

Find all multiplicative inverse under Z_{10}.

(7,3), (3,7), (9,9).

Euclidean Algorithm.

Extended Euclidean Algorithm : q r_1 r_2 r t_1 t_2 t

↓

We get multiplicative inverse.

Euclidean algo was used to find GCD of two numbers.

- 13 in Z_{20}

↓ a ↓ n

Algo:-

(1.) $r_1 \leftarrow n$ // initialization

$r_2 \leftarrow a$

(ii) $t_1 \leftarrow 0$ // Initializing again
$t_2 \leftarrow 1$

Generalized Euclidean algo

q	r_1	r_2	r	t_1	t_2	t
	20	13	7	0	1	-1
1	13	7	6	1	-1	1-1x1=2
1	7	6	1	-1	2	-3
6	6	1	0	2	-3	20
1	1	0		-3	20	

When $r_2 = 0$ ↑ GCD of two numbers

(iii) while ($r_2 > 0$)
{
$q = r_1 / r_2$
$r = r_1 - q r_2$
$t = t_1 - q t_2$
$r_1 \leftarrow r_2$
$r_2 \leftarrow r$
$t_2 \leftarrow t$
$t_1 \leftarrow t_2$
}

(iv) $a^{-1} = t_1 = -3$

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

17 is multiplicative inverse of 13 under Z_{20}.

Multiplicative inverse of 11 under Z_{26} using Extended Euclidean Algo.

$r = 26 - 2 \times 22$

(i) $r_1 \leftarrow 26$, $r_2 \leftarrow 26$ // 11
(ii) $t_1 \leftarrow 0$, $t_2 \leftarrow 1$

q	r_1	r_2	r	t_1	t_2	t
2	26	11	4	0	1	0 - 2x1 = -2
2	11	4	3	1	-2	1 - 2x(-2) = 5
1	4	3	1	-2	5	-2 - 1x(5) = -7
3	3	1	0	5	-7	5 - 3x(-7) = 26
	1	0		-7	26	

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

Using Euler totient function.

$A^{-1} \bmod M = A^{\phi(M)-1} \bmod M$
$A^{-1} \bmod 26 = A^{\phi(26)-1} \bmod 26$
$= A^{\phi(26)-1} \bmod 26$
$\phi(26) = 12$ $11^{12-1} \bmod 26 = 11^{11} \bmod 26$.

$11 \bmod 26 = 11$
$11^2 \bmod 26 = 17$
$11^4 \bmod 26 = ((11^2 \bmod 26) \times (11^2 \bmod 26)) \bmod 26$
$= (17 \times 17) \bmod 26 = 3$

$11^{11} \bmod 26 = (11^4 \bmod 26 \times 11^4 \bmod 26 \times 11^2 \bmod 26 \times 11 \bmod 26) \bmod 26$
$= (3 \times 3 \times 17 \times 11) \bmod 26$
$= 1683 \bmod 26 = 19$.

Q: Find the multiplicative inverse of 29 under Z_{80}. Or $29^{-1} \bmod 80$.

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	

$-11 \bmod 80$

$(80-11) \bmod 80 = 69 \bmod 80 = 69$

Check: $\frac{69 \times 29}{80} = \text{Rem } 1$

Assignment 1 (Submit : 10 sept, 2018)

1. What are different security services and security mechanisms that ensures security?
2. Explain different types of modes of operations of block cipher.
3. Differentiate b/w :- (i) cryptography & steganography.
   (ii) Block cipher & Stream cipher
   (iii) Confusion & diffusion

By Euler's totient

$29^{\phi(80)-1} \bmod 80$

$\phi(80) = \phi(5) \times \phi(2^4) = 4 \times (2^4 - 2^1) = 4 \times 8 = 32.$

$29^{31} \bmod 80$

FERMAT's THEOREM / FERMAT's LITTLE THEOREM

→ Apply when 'p' is prime

→ Helps in calculating exponent value.

Case 1: If p is a prime number & a is a positive integer such that p does not divides a, then following condition follows :-

$$a^{p-1} \equiv 1 \bmod p \qquad -(1)$$

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

Case 2: If p is a prime no and a is a positive integer (then if divide or not it follows) $a^p \equiv a \bmod p.$ (multiplying eq^n (1) by a)

$$a^p \bmod p = a \bmod p.$$

Case 3: If equation (1) is multiplied by a^{-1} both side

$$a^{p-2} \equiv a^{-1} \bmod p \checkmark$$

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

NOTE: $a^p \bmod b \Rightarrow$ if $(p >= b)$ then only use fermat (else no easy)

Q: $3^{10} \bmod 11$ (a, p)

1st case: $3^{11-1} \bmod 11 = 1 \bmod 11 = 1.$

Q: $3^{12} \bmod 11$ (a, p) 11th case: $(3^{10} \bmod 11 \cdot 3^2 \bmod 11) \bmod 11$

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

2nd case: $(3^{11} \bmod 11 \cdot 3 \bmod 11) \bmod 11$

$= (3 \bmod 11 \cdot 3) \bmod 11 = (3 \cdot 3) \bmod 11 = 9.$

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

3rd case: $7^{13-2} \bmod 13 = 7^{11} \bmod 13$ (solve by repetetive square method)

EULER'S THEOREM.

1. a is a positive integer and n is also positive integer, then

{ Not applicable when n is PRIME }

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

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

Multiplying by a^{-1}

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

Q: $6^{24} \bmod 35$ (a, n)

$\phi(35) = \phi(7) \times \phi(5) = 6 \times 4 = 24$

$= 6^{\phi(35)} \bmod 35 = 1.$

Q: $20^{62} \bmod 77$ (a, n)

$\phi(77) = \phi(7) \times \phi(11) = 6 \times 10 = 60.$

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

$= (20^{\phi(77)} \bmod 77 \times (20^{2} \bmod 77)) \bmod 77$

$= (1 \cdot 11) \bmod 77 = 15.$

Q: $10^{18} \bmod 19$ (prime)

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

Q: $7^{222} \bmod 10.$ $\phi(10) = \phi(5) \times \phi(2) = 4.$

$222 = 4 \times 55$

$= ((7^{4} \bmod 10)^{55} \cdot 7^{2} \bmod 10) \bmod 10$

$= ((1)^{55} \cdot 49 \bmod 10) \bmod 10$

$= (1 \cdot 49 \bmod 10) \bmod 10 = (1 \cdot 9) \bmod 10 = 9.$

Q: PT – NETWORK SECURITY.

Multiplicative key = 11, Additive key = 8

Calculate cipher text using AFFINE CIPHER

Q: PT – VIGENERE CIPHER

key – SECURITY SECURI

Calculate cipher text using VIGENERE CIPHER

Chinese Remainder Theorem

If we have congruence Equation (=), we find values from it.

$x \equiv a_1 \bmod m_1$
$x \equiv a_2 \bmod m_2$ → these modulus values must be co-prime when each other
$x \equiv a_3 \bmod m_3$

Solution (i) We find common modulus

$M = m_1 \times m_2 \times m_3$.

(ii) Now, we find

$M_1 = \frac{M}{m_1}$, $M_2 = \frac{M}{m_2}$, $M_3 = \frac{M}{m_3}$

(iii) Now we find M_1^{-1}, M_2^{-1}, M_3^{-1} (we find inverse corresponding to m_1, m_2 & m_3)

(iv) Now, $x = \left(a_1 \times M_1 \times M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}\right) \bmod M$.

Q: $x \equiv 2 \bmod 3$, $x \equiv 3 \bmod 5$ & $x \equiv 2 \bmod 7$.

(i) 3, 5 & 7 are co-prime values.

(ii) $M = 3 \times 5 \times 7 = 105$

(iii) $M_1 = \frac{105}{3} = 35$, $M_2 = \frac{105}{5} = 21$, $M_3 = \frac{105}{7} = 15$.

(iv) $M_1^{-1} = 35^{-1} \bmod 3$ ↳ w.r.t 1st modulus value.

$= 35^{\phi(3)-1} \bmod 3 = 35^{2-1} \bmod 3 = 35 \bmod 3$

$M_2^{-1} = 21^{-1} \bmod 5 = 21^{\phi(5)-1} \bmod 5 = 21^3 \bmod 5 = 1$
($\because 21 \bmod 5 = 1 \Rightarrow 1^3 \bmod 5 = 1$)

$M_3^{-1} = 15^{-1} \bmod 7 = 15^{\phi(7)-1} \bmod 7 = 15^5 \bmod 7 = 1$

$x = (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 105$
$= (140 + 63 + 30) \bmod 105$
$= 233 \bmod 105 = 23$.

Cross-Check.

$x = a_1 \bmod m_1$
$23 \equiv 2 \bmod 3$.
$23 \bmod 3 = 2 \bmod 3$ ✓ (satisfied).

$23 \bmod 5 = 3 \bmod 5$ ✓
and $23 \bmod 7 = 2 \bmod 7$ ✓.

Q: $x \equiv 2 \bmod 3$, $x \equiv 3 \bmod 5$, $x \equiv 4 \bmod 11$, $x \equiv 5 \bmod 16$ find the value of var x using CRT, it leaves 2 as remainder when divided by 3 & so on.

(i) 3, 5, 11, 16 are co-prime.

(ii) $M = 3 \times 5 \times 11 \times 16 = 8640$

(iii) $M_1 = \frac{2640}{1} = 880$ $M_2 = \frac{2640}{5} = 528$ $M_3 = \frac{2640}{11} = 240$

$M_4 = \frac{2640}{16} = 165$

(iv) $M_1^{-1} = 880^{-1} \bmod 3 = 880^{\phi(2)-1} \bmod 3$

$= 880 \bmod 3 = 1$

$M_2^{-1} = 528^{-1} \bmod 5 = 528^{\phi(5)-1} \bmod 5$
$= 528^3 \bmod 5 = 27 \bmod 5 = 2$

$M_3^{-1} = 240^{-1} \bmod 11 = 240^{9} \bmod 11$

$= 240^{11-2} \bmod 11 = (240)^{9} \bmod 11 = 9.5$

$M_4^{-1} = 165^{-1} \bmod 16 = 165$

$\phi(16) = \phi(2^4) = 2^4 - 2^3 = 16 - 8 = 8.$

$165^{7} \bmod 16 = 5^7 \bmod 16 = 78125 \bmod 16 = 13.$

9.

$165^{\phi(16)-1} \equiv 165^{-1} \bmod 16$

$x = (2 \times 880 \times 1 + 3 \times 528 \times 2 + 4 \times 240 \times 9 + 5 \times 165 \times 13) \bmod 2640$

$= (1760 + 3168 + 8640 + 10725) \bmod 2640$

$= 24292 \bmod 2640 = 533.$

$533 \bmod 3 = 2 \bmod 3$ ✓

$533 \bmod 5 = 3 \bmod 5$ ✓

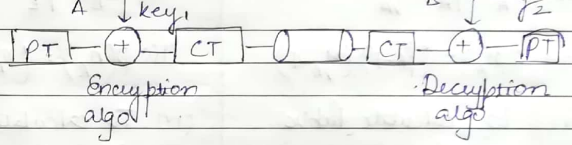
$533 \bmod 11 = 4 \bmod 11$

$533 \bmod 16 = 5 \bmod 16$ ✓

Public Key Cryptography

Till now, we have used a single key → symmetric key cryptography

Now, we will be using two key → public key & private key → asymmetric key.



Security → Authentication, Confidentiality, Integrity

User A encrypts msg using User B's public key. The private key associated with it can only be used by B.

We get Confidentiality.

When User A encrypts msg using User B's private key.

We get Authentication. We are getting digital signature. (∵ Private key is unique)

When a check value is added to a message. Using a method. At the decryption end, they are separated and checked using same method. It is known for Integrity.

CA → certificating authority.

e_A → gets registered (Users register public key)

RSA Algorithm

A — Devising Public key — B

A	B
(i) We choose p_A, q_A prime numbers.	(i) We choose p_B & q_B.
(ii) $n_A = p_A \times q_A$	(ii) $n_B = p_B \times q_B$.
(iii) $\phi(n_A) = (p_A - 1)(q_A - 1)$	(iii) $\phi(n_B) = (p_B - 1)(q_B - 1)$
(iv) To calculate Public key value	(iv) To calculate Public key value.
(a) $1 < e_A < \phi(n_A)$	(a) $1 < e_B < \phi(n_B)$
(b) $GCD(e_A, \phi(n_A)) = 1$ (that is, e_A & $\phi(n_A)$ are co-prime).	(b) $GCD(e_B, \phi(n_B)) = 1$
Devising private key.	
(c) $e_A \cdot d_A \equiv 1 \bmod \phi(n_A)$	(c) $e_B \cdot d_B \equiv 1 \bmod \phi(n_B)$

	A	B
Public	e_A	e_B
Private	d_A	d_B

Q: Suppose that $p = 7$, $q = 11$, $M = 5$

(i) $n = 7 \times 11 = 77$

(ii) $\phi(n) = \phi(7) \times \phi(11) = (7-1)(11-1) = 6 \times 10 = 60$

(iii) Ciphet text $= C = M^e \bmod n$

(iv) Decrypted text $= C^{de} \bmod n = M$.

(v) $1 < e < \phi(n)$ & $GCD(e, \phi(n)) = 1$

let $e = 13$.

$13 \cdot d \equiv 1 \bmod 60$

$d \equiv 13^{-1} \bmod 60$.

$13^{\phi(60)-1} \bmod 60$

$\phi(60) = \phi(2) \times \phi(3) \times \phi(5) \times \phi(2)$

$= 1 \times 2 \times 4 \times 1 = 8$

$13^7 \bmod 60$

$13 \bmod 60 = 13$

$13^2 \bmod 60 = 49$

$13^4 \bmod 60 = (13^2 \bmod 60 \times 13^2 \bmod 60) \bmod 60$

$= (49 \times 49) \bmod 60 = 1$.

$13^7 \bmod 60 = (13^4 \bmod 60 \times 13^2 \bmod 60 \times 13 \bmod 60) \bmod$

$= (1 \times 49 \times 13) \bmod 60$

$= 637 \bmod 60 = 37$

$d = 37$.

(vi) $C = M^e \bmod n$

$= 5^{13} \bmod 77$.

$5 \bmod 77 = 5$

$5^2 \bmod 77 = 25$

$5^4 \bmod 77 = (25 \times 25) \bmod 77 = 9$

$5^6 \bmod 77 = (9 \times 25) \bmod 77 = 71$

$5^{10} \bmod 77 = (71 \times 9 \times 25 \times 5) \bmod 77$

$= 79875 \bmod 77 = 26.$

(vii) $M = C^d \bmod n$

$= 26^{37} \bmod 77.$

$26 \bmod 77 = 26$

$26^2 \bmod 77 = 676 \bmod 77 = 60$

$26^4 \bmod 77 = (60 \times 60) \bmod 77 = 58$

$26^8 \bmod 77 = (58 \times 58) \bmod 77 = 3364 \bmod 77 = 53.$

$26^{10} \bmod 77 = (53 \times 60) \bmod 77 = 3180 \bmod 77 = 22.$

$26^{37} \bmod 77 = (21 \times 21 \times 21 \times 58 \times 60 \times 26) \bmod 77$

$= 110087016 \bmod 77$

$= 5.$

Message value can be in alphabetical form

M = CRYPTO

(i) (ii) (iii) (iv) (v) (vi)

Q: $p = 17, \quad q = 19, \quad M = 10$

(i) $p \times q = 17 \times 19 = 323.$

(ii) $\phi(n) = \phi(17) \times \phi(19) = 16 \times 18 = 288.$

(iii) $C = M^e \bmod n$

$1 < e < \phi(n) \quad \text{GCD}(e, \phi(n)) = 1$

Let $e = 15$

$15 \cdot d \equiv 1 \bmod 288$

$d = 5^{-1} \bmod 288.$

$\phi(288) = \phi(3) \times \phi(3) \times \phi(2) \times \phi(2) \times \phi(2) \times \phi(2) \times \phi(2)$

$= \phi(3^2 \times 2^5).$

$\phi(1^2) \times \phi(2^5)$

$(3^2 - 3) \times (2^5 - 2^4)$

$(9 - 3) \times (32 - 16)$

$2 \times 16 = 48$