Unit - 1

Que.

Q1 :- Explain the OSI Security Architecture & Define a different Security services?

(7M)

Q2 :- What is difference bet^n Substitution Encryption techniques and Transposition Encryption Techniques?

(6M)

Q3 :- Explain the substitution Techniques? If the cipher is keyed by a word "COMPUTER" and plaintext is "Please transfer one million dollars to my account six six two obtain the cipher text by Playfair substitution Method.

(7M)

Q4 :- What is cryptography? Explain the conventional Encryption model with neat diagram?

(6M)

Q5 :- Explain the OSI Security Architecture and Security attacks with example.

(8M)

Q6 :- Explain the various aspects of Information Security.

(5M)

Q7 :- Explain cryptanalysis and its types.

(5M)

Unit - I

Introduction :-

- Attributes of security
- OSI security Architecture ← security Attack, security mechanism, security service.
- Model for Network security

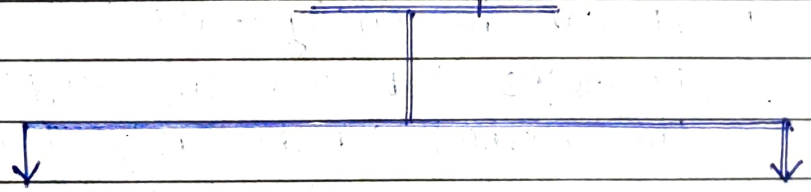
Mathematics of cryptography :-

- Modular Arithmetic
- Euclidean and extended Euclidean algorithm

classical encryption techniques :-

- Substitution techniques
  1) ceasar cipher
  2) Vigeneres ciphers
  3) Hill ciphers
  4) Playfair ciphers
- Transposition techniques.

→ **classical Encryption Techniques**



Substitution Technique	Transposition Technique
(1) Caesar cipher	(1) Rail Fence
(2) Monoalphabetic substitution	(2) Row column Transposition.
(3) Playfair cipher	
(4) Hill cipher	
(5) Polyalphabetic cipher	
(6) one Time pad.	

PAGE NO.:
DATE

Substitution techniques :-

1) Caesar cipher
2) Vigener's cipher
3) Hill ciphers
4) Playfair ciphers
5) one pad.

① Caesar cipher or additive cipher or shift cipher Caesar's code or caesar shift :-

Features of Caesar cipher Substitution Technique :-

① Stream cipher
② Substitution cipher
③ monoalphabetic cipher

Disadvantage of Caesar Cipher :-

① It can be easily hacked.
It means that message encrypted by this method can be easily decrypted.

② It provides very little security

③ By looking at the pattern of letters in it, the entire message can be decrypted.

Advantages of caesar cipher :-

① one of the simplest and easiest encryption methods that provide a layer of security to your data.

Q. Use additive cipher with key = 4 to encrypt message "Hello".

message : Hello
key : 4

⇒

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

P	Q	R	S	T	U	V	W	X	Y	Z
15	16	17	18	19	20	21	22	23	24	25.

Plaintext :- H E LL O key :- 4

↓ ↓ ↓ ↓ ↓

7 4 11 11 14

Encryption of HELLO :

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

$C = (H+4) \bmod 26$

$C = (7+4) \bmod 26$

$C = (11) \bmod 26$

$\boxed{C = 11}$ → L

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

$C = (E+4) \bmod 26$

$C = (4+4) \bmod 26$

$C = 8 \bmod 26$

$\boxed{C = 8}$ → I

Decryption of cipher text : LIPPS

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

$P = (L-4) \bmod 26$

$P = (11-4) \bmod 26$

$P = 7 \bmod 26$

$\boxed{P = 7}$ → H

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

$P = (I-4) \bmod 26$

$P = (8-4) \bmod 26$

$P = 4 \bmod 26$

$\boxed{P = 4}$ → E

PAGE NO.:
DATE

$C = (P + K) \bmod 26$
$C = (L + 4) \bmod 26$
$C = (11 + 4) \bmod 26$
$C = 15 \bmod 26$
$\boxed{C = 15}$
↓
P

$C = (P + K) \bmod 26$
$C = (O + K) \bmod 26$
$C = (14 + 4) \bmod 26$
$C = 18 \bmod 26$
$\boxed{C = 18}$
↓
S

$\boxed{\text{Cipher text : LIPPS}}$

$P = (C - K) \bmod 26$
$P = (P - 4) \bmod 26$
$P = (15 - 4) \bmod 26$
$P = 11 \bmod 26$
$\boxed{P = 11}$
↓
L

$P = (C - K) \bmod 26$
$P = (S - 4) \bmod 26$
$P = (18 - 4) \bmod 26$
$P = 14 \bmod 26$
$\boxed{P = 14}$
↓
O

$\boxed{\text{Plaintext : HELLO}}$

PAGE NO.:
DATE

$C = (P + K) \bmod 26$
$C = (L + 4) \bmod 26$
$C = (11 + 4) \bmod 26$
$C = 15 \bmod 26$
$C = 15$
↓
P

$C = (P + K) \bmod 26$
$C = (O + K) \bmod 26$
$C = (14 + 4) \bmod 26$
$C = 18 \bmod 26$
$C = 18$
↓
S

Cipher text : LIPPS

$P = (C - K) \bmod 26$
$P = (P - 4) \bmod 26$
$P = (15 - 4) \bmod 26$
$P = 11 \bmod 26$
$P = 11$
↓
L

$P = (C - K) \bmod 26$
$P = (S - 4) \bmod 26$
$P = (18 - 4) \bmod 26$
$P = 14 \bmod 26$
$P = 14$
↓
O

Plaintext : HELLO

Q. Use Caesar Cipher With key = 14 to encrypt message "TV"

message : TV
key : 14

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

P	Q	R	S	T	U	V	W	X	Y	Z
15	16	17	18	19	20	21	22	23	24	25.

26
52
78
104
130
156
182
208
234
260

Plaintext :- T V key :- 14
↓ ↓
19 21

Encryption of TV :

$C = (P+K) \bmod 26$
$C = (T+K) \bmod 26$
$C = (19+14) \bmod 26$
$C = 33 \bmod 26$

$26 \overline{)33}\ (1$, $33 - 26 = 07$

$\boxed{C = 7}$
↓
H

$C = (P+K) \bmod 26$
$C = (V+K) \bmod 26$
$C = (21+14) \bmod 26$
$C = 35 \bmod 26$

$26 \overline{)35}\ (1$, $35 - 26 = 9$

$\boxed{C = 9}$
↓
J

cipher text : HJ

Decryption of cipher text : HJ

$P = (C-K) \bmod 26$
$P = (H-K) \bmod 26$
$P = (7-14) \bmod 26$
$26 - 7 = 19$
$P = -7 \bmod 26$
$\boxed{P = 19}$
↓
T

$P = (C-K) \bmod 26$
$P = (J-K) \bmod 26$
$P = (9-14) \bmod 26$
$26 - 5 = 21$
$P = -5 \bmod 26$
$\boxed{P = 21}$
↓
V

plaintext : TV

(2) Vigener's cipher :-

(1) It is a poly alphabetic substitution cipher.

→ Plain text : GIVE MONEY
key : LOCK

→

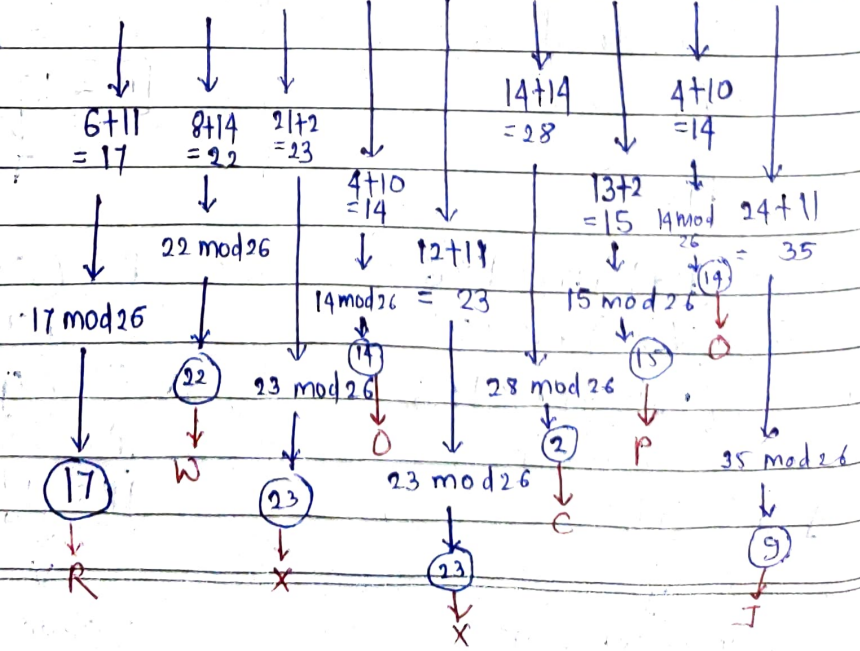
A	B	C	D	E	F	G	H	I	J	K	L
0	1	2	3	4	5	6	7	8	9	10	11

M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
12	13	14	15	16	17	18	19	20	21	22	23	24	25

(1) Encryption :-

Plaintext :	G	I	V	E	M	O	N	E	Y
	↓	↓	↓	↓	↓	↓	↓	↓	↓
	6	8	21	4	12	14	13	4	24

key :	L	O	C	K	L	O	C	K	L
	↓	↓	↓	↓	↓	↓	↓	↓	↓
	11	14	2	10	11	14	2	10	11



Cipher text :- RWXOX CPOJ

decrypt :-

Plaintext :-

G	I	V	E	M	O	N	F	Y
↓	↓	↓	↓	↓	↓	↓	↓	↓
6	8	21	4	12	14	13	4	24

key :	L	O	C	K	L	O	C	K	L
	↓	↓	↓	↓	↓	↓	↓	↓	↓
	11	14	2	10	11	14	2	10	11

Ciphertext :	R	W	X	O	X	C	P	O	J
	(17)	(22)	(23)	(14)	(23)	(2)	(15)	(14)	(9)

$D_i = (E_i - K_i) \bmod 26$
$= (17 - 11) \bmod 26$
$= 6 \bmod 26$
$D_i = 6$ → G

$D_i = (E_i - k_i) \bmod 26$
$= (X - C) \bmod 26$
$= (23 - 2) \bmod 26$
$= 21 \bmod 26$
$D_i = 21$ → V

$D_i = (E_i - k_i) \bmod 26$
$= (W - D) \bmod 26$
$= (22 - 14) \bmod 26$
$= 8 \bmod 26$
$D_i = 8$ → I

$D_i = (E_i - k_i) \bmod 26$
$= (O - K) \bmod 26$
$= (14 - 10) \bmod 26$
$= 4 \bmod 26$
$D_i = 4$ → E

PAGE NO.:
DATE

$D_i = (E_i - k_i) \bmod 26$
$= (X - L) \bmod 26$
$= (23 - 11) \bmod 26$
$= (12 \bmod 26)$
$D_i = 12$
↓
M

$D_i = (E_i - k_i) \bmod 26$
$= (J - L) \bmod 26$
$= (9 - 11) \bmod 26$
$= -2 \bmod 26$
$26 - 2 = 24$
$D_i = 24$
↓
Y

$D_i = (E_i - k_i) \bmod 26$
$= (C - O) \bmod 26$
$= (2 - 14) \bmod 26$
$= -12 \bmod 26$
$26 - 12 = 14$
$D_i = 14$
↓
O

$D_i = (E_i - k_i) \bmod 26$
$= (P - C) \bmod 26$
$= (15 - 2) \bmod 26$
$= 13 \bmod 26$
$D_i = 13$
↓
N

$D_i = (E_i - k_i) \bmod 26$
$= (O - K) \bmod 26$
$= (14 - 10) \bmod 26$
$= 4 \bmod 26$
$D_i = 4$
↓
E

plaintext :- GIVE MONEY

③ Hill cipher :-

Step 1 :- Select message to encrypt.

COMPUTER

Step 2 :- select a key is dbef

Step 3 :- Lets us assign a numerical equivalent

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Step 4 :- Convert the key dbef to a 2x2 matrix to each.

$$\text{key } K = \begin{bmatrix} d & b \\ g & f \end{bmatrix} = \begin{bmatrix} 3 & 1 \\ 6 & 5 \end{bmatrix}$$

key K is done.

Step 5 :- Convert the message COMPUTER to a n component vector.

$$n = 2 \times 2$$

$$\boxed{n = 2}$$

PAGE NO.:
DATE

$$\begin{bmatrix} C \\ O \end{bmatrix} \begin{bmatrix} M \\ P \end{bmatrix} \begin{bmatrix} U \\ T \end{bmatrix} \begin{bmatrix} E \\ R \end{bmatrix}$$

$$\begin{bmatrix} 2 \\ 14 \end{bmatrix} \begin{bmatrix} 12 \\ 15 \end{bmatrix} \begin{bmatrix} 20 \\ 19 \end{bmatrix} \begin{bmatrix} 4 \\ 17 \end{bmatrix}$$

Encryption

Step 6 :-

ciphertext = K * P mod 26

$$= \begin{bmatrix} 3 & 1 \\ 6 & 5 \end{bmatrix} * \begin{bmatrix} 2 \\ 14 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 3\times2 + 1\times14 \\ 6\times2 + 5\times14 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 6+14 \\ 12+70 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 20 \\ 82 \end{bmatrix} \text{ mod } 26$$

3
26 | 82
-78
04

0
26 | 20
-0
20

= 20 mod 26 ⇒ 20
82 mod 26

$$= \begin{bmatrix} 20 \\ 4 \end{bmatrix}$$

$$= \begin{bmatrix} U \\ E \end{bmatrix}$$

Decryption

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

↓ (inverse of K)

* inverse of K means inverse of a matrix
* 2x2 matrix means 4 no. ∵ $\begin{bmatrix} - & - \\ - & - \end{bmatrix}$

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

↓ adjoint

Compute $\frac{1}{|K|}$

⇒ $K = \begin{vmatrix} 3 & 1 \\ 6 & 5 \end{vmatrix} = |3 \times 5 - 6 \times 1| = |15 - 6| = 9$

Rule $a \bmod b = 1$

GCD $(a, b) = 1$

$9 \bmod 26$

$9 \times 1 \bmod 26$

$9 \bmod 26 \Rightarrow 9$

$\frac{1}{|K|} = 3$

$9 \times 2 \bmod 26$

$18 \bmod 26 \Rightarrow 18$

∵ $8 \times 1 \bmod 26$

$8 \bmod 26$

$26 \overline{)27}\ (1$

26

01

$9 \times 3 \bmod 26$

$27 \bmod 26 \Rightarrow 1$

PAGE NO.:
DATE

compute adj(k)

$$K = \begin{bmatrix} 3 & 1 \\ 6 & 5 \end{bmatrix}$$

$$= \begin{bmatrix} 5 & -1 \\ -6 & 3 \end{bmatrix}$$

$$K^{-1} = \frac{1}{|K|} \text{adj}(K) \longrightarrow \text{formula}$$

$$K^{-1} = 3 * \begin{bmatrix} 5 & -1 \\ -6 & 3 \end{bmatrix}$$

$$K^{-1} = \begin{bmatrix} 3x5 & 3x-1 \\ 3x-6 & 3x3 \end{bmatrix}$$

$$K^{-1} = \begin{bmatrix} 15 & -3 \\ -18 & 9 \end{bmatrix}$$

To avoid -ve no just add +26 to negative no.

$$K^{-1} = \begin{bmatrix} 15 & -3+26 \\ -18+26 & 9 \end{bmatrix}$$

$$K^{-1} = \begin{bmatrix} 15 & 23 \\ 8 & 9 \end{bmatrix}$$

then decryption formula

$$\text{Plaintext} = k^{-1} \times C \bmod 26$$

$$= \begin{bmatrix} 15 & 23 \\ 8 & 9 \end{bmatrix} \times \begin{bmatrix} U \\ E \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 15 & 23 \\ 8 & 9 \end{bmatrix} \times \begin{bmatrix} 20 \\ 4 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 15 \times 20 + 23 \times 4 \\ 8 \times 20 + 9 \times 4 \end{bmatrix}$$

$$= \begin{bmatrix} 300 + 92 \\ 160 + 36 \end{bmatrix}$$

$$= \begin{bmatrix} 392 \\ 196 \end{bmatrix} \bmod 26$$

$$= 392 \bmod 26$$
$$196 \bmod 26$$

$$= \begin{bmatrix} 2 \\ 14 \end{bmatrix}$$

$$= \begin{bmatrix} C \\ O \end{bmatrix}$$

PAGE NO.:
DATE

④ Playfair cipher :-

→ ① Aka Playfair square or Wheatstone - playfair cipher.

② Manual symmetric encryption technique.
③ First literal diagram substitution cipher
④ Invented in 1854 by Charles Wheatstone
⑤ Bore the name of Lord playfair for promoting its use.

→ ① Multiple letter encryption cipher
② Digrams
③ 5 x 5 matrix constructed using a keywor

→ Rules for encryption Using Playfair cipher.

① Digrams
② Repeating letters - filler letter
③ same column |↓| wrap around
④ same row |→| wrap around
⑤ Rectangle |⇆| swap.

Plaintext → attack
Digrams → at ta ck

Plaintext → neso academy
Digrams → ne so ac ad em yx

Plaintext → balloon
ba ll oo n ⇒ filler letter x

ba lx lo on.

Ex., cipher is keyed by a word COMPUTER.

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

5 x 5

Plaintext :- CNSHCI
Digram :-

CN	SH	CI
KM	QI	DU