SOMAIYA
VIDYAVIHAR UNIVERSITY

Batch: SY-IT(B3)	Roll No.: 16010423076
Name : Ritesh Jha	
Course : ITC	
Experiment / assignment / tutorial No. 7	
Grade:	Signature of the Faculty with date

Tutorial - 7

Sol^n Q1) a) Substitution Cipher

In this cipher, each letter in the plaintext is replaced by another letter or symbol. The key property is that it maintains the same length for both plaintext and ciphertext.

b) Transposition Cipher

This cipher rearranges the positions of the letters in the plaintext according to a specific system.
The key property is that the order of the letters is altered, but the original letters remain unchanged.

c) Assymmetric cryptography.

It uses a pair of public & private keys.
The public key encrypts the data, while only the private key can decrypt it, ensuring secure communication without sharing secret keys.

Sol^n Q2) a) The relationship between a, b & m is as follows :

i) a must be coprime with m (i.e. gcd (a,m) = 1)
ii) b can be any int b/w 0 & m-1
iii) a must have an inverse modulo m for the cipher to be decryptable.

b) Encryption function given :

$c_i = (3x_i + 7) \bmod 26$

Plaintext : "security"

from the function, we can derive that $k_1 = 3$ & $k_2 = 7$.

We know that,

letters of the word "security" converted to numbers are:-

s	18	∴ $(3 \times 18 + 7) \bmod 26$	=	9	→	J
e	4	$(3 \times 4 + 7) \bmod 26$	=	19	→	T
c	2	$(3 \times 2 + 7) \bmod 26$	=	13	→	N
u	20	$(20 \times 3 + 7) \bmod 26$	=	15	→	P
r	17	$(3 \times 17 + 7) \bmod 26$	=	6	→	G
i	8	$(3 \times 8 + 7) \bmod 26$	=	5	→	F
t	19	$(3 \times 19 + 7) \bmod 26$	=	12	→	M
y	24	$(3 \times 24 + 7) \bmod 26$	=	1	→	B

∴ Encrypted Word : JTNPGFM B

For decryption, we use

$$\boxed{\begin{array}{l} T = ((C - k_2) \bmod 26 \\ P = (T \times k_1^{-1}) \bmod 26 \end{array}}$$

To find inverse

$3^{-1} \bmod 26$

$3 \times x \bmod 26 = 1$

$3 \times 9 \bmod 26 = 1$

∴ $k_1^{-1} = 9$

∴ The combined eqⁿ becomes

$$\boxed{x = 9(c - 7) \bmod 26}$$

Decrypting : " JTNPGFMB "

J	9	∴ 9(2) mod 26 = 18	→	S
T	19	9(12) mod 26 = 4	→	E
N	13	9(6) mod 26 = 2	→	C
P	15	9(8) mod 26 = 20	→	U
G	6	9(-1) mod 26 = -9 % 26 = 17	→	R
F	5	9(-2) mod 26 = -18 % 26 = 8	→	I
M	12	9(5) mod 26 = 19	→	T
B	1	9(-6) mod 26 = -54 % 26 = 24	→	Y