SOMAIYA VIDYAVIHAR UNIVERSITY

Batch: B2 Roll No.: 16010421119
Name : Aarya Tiwari
Course : ITC
Experiment / assignment / tutorial No. 8
Grade: Signature of the Faculty with date

ITC Tutorial 8

Name - Aarya Tiwari
Roll no. - 16010421119
Batch - B2

Q1) Show how RSA algorithm can be used for encryption and decryption using the following values : p=7 , q=11 , m=3

Q2) Use the vigener cipher method to encode and decode the message 'GIRAFFE' using encryption Key "XYZ"

Q3) Use the Affine substitution cipher to encode and decode the message "UKRAINE" : Assume the values , a=9, b=2, m=26.

Ans1- p = 7
q = 11
m = 3
So we have to compute n.

$n = p * q \Rightarrow = 7 \times 11 = 77$

$\phi(n) = (p-1) * (q-1)$

[p and q are both prime numbers]

$\phi(77) = (7-1)(11-1)$
$= (6)(10)$
$= 60.$

choosing value of e such that

$1 < e < \phi(n)$

e and $\phi(n)$ are co-prime

let $e = 7$

Find d such that its the inverse of 'e'

$(d * e) = 1 \% \phi(n)$

$(d * e) \% \phi(n) = 1$

Assuming values for d.

put $d = 1$

$\therefore (1 \times 7) \% 60 = 7$

put $d = 2$

$(2 \times 7) \% 60 = 14$

put $d = 3$

$(3 \times 7) \% 60 = 21$

and so on

put $d = 43$

Public Key is $(e, n) \Rightarrow (7, 77)$

Private Key is $(d, n) \Rightarrow (43, 77)$

∴ The encryption of $m=3$ is

$$c = m^e \% n$$
$$= 37 \% 77$$
$$= 31$$
$$\therefore c = 31$$

∴ Decryption of $c=31$ is

$$m = c^d \% n$$
$$31^{43} \% 77$$
$$= 3$$

$$\boxed{m=3}$$

Thus, we perform encryption and decryption and get $\boxed{m=3}$.

Ans 2(b) message = 'GIRAFFE'
encryption key = 'XYZ' ; Vigener cypher method.

(1) We assign values to letters A – Z:

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

G	I	R	A	F	F	F
X	Y	Z	X	Y	Z	X

$C_i = (P_i + K_i) \bmod 26$; P_i : Code corresponding to P_i (Plain text)

$P_i + K_i$	C_i	$C_i \% 26$	
		3	D
G + X	6 + 23	3	D
I + Y	8 + 24	6	G
R + 2	17 + 25	16	a
A + X	0 + 23	23	X
F + Y	5 + 24	3	D
F + 2	5 + 25	4	E
E + X	4 + 23	1	B

The encrypted message is "D G q X D E B

for decryption.

D	G	Q	X	D	E	B
X	Y	2	X	Y	2	X

$P_i = (C_i - K_i) \bmod 26.$

$C_i - K_i$	P_i	$P_i \% 26$	m
D - X	3 - 23	6	G
G - Y	6 - 24	8	I
Q - 2	16 - 25	17	R
X - X	23 - 23	0	A
D - Y	3 - 24	5	F
E - 2	4 - 25	5	F
B - X	1 - 23	4	E

message after decryption is 'GIRAFFE'

SOMAIYA VIDYAVIHAR UNIVERSITY

Batch: _____ Roll No.: _____
Name : _____
Course : _____
Experiment / assignment / tutorial No. _____
Grade: _____ Signature of the Faculty with date

Ans 3- message - 'UKRAINE'

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

Affine substitution cipher method.

$c = (ax + b) \bmod m$.

$a = 9$, $b = 2$, $m = 26$. (given)

Encoding

m	U	K	R	A	I	N	F
x	20	10	17	0	8	13	4
c	0	14	25	2	22	15	12
	A	O	Z	C	W	P	M.

→ 'AOZCWPM' after encryption.

Decoding $a \cdot y = 1 \bmod m$.

$\therefore a \cdot y \bmod m = 1$,

y	a·y	a·y % 26
1	9	9
2	18	18
3	27	1

$\therefore y = 3$

m: $y(c-b) \bmod 26$

$= 3(c-2) \% 26$

c	A	O	2	C	W	F	M
x	0	14	25	2	22	15	12
m	20	10	17	0	8	13	4
m.	U	K	R	A	I	N	E

Decoded message : 'UKRAINE'