TUT-8

Name:- Soumen Samanta
Batch - B1
16010420133

Q1] Show that how RSA algorithm can be used for encryption & decryption using following values.

$p = 7, q = 11, m = 3$

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

$\phi(n) = (p-1)(q-1)$
$= (7-1)(11-1)$
$\phi(n) = 60$

For value of e,

$1 < e < 60$
$\gcd(e, \phi(n)) = 1$
$e = 7$

for finding d.

$1 \equiv ed \bmod \phi(n)$
$1 \equiv 7d \bmod 60$
$d = 43$

public key = $\{e, n\} = \{7, 77\}$
private key = $\{d, n\} = \{43, 77\}$

Here m=3

Encryption

$c = m^e \bmod n$

$= 3^{-7} \bmod 77$

$= 2187 \bmod 77$

$c = 31$

Decryption

$M = C^d \bmod n$

$= 31^{43} \bmod 77$

$= (31^2)^{21} \cdot 31 \cdot \bmod 77$

$= ((31^2 \bmod 77)^{21} \bmod 77)(31 \bmod 77) \bmod 77$

$= ((31^2 \bmod 77)^{21} \bmod 77) 31 \bmod 77$

$= ((37)^{21} \bmod 77) 31 \bmod 77.$

$= ((37^2)^{10} 37 \bmod 77) \cdot 31 \bmod 77$

$= ((((37^2 \bmod 77)^{10} \bmod 77)(37 \bmod 77)) \bmod 77).$
$31 \bmod 77$

∴ So after doing all the operations again we get.

$= ((12146 \bmod 77) 37 \bmod 77) \cdot 31 \bmod 77)$
$(67 \cdot 37 \bmod 77) \cdot 31 \bmod 77$

$= [2479 \bmod 77] \cdot 31 \bmod 77$

~~$= 15 \cdot 31 \bmod$~~

$= 15 \cdot 31 \bmod 77 = 465 \bmod 77$

$M = 3$

Q2] use the vigenere cipher method to encode & decode the message "GIRAFFE" using the encryption key "XYZ".

P.T - GIRAFFE

key - X Y Z

23 24 25

Encryption:

main Text	G	I	R	A	F	F	E	
value of PT(Pi)	6	8	17	0	5	5	4	
ki	23	24	25	23	24	25	23	
$C_i \equiv (P_i + k_i) \bmod 26$	3	6	16	23	3	4	1	
T	D	G	Q	X	D	E	B	

Decryption:

$D_i = (C_i - k_i) \bmod 26$

D	G	Q	X	D	E	B	
6	8	17	0	5	5	4	
G	I	R	A	F	F	E	

Q3] Use the Affine substitution cipher to encode & decode the message "UKRAINE" Assume the values a=9, b=2, m=26

Plain Text = U K R A I N E

Encryption :- $y = (ax+b) \bmod m$.

Plain Text	U	K	R	A	I	N	E
x	20	10	17	0	8	13	4
$9x+2$	182	92	155	2	74	119	38
y	0	14	25	2	22	15	12
Cipher Text	A	O	Z	C	W	P	M

Encoded msg : AOZCWPM.

Decryption :- $D(Y) = (a^{-1}(y-b)) \bmod 26$

$\therefore a = 9, b = 2,$ & $a^{-1} = x$

x value should be such that $9x \bmod 26 = 1$

$9x \bmod 26 = 1$

$\therefore 9 \times 3 \bmod 26 = 1 \quad \therefore 27 \bmod 26 = 1$

$\therefore x = 3$

$\therefore D(Y) = 3(y-b) \bmod 26 = 3(y-2) \bmod 26$

Cipher Text	A	O	Z	C	W	P	M
y	0	14	25	2	22	15	12
$3(y-2)$	20	36	69	0	60	39	30
$D(Y)$	20	10	17	0	8	13	4
Plain Text	U	K	R	A	I	N	E

Decoded message : UKRAINE.