Problems on RSA

1. $p = 7$, $q = 11$, $e = 13$, P.T $= 17$

<u>Sol</u>: $n = p \times q = 7 \times 11 = 77$ Modulus

$\phi(n) = (p-1)(q-1) = 6 \times 10 = 60$ Totient Function

Now, Calculate d

$(d \times e) \bmod \phi(n) \equiv 1$

$\Rightarrow (d \times 13) \bmod 60 \equiv 1$

e $\phi(n)$

We solve for 'd' using Extended Euclidean Algorithm.

As $\phi n = 60$

$e = 13$

Row	a	b	d	k
1	1	0	60	—
2	0	1	13	4
3	1	-4	8	1
4	-1	5	5	1
5	2	-9	3	1
6	-3	14	2	1
7	5	-23	1	2

ϕn e

If d is negative.

$\therefore d_{New} = d_{old} + \phi(n)$

$= -23 + 60$

$\therefore \boxed{d = 37}$

Public key $\Rightarrow (e, n) \Rightarrow (13, 77)$

Private key $\Rightarrow (d, n) \Rightarrow (37, 77)$

For Encryption

$$CT = (PT)^e \bmod n$$

$$= (17)^{13} \bmod 77$$

$$= (17)^{8+4+1} \bmod 77$$

$$= (37 \times 53 \times 17) \bmod 77$$

$$\therefore \boxed{CT = 73}$$

$17 \bmod 77 = 17$

$\Rightarrow 17^2 \bmod 77 = 58$

$\Rightarrow 17^4 \bmod 77 = (58)^2 \bmod 77 = 53$

$\Rightarrow (17)^8 \bmod 77 = (53)^2 \bmod 77 = 37$

Public key $\Rightarrow (e, n) \Rightarrow (3, 77)$

Private key $\Rightarrow (d, n) \Rightarrow (37, 77)$

For Decryption

$$PT = (CT)^d \bmod n$$

$$= (73)^{37} \bmod 77$$

$$= (73^{32+4+1}) \bmod 77$$

$$= (16 \times 25 \times 73) \bmod 77$$

$\therefore$ $\boxed{PT = 17}$

$\because$ $73 \bmod 77 = 73$

$\Rightarrow (73)^2 \bmod 77 = 16$

$\Rightarrow (73)^4 \bmod 77 = (16)^2 \% 77 = 25$

$\Rightarrow (73)^8 \bmod 77 = (25)^2 \% 77 = 9$

$\Rightarrow (73)^{16} \bmod 77 = (9)^2 \% 77 = 4$

$\Rightarrow (73)^{32} \bmod 77 = (4)^2 \% 77 = 16$

Q.2 $p = 3$, $q = 11$, $M = 12$, Apply RSA to encrypt & decrypt.

Sol:

$$n = p \times q = 3 \times 11 = 33$$

$$\phi(n) = (p-1)(q-1) = 2 \times 10 = 20$$

Find 'e' such that it is relatively prime to $\phi(n)$

(Generally, we don't take e having same value as either p or q even if it's relatively prime to $\phi(n)$)

$$\boxed{\therefore \; e = \qquad}$$

$e = 7,$

$\therefore$ find 'd' such that $(e \times d) \bmod \phi(n) \equiv 1$

$\therefore (7 \times d) \bmod (20) \equiv 1$

$\therefore$ By Extended Euclidean Algorithm

Row	a	b	d	K
1	1	0	20	—
2	0	1	7	2
3	1	-2	6	1
4	-1	3	1	6

$\therefore d = 3$

As

$7 \times 3 = 21$

$\because 21 \bmod 20 = 1$

For Encryption,

$$CT = (PT)^{e} \bmod n$$

$$= (12)^{7} \bmod 33$$

Now, $12 \bmod 33 = 12$

$12^{2} \bmod 33 = 12$

$12^{4} \bmod 33 = 12$

$\vdots$

$\therefore (12)^{7} \bmod 33 = 12^{1+2+4} \bmod 33$

$$\boxed{CT = (12 \times 12 \times 12) \% 33 = 12}$$

For Decryption

$$PT = (CT)^{d} \bmod 33$$

$$= (12)^{3} \bmod 33$$

$$\Rightarrow 12^{1+2} \bmod 33$$

$$\Rightarrow (12 \times 12) \bmod 33$$

$$\Rightarrow 144 \% 33$$

$$\boxed{PT \Rightarrow 12}$$

Hence Proved

Q.3. $p=7$, $q=11$, $e=17$, $M=25$

Sol: $n = 7 \times 11 = 77$

$\phi(n) = 6 \times 10 = 60$

$e = 17$

Find d ?

Using Extended Euclidean Algorithm

Row	a	b	d	k
1	1	0	60	–
2	0	1	17	3
3	1	-3	9	1
4	-1	4	8	1
5	2	$\boxed{-7}$	1	8

As $d = -7$

So we need to make it positive by adding $\phi(n)$

$$\therefore d = -7 + \phi(n)$$

$$\Rightarrow -7 + 60$$

$$\Rightarrow 53$$

Encryption: $CT = (PT)^e \bmod n$

$$= (25)^{17} \bmod 77$$

$$(25)^{17} = \underbrace{25^{1+16} \bmod 77}$$

$$\Rightarrow 25^2 \bmod 77 = 9$$

$$\Rightarrow 25^4 \bmod 77 = (9)^2 \bmod 77 = 4$$

$$\Rightarrow 25^8 \bmod 77 = (4)^2 \bmod 77 = 16$$

$$\Rightarrow (25)^{16} \bmod 77 = 25$$

$$\therefore \boxed{CT = (25 \times 25) \bmod 77 = 9}$$

Decryption:

$$PT = (CT)^d \bmod n$$
$$= (9)^{53} \bmod 77$$

$9 \bmod 77 = 9$

$9^2 \bmod 77 = 4$

$9^4 \bmod 77 = 16$

$9^8 \bmod 77 = 25$

$9^{16} \bmod 77 = 9$

$9^{32} \bmod 77 = 4$

$$\because (9)^{53} = 9^{1+4+16+32}$$

$$\therefore (9)^{53} \bmod 77 = (9 \times 16 \times 9 \times 4) \bmod 77$$
$$= (5184) \bmod 77$$

$$\therefore \boxed{PT = 25}$$

Hence Proved

Q.4: For the given parameters $p = 3$, $q = 19$, find the value of 'e' & 'd' using RSA algorithm & encrypt the message $M = 6$.

Sol:

$$n = p \times q = 3 \times 19 = 57$$

$$\phi(n) = (p-1)(q-1) = 36$$

So we choose 'e' =

Hence $d =$

Using Extended Euclidean Algorithm

Row	a	b	d	k
1	1	0	36	–
2	0	1	5	7
3	1	−7	1	5

Encryption

$CT = (PT)^e \bmod n$

$= (6)^5 \bmod 57$

$\Rightarrow (6)^{1+4} \bmod 57$

1959552

34378

$\because 6^2 \bmod 57 = 36$

$6^4 \bmod 57 = 42$

$\therefore 6^5 \bmod 57 = (6 \times 42) \bmod 57$

$\boxed{CT = 24}$

Decryption

$PT = (CT)^d \bmod n$

$= (24)^{29} \bmod 57$

$\Rightarrow (24)^{1+4+8+16} \bmod 57$

$\because (24)^2 \bmod 57 = 6$

$(24)^4 \bmod 57 = 36$

$(24)^8 \bmod 57 = 42$

$(24)^{16} \bmod 57 = 54$

$\therefore (24)^{29} \bmod 57 = (24 \times 36 \times 42 \times 54) \bmod 57$

$\therefore \boxed{PT \Rightarrow 6}$