Paillier Encryption numerical :-

1. Public key (n, g)

$n \longrightarrow$ product of two large primes nos. p & q. $(p \times q)$

$g : \longrightarrow$ Integer in $Z^*_{n^2}$ (multiplicative group) of integers.

2. Private key. (λ, μ)

$$\lambda = LCM (p-1)(q-1)$$

$$\mu = (L(g^\lambda \bmod n^2))^{-1} \bmod n$$

3. Encryption [Encrypt message m] by :-

$$C = g^m \cdot r^n \bmod n^2$$

[r is random number $\in Z_n^*$]

4. Decryption :- Compute m for ciphertext C.

$$m = L((C^\lambda \bmod n^2) \cdot \mu \bmod n) \cdot \mu \bmod n.$$

p, q, g, m & r provided. sometimes C & μ.

Numerical :-

Given :- $p = 7$ & $q = 11$

1. Calculate $n = p \times q = 77$

2. Compute $n^2 = 77 \times 77 = 5929$

3. Compute $\lambda = lcm(p-1, q-1)$

$= LCM(6, 10)$

$= 30$

3. g will be given $= 5652$

4. Compute $\mu = (L(g^\lambda \bmod n^2))^{-1} \bmod n$

→ Calculating $g^\lambda \bmod n^2$ first.

$5652^{30} \bmod 5929 = 3928$

→ Now Calculate $L(x) = \frac{x-1}{n}$

Here $x = g^\lambda \bmod n^2 = 3928$

So, $L(3928) = \frac{3928-1}{77} = 51$

→ Compute μ, finally :-

$\mu = 51^{-1} \bmod 77 = 74$

public key $(n, g) = (77, 5652)$

private key $(\lambda, \mu) = (30, 74)$

5. Encryption:- $m = 42$ [given message length.]

$r = 23$ [given] → random number.

→ Compute ciphertext.

$c = g^m \cdot r^n \bmod n^2$ [learn]

break & solve

→ $g^m \bmod n^2 = 5652^{42} \bmod 5929$

$= 4137.$

→ Compute. $r^n \bmod n^2$

~~$5652^{42} \bmod 5929 = 4$~~

$23^{77} \bmod 5929 = 4852$

→ Compute $c = (4137 \cdot 4852) \bmod 5929$

$= 4624$

6. ciphertext $c = 4624.$

7. Decryption:-

$m = (L(c^\lambda \bmod n^2) \cdot \mu) \bmod n$

→ Compute $c^\lambda \bmod n^2$

$4624^{30} \bmod 5929 = 4852$

→ Compute $L(x) = \frac{x-1}{n}$

$L(4852) = \frac{4852-1}{77} = 42$ u

$m = (42 \cdot 74) \bmod 77 = 42$

Decrypted message $m = 42$ u