RSA Key generation:

1. Choose two large prime numbers they should not be equal
2. Compute the modulus **n**, n = p \* q
3. Compute the euler’s totient, **ϕ(n)**=(p−1)×(q−1)
4. Select an integer **e** such that 1<**e**<ϕ(n) and e is coprime with ϕ(n). Common choices for e include 3, 17, and 65537 due to their efficient properties.
5. Compute the Private Exponent **d**, d×e≡1(modϕ(n))
6. Form the Public and Private Keys
   1. **Public Key**: (e,n)
   2. **Private Key**: (d,n)
7. Encryption: **c=m^e(mod n)**
   1. Where m is the plaintext represented as integer
8. Decryption **m=c^d(mod n)**

**Solving:**

Q.1]

Solution:

Choose p = 3 and q = 11

Compute n = p \* q = 33

Computer ϕ(n) = (p -1)(q-1) = 20

Let e = 7

Compute a value for d such that (d\*e) % ϕ(n) = 1. One solution is d = 3 [3(3\*7)%20 = 1]

Public key is (7,33)

Private key is (3,33)

**A] for 3, 4, 1**

pt = 3

p = 3, q = 11, n = 33

e = 7

d = 3

encryption of "3" => 3^7 % 33 = 9

decryption of "9" => 9^3 % 33 = 3

encryption of "4" => 4^7 % 33 = 16384 mod 33 => 16

decryption of "16" => 16^3 % 33 = 4096 mod 33 => 4

encryption of "1" => 1^7 % 33 = 1 mod 33 => 1

decryption of "1" => 1^3 % 33 = 1 mod 33 => 1