**# SOHAM CHAVAN 11**

**import math**

**# setting the values of p and q (two distinct prime numbers)**

**p = 3**

**q = 7**

**# calculating n**

**n = p\*q**

**print("n =", n)**

**# calculating eulers totient function**

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

**# e = public exponent**

**e = 2**

**while(e<phi):**

**if (math.gcd(e, phi) == 1):**

**break**

**else:**

**e += 1**

**print("e =", e)**

**# step 5**

**k = 2**

**d = ((k\*phi)+1)/e**

**print("d =", d)**

**print(f'Public key: {e, n}')**

**print(f'Private key: {d, n}')**

**# plain text**

**msg = 11**

**print(f'Original message:{msg}')**

**# encryption**

**C = pow(msg, e)**

**C = math.fmod(C, n)**

**print(f'Encrypted message: {C}')**

**# decryption**

**M = pow(C, d)**

**M = math.fmod(M, n)**

**print(f'Decrypted message: {M}')**

