Assignment 4

Network Security (UCS727)

Name:	Sachleen Singh Chani
Roll No.:	101506143
Date:	May 2021

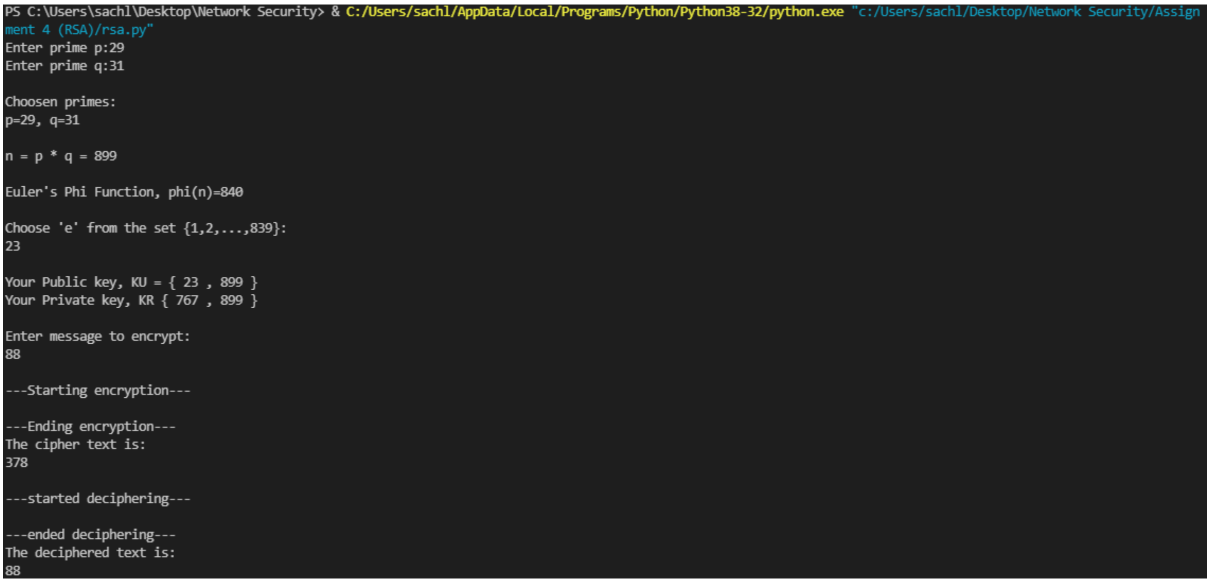
Q1. Write a program to implement the RSA public-key encryption.

Answer:

Code –

```
#RSA encryption
#extended Euclidean algorithm
def egcd(a,b):
    if(a<b):
        a, b = b, a
    if(b==0):
        return a,0,1

    g,t1,s1 = egcd(b, a%b)
    t = s1 - a//b * t1
    s = t1

    return g,t,s


#encryption fucntion
def enc(plain,public):
    print("\n---Starting encryption---")

    e,n = public

    cipher = plain**e % n

    print("\n---Ending encryption---")
    return cipher


def denc(cipher,private):
    print("\n---started deciphering---")

    d,n = private

    decipher = cipher**d % n

    print("\n---ended deciphering---")
    return decipher


#key generation
p = int(input("Enter prime p:"))
q = int(input("Enter prime q:"))
print("\nChoosen primes: \np=" + str(p) + ", q=" + str(q) + "\n")

n = p * q
print("n = p * q = " + str(n) + "\n")

phi = (p-1) * (q-1)
print("Euler's Phi Function, phi(n)=" + str(phi) + "\n")

print("Choose \'e\' from the set {1,2,...,%d}:" %(phi-1))
e = int(input())

g,d,s = egcd(e, phi)

#to make sure e is a coprime number
while(g!=1):
    e=int(input("'e' should be coprime to phi! e="))
    g,d,s = egcd(e,phi)

#to make the inverse as a positive integer
while(d<0):
    d += phi

#public and private keys
public  = (e,n)
private = (d,n)
print("\nYour Public key, KU = {",e,",",n,"}")
print("Your Private key, KR {",d,",",n,"}")

#user input plain text
print("\nEnter message to encrypt:")
plain = int(input())

#calling cipher function
cipher = enc(plain,public)
print("The cipher text is:")
print(cipher)

#calling decipher function
decipher = denc(cipher,private)
print("The deciphered text is:")
print(decipher)
```

Result –



```
PS C:\Users\sachl\Desktop\Network Security> & C:/Users/sachl/AppData/Local/Programs/Python/Python38-32/python.exe "c:/Users/sachl/Desktop/Network Security/Assign
ment 4 (RSA)/rsa.py"
Enter prime p:29
Enter prime q:31

Choosen primes:
p=29, q=31

n = p * q = 899

Euler's Phi Function, phi(n)=840

Choose 'e' from the set {1,2,...,839}:
23

Your Public key, KU = { 23 , 899 }
Your Private key, KR { 767 , 899 }

Enter message to encrypt:
88

---Starting encryption---

---Ending encryption---
The cipher text is:
378

---started deciphering---

---ended deciphering---
The deciphered text is:
88
```

Figure 1 Result for RSA encryption