

ASSIGNMENT – 4

CSCI-6708 Advanced Network Security

Exercise 2

Sumit Singh

B00882103

Sm435410@dal.ca

Sample input 1:

P = 11

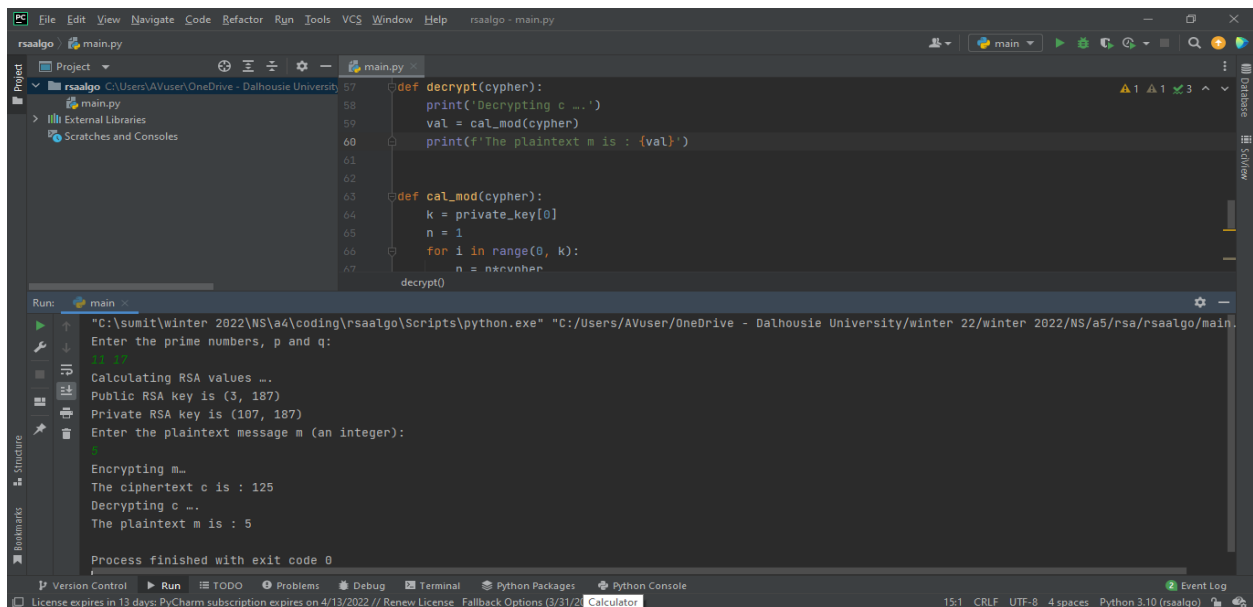
q = 17

Public key = (3, 187)

Private Key = (107, 187)

m = 5

c = 125



The screenshot shows a Python IDE with a project named 'rsaalgo'. The main.py file contains the following code:

```
def decrypt(cypher):
    print('Decrypting c ...')
    val = cal_mod(cypher)
    print(f'The plaintext m is : {val}')

def cal_mod(cypher):
    k = private_key[0]
    n = 1
    for i in range(0, k):
        n = n*cypher
```

The Run window shows the execution output:

```
"C:\sumit\winter 2022\NS\A4\coding\rsaalgo\Scripts\python.exe" "C:/Users/AVuser/OneDrive - Dalhousie University/winter 22/winter 2022/NS/a5/rsa/rsaalgo/main.py"
Enter the prime numbers, p and q:
11 17
Calculating RSA values ...
Public RSA key is (3, 187)
Private RSA key is (107, 187)
Enter the plaintext message m (an integer):
5
Encrypting m...
The ciphertext c is : 125
Decrypting c ...
The plaintext m is : 5
Process finished with exit code 0
```

Sample input 2:

P = 31

q = 47

Public key = (7, 1457)

Private Key = (1183, 1457)

m = 20

c = 731

The screenshot shows a PyCharm IDE with a Python script named `main.py`. The script defines two functions: `decrypt(cypher)` and `cal_mod(cypher)`. The `decrypt` function prints "Decrypting c ...", calls `cal_mod`, and prints the result. The `cal_mod` function uses a private key `private_key[0]` to calculate the plaintext `m` from the ciphertext `c`. The Run window shows the following output:

```
Enter the prime numbers, p and q:
11 47
Calculating RSA values ...
Public RSA key is (7, 1457)
Private RSA key is (1183, 1457)
Enter the plaintext message m (an integer):
20
Encrypting m...
The ciphertext c is : 731
Decrypting c ...
The plaintext m is : 20
Process finished with exit code 0
```

Sample input 3:

P = 313

q = 109

Public key = (5, 34117)

Private Key = (26957, 34117)

m = 100

c = 247

The screenshot shows the same PyCharm IDE with the `main.py` script. The Run window shows the following output for sample input 3:

```
Enter the prime numbers, p and q:
313 109
Calculating RSA values ...
Public RSA key is (5, 34117)
Private RSA key is (26957, 34117)
Enter the plaintext message m (an integer):
100
Encrypting m...
The ciphertext c is : 247
Decrypting c ...
The plaintext m is : 100
Process finished with exit code 0
```

