RSA Algorithm
Cryptography – Lab 4

Name: Ojas Patil
Reg No: 21BAI1106

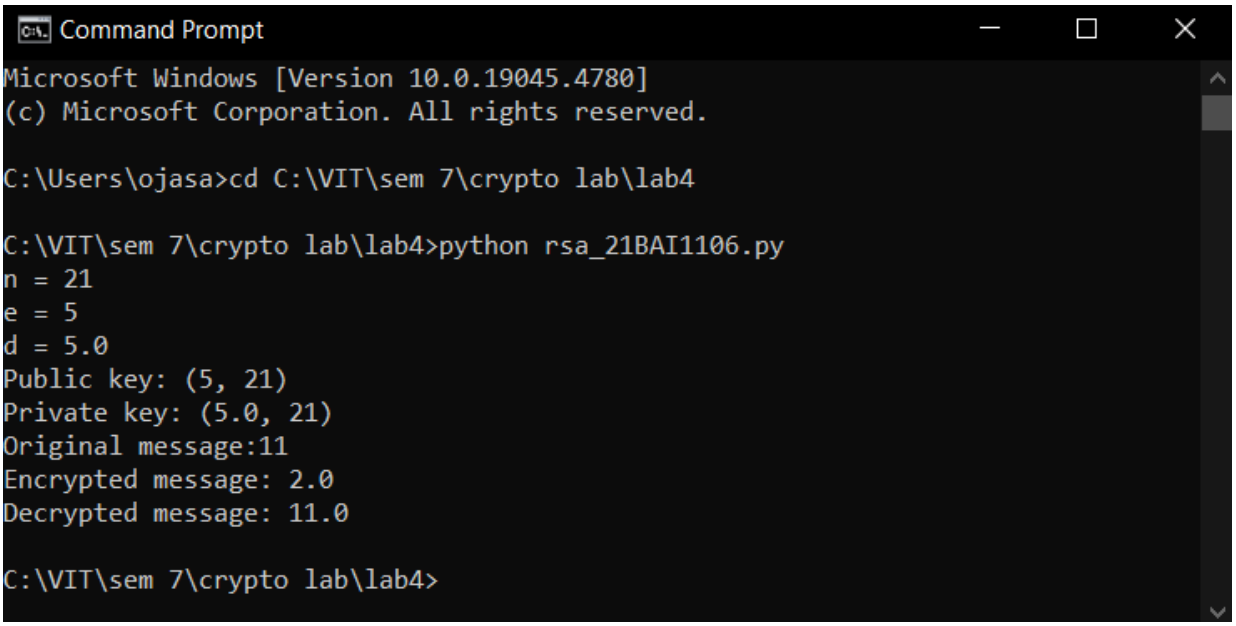
Task

To Develop a Python-based RSA Algorithm implementation.

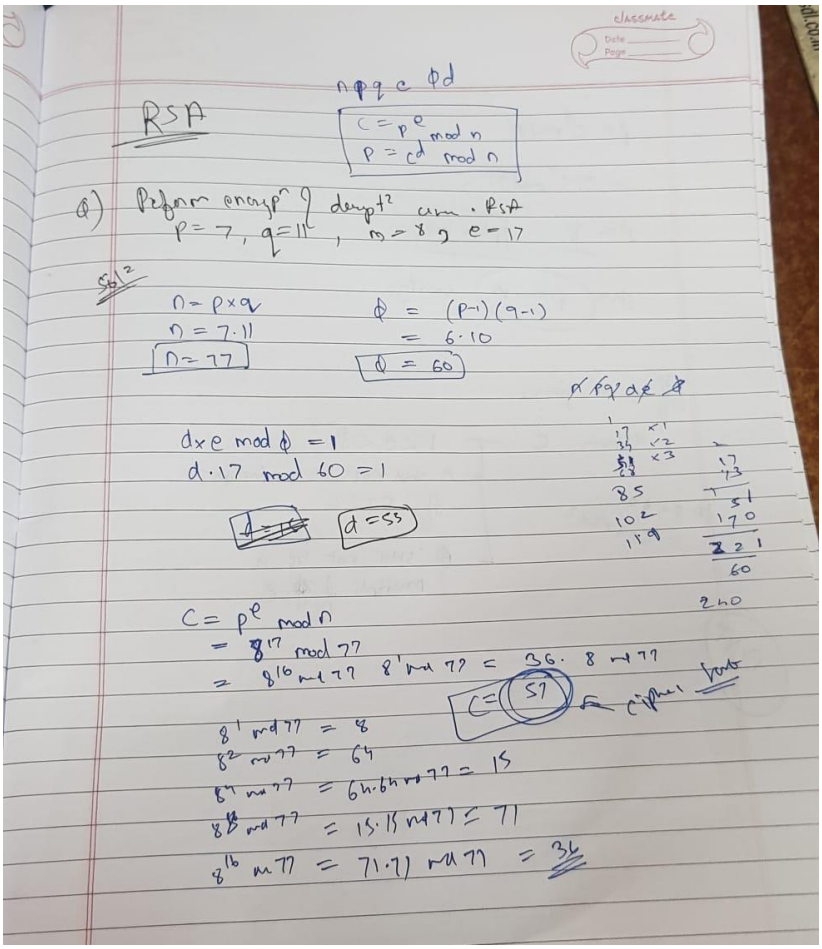
RSA Algorithm - Definition

RSA algorithm is an asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. **Public Key** and **Private Key.** As the name describes that the Public Key is given to everyone and the Private key is kept private.

RSA Algorithm - Output Snapshot



RSA - Handwritten sum



Source Code

```
import math

# step 1
p = 3
q = 7

# step 2
n = p*q
print("n =", n)

# step 3
phi = (p-1)*(q-1)

# step 4
```

```
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}')
```

Conclusion

The implementation of RSA Algorithm in Python successfully demonstrates the core components of the algorithm and provides a foundational understanding of RSA and its practical application in securing data.