Ganpat University

॥ विद्यया समाजोत्कर्षः ॥

Institute of Computer Technology

Name: Tushar Panchal

En.No: 21162101014

Sub: INS (INFORMATION SECURITY)

Branch: CBA

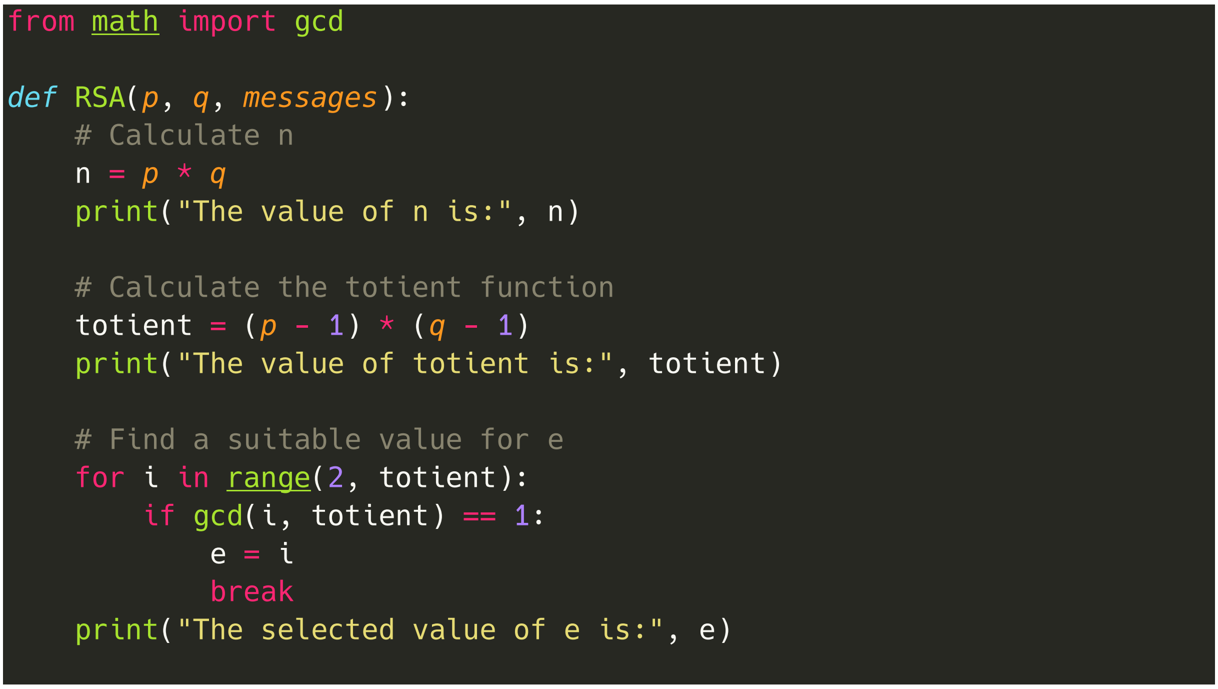
Batch:61

-----------------------------PRACTICAL 07-----------------------------

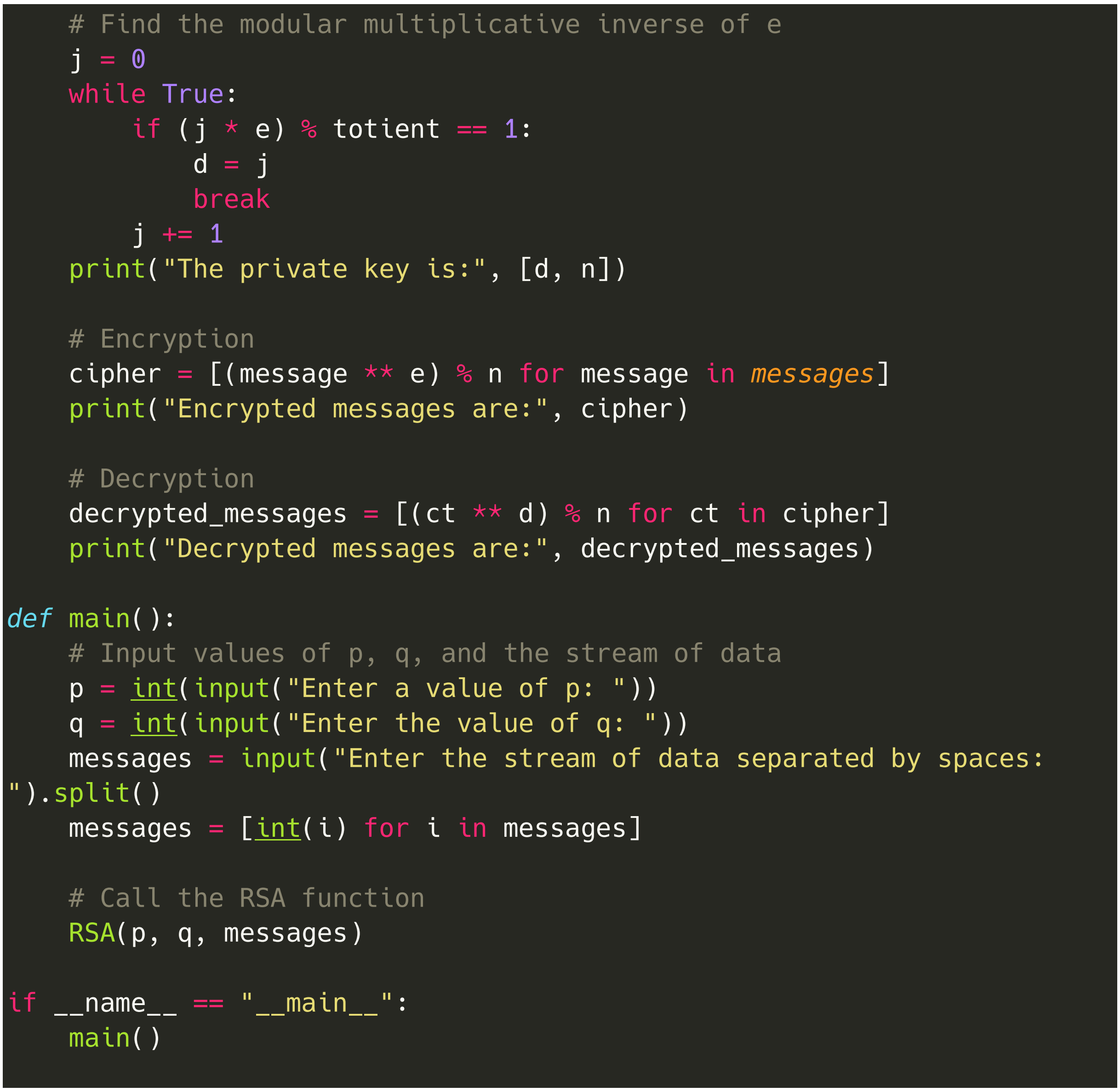
❖ AIM :

An organization wants to achieve encryption of data using Asymmetric key cryptography. The Public key will be available to all employee, and private key will be individual for each employee for communication. Your task is to find out Public key for organization and private key for 1 employee. Also provide how data will be encrypted using this public key & private key.

✓ Source Code :

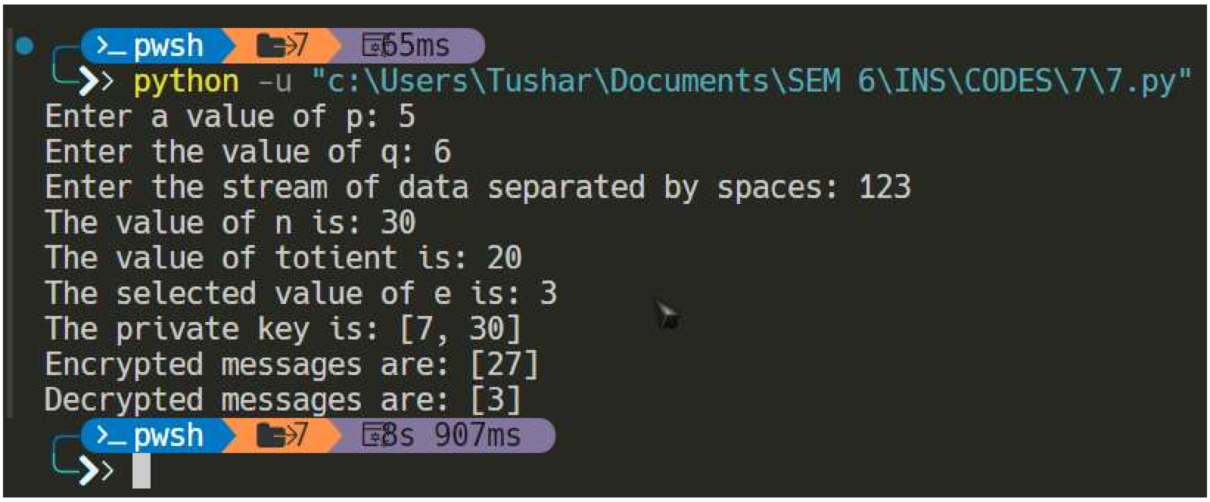


```python
from math import gcd

def RSA(p, q, messages):
    # Calculate n
    n = p * q
    print("The value of n is:", n)

    # Calculate the totient function
    totient = (p - 1) * (q - 1)
    print("The value of totient is:", totient)

    # Find a suitable value for e
    for i in range(2, totient):
        if gcd(i, totient) == 1:
            e = i
            break
    print("The selected value of e is:", e)
```



```
    # Find the modular multiplicative inverse of e
    j = 0
    while True:
        if (j * e) % totient == 1:
            d = j
            break
        j += 1
    print("The private key is:", [d, n])

    # Encryption
    cipher = [(message ** e) % n for message in messages]
    print("Encrypted messages are:", cipher)

    # Decryption
    decrypted_messages = [(ct ** d) % n for ct in cipher]
    print("Decrypted messages are:", decrypted_messages)

def main():
    # Input values of p, q, and the stream of data
    p = int(input("Enter a value of p: "))
    q = int(input("Enter the value of q: "))
    messages = input("Enter the stream of data separated by spaces:
").split()
    messages = [int(i) for i in messages]

    # Call the RSA function
    RSA(p, q, messages)

if __name__ == "__main__":
    main()
```

- ✓ **Output :**



```
 >_ pwsh   7   65ms
 >> python -u "c:\Users\Tushar\Documents\SEM 6\INS\CODES\7\7.py"
 Enter a value of p: 5
 Enter the value of q: 6
 Enter the stream of data separated by spaces: 123
 The value of n is: 30
 The value of totient is: 20
 The selected value of e is: 3
 The private key is: [7, 30]
 Encrypted messages are: [27]
 Decrypted messages are: [3]
 >_ pwsh   7   8s 907ms
 >>
```