EXP NO: 2a
DATE: 02/03/24

RSA ALGORITHM

AIM:

To write a python program implementing the RSA algorithm

ALGORITHM:

1. Choose two large prime numbers (p and q)
2. Calculate n = p*q and z = (p-1)(q-1)
3. Choose a number e where 1 < e < z.
4. Calculate d = e-1mod(p-1)(q-1)
5. You can bundle private key pair as (n,d)
6. You can bundle public key pair as (n,e)

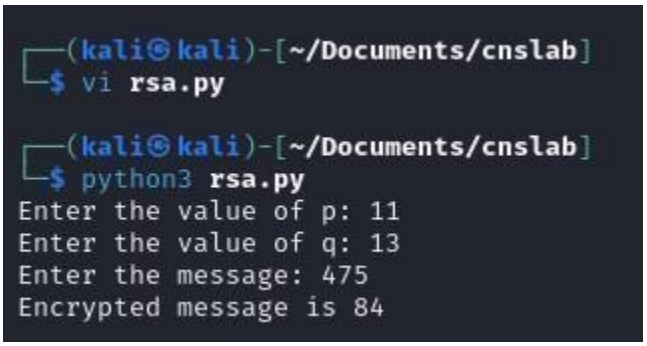
Encrypt using public key and decrypt using private key

PROGRAM:

```
from math import gcd

# defining a function to perform RSA approch
def RSA(p: int, q: int, message: int):
    # calculating n
    n = p * q

    # calculating totient, t
    t = (p - 1) * (q - 1)

    # selecting public key, e
    for i in range(2, t):
        if gcd(i, t) == 1:
            e = i
            break

    # selecting private key, d
    j = 0
    while True:
        if (j * e) % t == 1:
            d = j
            break
        j += 1

    # performing encryption
    ct = (message ** e) % n
    print(f"Encrypted message is {ct}")
```

```
    # performing decryption
    mes = (ct ** d) % n
    print(f"Decrypted message is {mes}")

p=int(input("Enter the value of p: "))
q=int(input("Enter the value of q: "))
msg=int(input("Enter the message: "))
RSA(p,q,msg)
```

OUTPUT:



RESULT:

Thus, a python program is implemented to demonstrate RSA Algorithm.