EX NO:4 **REGNO: 210701509**

DATE:

RSA ALGORITHM

AIM:

To implement RSA algorithm with key generation, encryption and decryption for the user input message.

ALGORITHM:

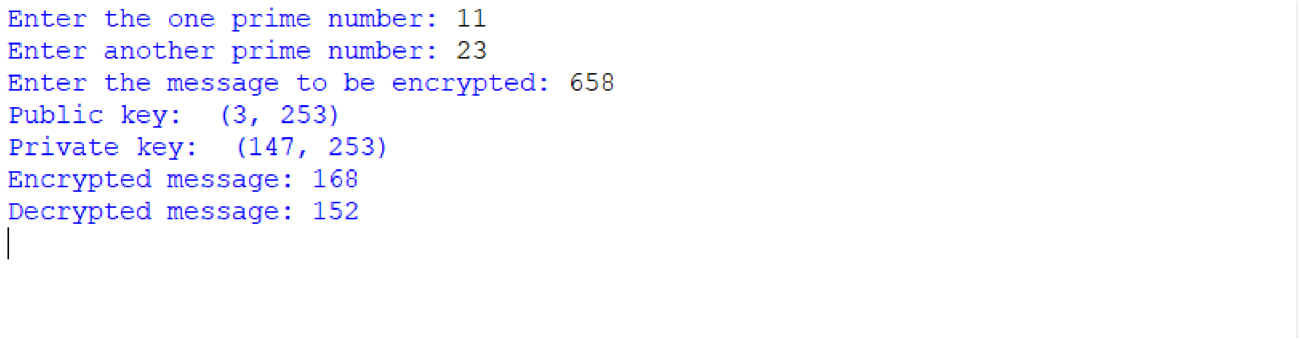
- Get two prime numbers P and Q from the user
- Initiate generate_keypair() function to create public key and private key
- Public key will be selected based on satisfying of conditions
- Private key will be found based on D=E^{-1}mod ((P-1)*(Q-1))
- Get the message from the user to be encrypted
- Encrypted the message using public key
- Decrypt the message using private key

PROGRAM:

```
import math

def gcd(a, b):
    while b != 0:
        a, b = b, a % b
    return a

def generate_keypair(p, q):
    n = p * q
    phi = (p - 1) * (q - 1)

    e = 3
    while gcd(e, phi) != 1:
        e += 2

    d = pow(e, -1, phi)

    return ((e, n), (d, n))

def encrypt(pk, message):
    key, n = pk
    cipher = (message ** key) % n
    return cipher

def decrypt(pk, ciphertext):
    key, n = pk
    plain = (ciphertext ** key) % n
    return plain

p = int(input("Enter the one prime number: "))
q = int(input("Enter another prime number: "))
public, private = generate_keypair(p, q)
```

```
message = int(input("Enter the message to be encrypted: "))
print("Public key: ",public)
print("Private key: ",private)
encrypted_msg = encrypt(public, message)
print("Encrypted message:", encrypted_msg)

decrypted_msg = decrypt(private, encrypted_msg)
print("Decrypted message:", decrypted_msg)
```

OUTPUT:



```
Enter the one prime number: 11
Enter another prime number: 23
Enter the message to be encrypted: 658
Public key:  (3, 253)
Private key:  (147, 253)
Encrypted message: 168
Decrypted message: 152
```

RESULT: