EXP NO: 2a
DATE:

RSA ALGORITHM

AIM:

To write a C program to implement and perform RSA algorithm

ALGORITHM:

Step 1 : Start.

Step 2 : Include necessary header files.

Step 3 : Create a function for calculating GCD(Greatest Common Divisor).

Step 4 : Define GCD function.

Step 5 : Create a function for encryption and decryption process.

Step 6 : Define encryption and decryption function.

Step 7 : Call both encryption and decryption function inside main function.

Step 8 : End.

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:

```
┌──(kali㉿kali)-[~/Documents/cnslab]
└─$ vi rsa.py

┌──(kali㉿kali)-[~/Documents/cnslab]
└─$ python3 rsa.py
Enter the value of p: 11
Enter the value of q: 13
Enter the message: 475
Encrypted message is 84
```

RESULT:

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