

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 $d = e^{-1} \bmod (p-1)(q-1)$
 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 approach
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

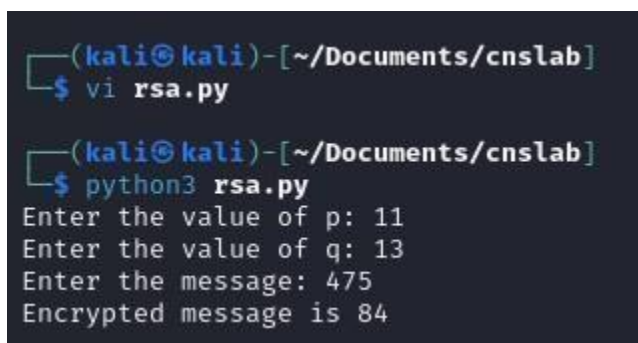
    # selecting private key, d
    j = 0
    while True:
        if (j * e) % t == 1:
            d = j
            break
        j += 1

    # 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:

A terminal window with a dark background and light blue text. The prompt is '(kali@kali)-[~/Documents/cnslab]'. The user enters '\$ vi rsa.py'. The prompt changes to '\$ python3 rsa.py'. The user enters '11' for p, '13' for q, and '475' for the message. The output is 'Encrypted message is 84'.

```
(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.