Exp: 2A **RSA Algorithm**
Date: 02-03-2024

Aim:

To write a python program implementing the RSA algorithm.

Algorithm:

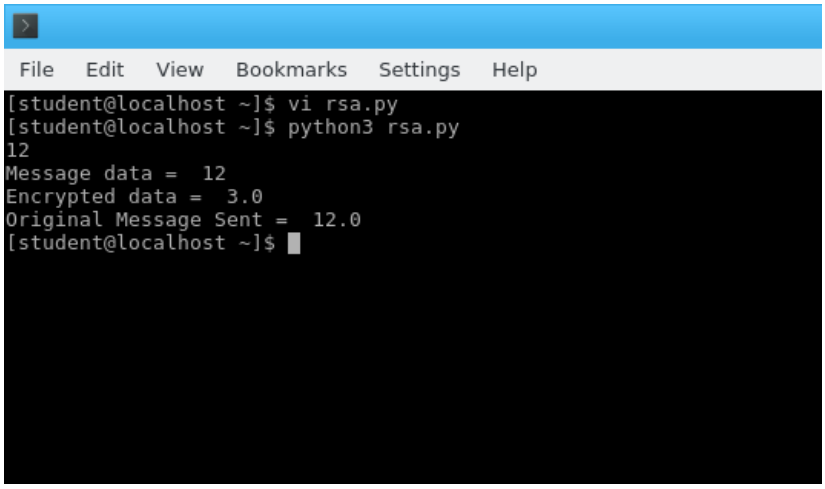
1. Choose two large prime numbers (p and q)
2. Calculate n = p*q and z = (p-1)(q-1)
3. Choose a number e where 1 < e < z.
4. Calculate d = e-1mod(p-1)(q-1)
5. You can bundle private key pair as (n,d)
6. You can bundle public key pair as (n,e)
7. Encrypt using public key and decrypt using private key.

Program:

```
import math
def gcd(a, h):
    temp = 0
    while(1):
        temp = a % h
        if (temp == 0):
            return h
        a = h
        h = temp
p = 3
q = 7
n = p*q
e = 2
phi = (p-1)*(q-1)
while (e < phi):
     if(gcd(e, phi) == 1):
        break
    else:
        e = e+1
k = 2
```

```
d = (1 + (k*phi))/e
msg = int(input())
print("Message data = ", msg)
c = pow(msg, e)
c = math.fmod(c, n)
print("Encrypted data = ", c)
m = pow(c, d)
m = math.fmod(m, n)
print("Original Message Sent = ", m)
```

Output:



Result:

Thus the python program for RSA algorithm is implemented successfully.