RSA Algorithm

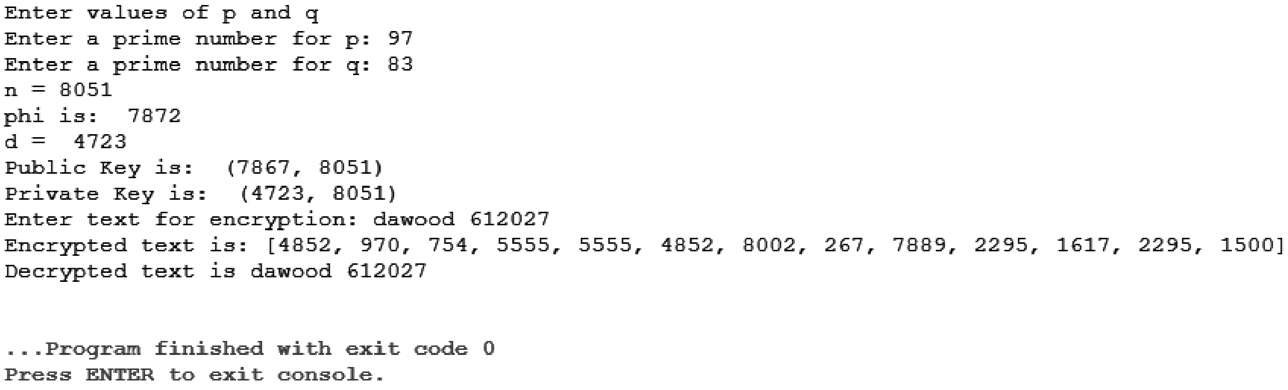
Code:

```
import math

def prime_check(a):
   if(a==2):
      return True
   elif((a<2) or ((a%2)==0)):
      return False
   elif(a>2):
      for i in range(2,a):
         if not(a%i):
            return False
      return True

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

def modinv(a, m):
   for x in range(1, m):
      if (a * x) % m == 1:
         return x
   return None

def coprimes(a):
   l = []
   for x in range(2, a):
      if gcd(a, x) == 1 and modinv(x,phi) != None:
         l.append(x)
   for x in l:
      if x == modinv(x,phi):
         l.remove(x)
   return l

def encrypt(pub_key,n_text):
   e,n=pub_key
   x=[]
```

```
    m=0
    for i in n_text:
        m= ord(i)
        c=(m**e)%n
        x.append(c)
    return x

def decrypt(priv_key,c_text):
    d,n=priv_key
    txt=c_text
    x=''

    m=0
    for i in txt:
        if(i=='400'):
            x+=' '
        else:
            m=(int(i)**d)%n
            c=chr(m)
            x+=c
    return x

print("Enter values of p and q")
p = int(input("Enter a prime number for p: "))
q = int(input("Enter a prime number for q: "))
check_p = prime_check(p)
check_q = prime_check(q)

while not (check_p and check_q):
    p = int(input("Enter a prime number for p: "))
    q = int(input("Enter a prime number for q: "))
    check_p = prime_check(p)
    check_q = prime_check(q)

n = p * q
print("n =",n)
phi = (p-1)*(q-1)
print("phi is: ",phi)

e = coprimes(phi)
e = e[len(e) - 1]
d = modinv(e,phi)
print("d = ", d)
```

```
public = (e,n)
private = (d,n)
print("Public Key is: ",public)
print("Private Key is: ",private)

text = input("Enter text for encryption: ")
c = encrypt(public, text)
print("Encrypted text is:", c)
t = decrypt(private, c)
print("Decrypted text is", t)
```

Output:



```
Enter values of p and q
Enter a prime number for p: 97
Enter a prime number for q: 83
n = 8051
phi is:  7872
d =  4723
Public Key is:  (7867, 8051)
Private Key is:  (4723, 8051)
Enter text for encryption: dawood 612027
Encrypted text is: [4852, 970, 754, 5555, 5555, 4852, 8002, 267, 7889, 2295, 1617, 2295, 1500]
Decrypted text is dawood 612027


...Program finished with exit code 0
Press ENTER to exit console.
```