Code:

```
import math


def gcd(a, b):
    if a == 0:
        return b


    return gcd(b % a, a)


def mod_Inv(A, M):
    for X in range(1, M):
        if (((A % M) * (X % M)) % M == 1):
            return X
    return -1


print("RSA Algorithm")
p = int(input("Enter value of p:"))
q = int(input("Enter value of q:"))


n = p * q
```

```
phi_n = (p-1) * (q-1)


e = 2
while (e < phi_n):
   if(gcd(e, phi_n) == 1):
      break
   else:
       e = e+1
print("Public key is", e)


k = 2
i = 0
d = mod_Inv(e, phi_n)
print("Private key is ",d)
print("1. Encryption\n2. Decryption")
option = int(input("Enter option number:"))

if option == 1:
   plain_text = int(input("Enter plain text:"))
   cipher_text = math.pow(plain_text, e)
   cipher_text = cipher_text % n
   print("Cipher text is ", cipher_text)

elif option == 2:
   cipher_text = int(input("Enter cipher text:"))
   plain_text = math.pow(cipher_text, d)
```

```
    plain_text = plain_text % n
    print("Plain text is ", plain_text)

else:
    print("Wrong option selected")
```