Name: Gaurang Vaghela
Rollno: TEAD-22561
Mini Project Lab
Practical 3
Problem Statement: Implementation of RSA Algorithm

Code:

```
import math

# Step 1
p = int(input("Enter the value for p: "))
q = int(input("Enter the value for q: "))

# Step 2: Compute n
n = p * q
print("n =", n)

# Step 3: Compute φ(n)
phi = (p - 1) * (q - 1)
print("φ(n) =", phi)

# Step 4: Choose e (must be coprime with φ(n))
e = int(input("Enter the value for e: "))

while math.gcd(e, phi) != 1:
    e += 1

print("e =", e)

# Step 5: Compute d (Modular Inverse of e mod φ(n))
d = pow(e, -1, phi)
print("d =", d)

print(f"Public Key: ({e}, {n})")
print(f"Private Key: ({d}, {n})")

# Step 6: Encryption
msg = int(input("Enter the message: "))
print(f"Original message: {msg}")

C = pow(msg, e, n)
print(f"Encrypted message: {C}")
```

```
# Step 7: Decryption
M = pow(C, d, n)
print(f"Decrypted message: {M}")
```

Output:

```
Enter the value for p:  7
Enter the value for q:  13
n = 91
ϕ(n) = 72
Enter the value for e:  5
e = 5
d = 29
Public Key: (5, 91)
Private Key: (29, 91)
Enter the message:  44
Original message: 44
Encrypted message: 18
Decrypted message: 44
```