D15B/37 **Mikil Lalwani** **Security Lab**

Experiment No 6

Aim-

Write a Program to Implement and analyze the RSA cryptosystem.

Theory-

RSA algorithm is an asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes, the Public Key is given to everyone and the Private key is kept private.
An example of asymmetric cryptography :
A client (for example browser) sends its public key to the server and requests some data.
The server encrypts the data using the client's public key and sends the encrypted data.
The client receives this data and decrypts it.
Since this is asymmetric, nobody else except the browser can decrypt the data even if a third party has the public key of the browser.
The idea! The idea of RSA is based on the fact that it is difficult to factorize a large integer. The public key consists of two numbers where one number is the multiplication of two large prime numbers. And private keys are also derived from the same two prime numbers. So if somebody can factorize the large number, the private key is compromised. Therefore, encryption strength lies in the key size; if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024-bit keys could be broken in the near future. But till now it seems to be an infeasible task.

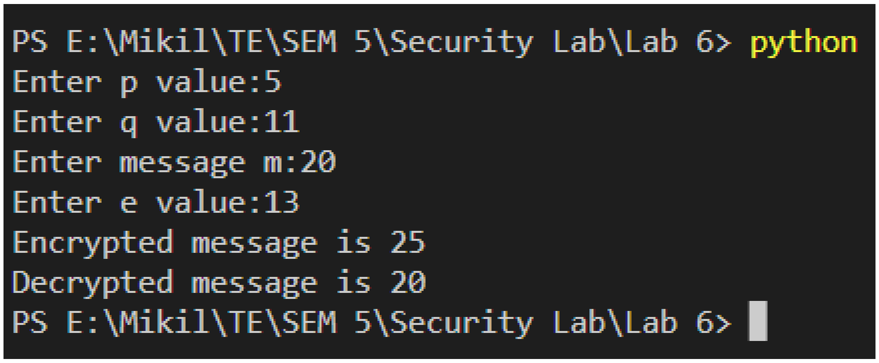
Algorithm-

1. Take the value of p,q,e, and m from the user.
2. Calculate n = p * q and phi(n) = (p-1)*(q-1).
3. Find the value of d = e mod phi(n).
4. The encrypted message is C = m^e * mod n.
5. The decrypted message is M = m^d * mod n.

Code-

```
def encrypt(m,e,n):
    C = (m ** e) % n
    return C

def decrypt(C,d,n):
    M = (C ** d) % n
    return M

def eea(a,b):
    t1 = 0
    t2 = 1

    q = a//b
    r = a%b
    t = t1 - t2*q

    while(r != 0):
        a = b
        b = r
        t1 = t2
        t2 = t

        q = a/b
        r = a%b
        t = t1 - t2*q
    return t2

p = int(input("Enter p value:"))
q = int(input("Enter q value:"))
m = int(input("Enter message m:"))
e = int(input("Enter e value:"))

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

d = eea(phi_n, e)
if(d<0):
    d = phi_n + d
C = encrypt(m, e, n)
M = decrypt(C, d, n)

print("Encrypted message is "+ str(C))
print("Decrypted message is "+ str(M))
```

Output -



```
PS E:\Mikil\TE\SEM 5\Security Lab\Lab 6> python
Enter p value:5
Enter q value:11
Enter message m:20
Enter e value:13
Encrypted message is 25
Decrypted message is 20
PS E:\Mikil\TE\SEM 5\Security Lab\Lab 6>
```

Conclusion-

Thus we have successfully written a Program to implement and analyze the RSA cryptosystem.