**Cryptography & Network Security-Lab 5**

1. Generate a public key and private key for the user who wish to use Public Key Infrastructure (PKI) like RSA to send the information through an insecure communication channel. The protocol for key-pair generation in RSA is given below:

* Generate two large random primes, p and q
* Compute n=pxq
* Compute ϕ=(p−1)(q−1)
* Choose an integer e, 1<e<ϕ, such that gcd(e,ϕ)=1
* Compute the secret exponent d, 1<d<ϕ, such that ed≡1modϕ
* The public key= (e, n)
* The private key (d, n)

1. Make use of the generated public-private key pair to encrypt and decrypt the messages from source to the destination. (Assume M=10)

**Encryption Process (Sender):**

* Use public key (e, n)
* Represents the plaintext message as a positive integer m with 1<m<n
* **Computes the ciphertext C=Me mod n**
* Sends the ciphertext C to the destination B.

**Decryption Process:**

* Use Recipient private key (d, n)
* **Computes the plaintext M=Cd mod n**
* Extracts the plaintext Message M

**Expected Output:**

**Sender:**

Enter primes p, q

Select e=?

public key: (e, n)

Enter plaintext

Encryption data:

C=Me mod n

Send ‘C’ to Receiver (Use Simple Socket Programming)

-------------------------------------------------------------

**Receiver:**

Enter Primes p, q (Assume previous values)

Select e=? (Input ‘e’ used at the sender)

Compute d=?

Private Key (d, n)

Read Cipher text from the Sender

M=Cd mod n