Assignment B4

Roll No: 41449

Title: Implementation of RSA

Problem Statement : Implementation of RSA

Objective : To understand how RSA algorithm works

Outcome : Understaning and implementation of asymmetric encryption using RSA.

Concept related theory :

RSA algorithm involves three steps

1. Key Generation

2. Encryption

3. Decryption

1. Key Generation

The key generation algorithm works as follows:

*1.* Generate two large random primes, *p* and *q*, of approximately equal size such that their

product *n*=*pq* is of the required bit length, e.g. 1024 bits.

2. Compute *n*=*pq* and *ϕ*=(*p*−1)()(*q*−1)()

3. Choose an integer *e*, 1)(<*e*<*ϕ*, such that gcd(*e*,*ϕ*)=1)

4. Compute the secret exponent *d*, 1)(<*d*<*ϕ*, such that *ed*≡1mod*ϕ*

5. The public key is (*n*,*e*) and the private key (n,*d*). Keep all the values d, p, q and *ϕ* secret.

2. Encryption:

Sender A does the following:-

1. Obtains the recipient B's public key (*n*,*e*)

2. Represents the plaintext message as a positive integer M with 1<*M*<*n*

3. Computes the ciphertext *C*=M *e* mod *n*

4. Sends the ciphertext C *t*o B.

3. Decryption

Recipient B does the following:-

*1.* Uses his private key (*n*,*d*) to compute *m*=C *d* mod *n*

2. Extracts the plaintext from the message representative *m*

Conclusion :

Successfully implemented RSA algorithm

Result :

