**Assignment 3**

**Name**:Bhavin Patil

**Roll No:** 66

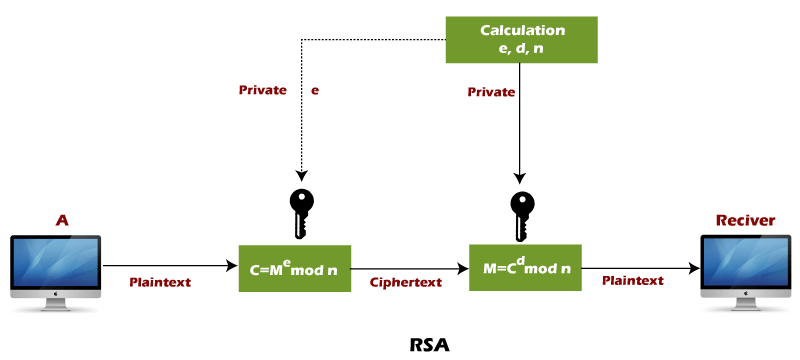
**TY-CS-D**

**Encryption and Decryption by RSA algorithm**

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 that the Public Key is given to everyone and the Private key is kept private.

**An example of asymmetric cryptography :**

1. A client (for example browser) sends its public key to the server and requests some data.
2. The server encrypts the data using the client’s public key and sends the encrypted data.
3. The client receives this data and decrypts it.



**RSA algorithm uses the following procedure to generate public and private keys:**

* Select two large prime numbers, p and **q**.
* Multiply these numbers to find **n = p x q,** where **n** is called the modulus for encryption and decryption.
* Choose a number **e** less than **n**, such that n is relatively prime to **(p - 1) x (q -1).** It means that **e** and **(p - 1) x (q - 1)** have no common factor except 1. Choose "e" such that 1<e < φ (n), e is prime to φ (n) ,**gcd (e,d(n)) =1**
* If **n = p x q,** then the public key is <e, n>. A plaintext message **m** is encrypted using public key <e, n>. To find ciphertext from the plain text following formula is used to get ciphertext C.  
  **C=me modn**  
  Here**, m** must be less than **n**. A larger message (>n) is treated as a concatenation of messages, each of which is encrypted separately.
* To determine the private key, we use the following formula to calculate the d such that:  
  **De mod{(p-1)x(q-1)}=1**  
  **Or**  
  **De mod φ (n) = 1**
* The private key is <d, n>. A ciphertext message **c** is decrypted using private key <d, n>. To calculate plain text **m** from the ciphertext c following formula is used to get plain text m.  
  **m = cd mod n**

**Code:**

#include<iostream>

#include<math.h>

using namespace std;

int gcd(int a, int b) {

   int t;

   while(1) {

      t= a%b;

      if(t==0)

      return b;

      a = b;

      b= t;

   }

}

int main() {

   //2 random prime numbers

   double p;

   double q;

   cout<<"Enter 2 prime numbers: ";

   cin>>p>>q;

   double n=p\*q;

   double track;

   double phi= (p-1)\*(q-1);

   double e=7;

   while(e<phi) {

      track = gcd(e,phi);

      if(track==1)

         break;

      else

         e++;

   }

   double d1=1/e;

   double d=fmod(d1,phi);

   double message;

   cout<<"Enter the message: ";

   cin>>message;

   double c = pow(message,e);

   double m = pow(c,d);

   c=fmod(c,n);

   m=fmod(m,n);

   cout<<"Original Message = "<<message;

   cout<<" \n"<<"p = "<<p;

   cout<<" \n"<<"q = "<<q;

   cout<<" \n"<<"n = pq = "<<n;

   cout<<" \n"<<"phi = "<<phi;

   cout<<" \n"<<"e = "<<e;

   cout<<" \n"<<"d = "<<d;

   cout<<" \n"<<"Encrypted message = "<<c;

   cout<<" \n"<<"Decrypted message = "<<m;

   return 0;

}

**Output:**

