| **Sno**: 5 | **Experiment name:** RSA Encryption and Decryption Algorithm | **Date:02-12-20** |
|---|---|---|

**Aim:** Using the RSA algorithm Encrypt text data and decrypt the same.

**Description:** RSA Algorithm is used to encrypt and decrypt data in modern computer systems and other electronic devices. RSA algorithm is an asymmetric cryptographic algorithm as it creates 2 different keys for the purpose of encryption and decryption. ... RSA makes use of prime numbers (arbitrary large numbers) to function.

To make things more efficient, a file will generally be encrypted with a symmetric-key algorithm, and then the symmetric key will be encrypted with RSA encryption. Under this process, only an entity that has access to the RSA private key will be able to decrypt the symmetric key.Without being able to access the symmetric key, the original file can't be decrypted. This method can be used to keep messages and files secure, without taking too long or consuming too many computational resources.

**Algorithm:**

The following steps to work on RSA algorithm

1. Generate the RSA modulus
   The initial procedure begins with selection of two prime numbers namely p and q, and then calculating their product N, as shown −
   $$N=p*q$$
   Here, let N be the specified large number.
2. Derived Number (e)
   Consider number e as a derived number which should be greater than 1 and less than (p-1) and (q-1). The primary condition will be that there should be no common factor of (p-1) and (q-1) except 1
3. Public key
   The specified pair of numbers **n** and **e** forms the RSA public key and it is made public.
4. Private Key
   Private Key **d** is calculated from the numbers p, q and e. The mathematical relationship between the numbers is as follows −
   $$ed = 1 \bmod (p-1)(q-1)$$
   The above formula is the basic formula for Extended Euclidean Algorithm, which takes p and q as the input parameters.
5. Encryption Formula $C = Pe \bmod n$
6. Decryption Formula Plaintext = $Cd \bmod n$

**Sample Input & Output:**

```
Enter the numbered message:
2
Enter two prime numbers:
7 11
the value of totent function = 60
The value of e = 7
The value of d = 43
Encrypted message is:
51.0
Derypted message is:
12.0
```

**Source Code:**

```
Import java.util.*;
class RSA
{
        public static void main(String args[])
        {
                int msg;
                System.out.println("Enter the numbered message: ");
                Scanner sc=new Scanner(System.in);
                msg=sc.nextInt();
                int p,q;
                System.out.println("Enter two prime numbers: ");
                p=sc.nextInt();
                q=sc.nextInt();
                int n=p*q;
                int e;
                int pi=(p-1)*(q-1);
                System.out.println("the value of totent function = "+pi);
                for(e=2;e<pi;e++)
                {
                        if(gcd(e,pi)==1)
                        {
                                break;
                        }
                }
                int d=0;
                System.out.println("The value of e = "+e);
                for(int i=1;i<pi;i++)
                {
                        if(e*i%pi==1)
                        {
```

```
                                d=i;
                                break;
                        }
                }
                System.out.println("the value of d = "+d);
                double c=Math.pow(msg,e)%n;
                System.out.println("Encrypted message is: \n"+c);
                System.out.println("Derypted message is:
                \n"+(Math.pow(c,d)%n));
        }
        public static int gcd(int e, int z)
        {
                if(e%z==0)
                        return z;
                return gcd(z,e%z);
        }
}
```

**Execution Results :** All test cases have succeded

| Test Case - 1 |
| --- |
| Enter·the·numbered·message:· |
| 2 |
| Enter·two·prime·numbers:· |
| 7 11 |
| the·value·of·totent·function·=·60 |
| The·value·of·e·=·7 |
| The·value·of·d·=·43 |
| Encrypted·message·is:· |
| 51.0 |
| Derypted·message·is:· |
| 12.0 |

| Test Case -2 |
| --- |
| Enter·the·numbered·message:· |
| 1234 |
| Enter·two·prime·numbers:· |

| |
|---|
| 3 7 |
| the·value·of·totent·function·=·12 |
| The·value·of·e·=·5 |
| The·value·of·d·=·5 |
| Encrypted·message·is:· |
| 4.0 |
| Derypted·message·is:· |
| 16.0 |

| **Test Case -3** |
|---|
| Enter·the·numbered·message:· |
| 2323 |
| Enter·two·prime·numbers:· |
| 5 35 3 |
| the·value·of·totent·function·=·8 |
| The·value·of·e·=·3 |
| The·value·of·d·=·3 |
| Encrypted·message·is:· |
| 2.0 |
| Derypted·message·is:· |
| 8.0 |

**Result:** Successfully completed RSA Encryption and Decryption Algorithm.