Assignment 9

AIM: Implement the RSA Algorithm.

THEORY:

RSA is an asymmetric cryptography algorithm which works on two keys-public key and private key.

Algorithm :

Begin

1. Choose two prime numbers p and q.
2. Compute n = p*q.
3. Calculate phi = (p-1) * (q-1).
4. Choose an integer e such that 1 < e < phi(n) and gcd(e, phi(n)) = 1; i.e., e and phi(n) are coprime.
5. Calculate d as d ≡ e−1 (mod phi(n)); here, d is the modular multiplicative inverse of e modulo phi(n).
6. For encryption, c = me mod n, where m = original message.
7. For decryption, m = c d mod n.

End

PROGRAM :

```
#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() {
  double p = 13;
  double q = 11;
  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 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 :

```
"C:\Users\Ankit Goyal\OneDrive\Documents\labs\8th Sem Lab\ISS\rsa.exe"
Enter Message82
Original Message = 82
p = 13
q = 11
n = pq = 143
phi = 120
e = 7
d = 0.142857
Encrypted message = 69
Decrypted message = 82
Process returned 0 (0x0)   execution time : 11.019 s
Press any key to continue.
```