Name: Mohan Ramchandra Patil

Reg. No : 19141267

IS Exp5- Implementation of RSA Algorithm

Code:

```
#include<iostream>
#include<stdlib.h>
#include<math.h>
#include<string.h>
using namespace std;
int x, y, n, t, i, flag;

long int e[50], d[50], temp[50], j;
char en[50], m[50];
char msg[100];
int prime(long int);
void encryption_key();
long int cd(long int);
void encrypt();
void decrypt();
int main(){
 cout << "\n Enter the First Prime Number : \n";
 cin >> x;
 flag = prime(x);
 if(flag == 0){
 cout << "\n Invalid Input \n";
 exit(0);}
 cout << "\nEnter the Second Prime Number : \n";
 cin >> y;
 flag = prime(y);
 if(flag == 0 || x == y)
 {
 cout << "\n Invalid Input \n";
 exit(0);
 }
 cout << "\nEnter Message to Encrypt : \n";
 cin >> msg;
 for(i = 0; msg[i] != NULL; i++)
 m[i] = msg[i];
 n = x * y;
 t = (x - 1) * (y - 1);
 encryption_key();
 cout << "\nPossible values of e ans d are : \n";
 for(i = 0; i < j - 1; i++)
 cout << "\n" << e[i] << "\t" << d[i];
 encrypt();
 decrypt();
 return 0;
}
int prime(long int pr)
{
 int i;
 j = sqrt(pr);
```

```
 for(i = 2; i <= j; i++)
 {
 if(pr % i == 0)
 return 0;
 }
 return 1;
}
void encryption_key()
{
 int k;
 k = 0;
 for(i = 2; i < t; i++)
 {
 if(t % i == 0)
 continue;
 flag = prime(i);
 if(flag == 1 && i != x && i != y)
    {
 e[k] = i;
 flag = cd(e[k]);
 if(flag > 0)
 {
 d[k] = flag;
 k++;
 }
 if(k == 99)
 break;}}}
long int cd(long int a)
{
 long int k = 1;
 while(1)
 {
 k = k + t;
 if(k % a == 0)
 return(k/a);
 }
}

void encrypt()
{
 long int pt, ct, key = e[0], k, len;
 i = 0;
  len = strlen(msg);
 while(i != len)
 {
 pt = m[i];
 pt = pt - 96;
 k = 1;
 for(j = 0; j < key; j++)
 {
 k = k * pt;
 k = k % n;
 }
```

```
 temp[i] = k;
 ct= k + 96;
 en[i] = ct;
 i++;
 }
 en[i] = -1;
 cout << "\n\nThe Encrypted message is : \n";
 for(i=0; en[i] != -1; i++)
 cout << en[i];
}
void decrypt()
{
 long int pt, ct, key = d[0], k;
 i = 0;
 while(en[i] != -1)
 {
 ct = temp[i];
 k = 1;
 for(j = 0; j < key; j++)
 {
 k = k * ct;
 k = k % n;
 }
 pt = k + 96;
 m[i] = pt;
 i++;
 }
 m[i] = -1;
 cout << "\n\n The Decrypted message : \n";
 for(i = 0; m[i] != -1; i++)
 cout << m[i];
 cout << endl;}
```

Output:

```
  Enter the First Prime Number :
 3

 Enter the Second Prime Number :
 17

 Enter Message to Encrypt :
 mohanpatil

 Possible values of e ans d are :

 5       13
 7       23
 11      3
 13      5

 The Encrypted message is :
 mäza}paeèc

  The Decrypted message :
 mohanpatil
```