Lab-04

AIM:- Write a pragrum to implement
1. square and Multiply function
2. RSA algorithm.

1) Square and Multiply function

```
#include< bits/stdc++.h>
using namespace std;

int squarreAndMultiply (int a, int b, int n)
{
        int z = 1;
        bitset<16> b_(b); // convert to binary.
        string binary = b_.to_string();

        for(int i=0; i< binary.length(); ++i)
        {
              z = (z*z) % n;

              if( binary[i]=='1')
                    z =(z*a) % n;
        }
        return z;
}
```

```
int main()
{
      int a,b,n;

      cin>>a>>b>>n;

      cout<<" a^b mod n:" << squreAndmultiply(a,b,n);
      cout<<endl;
      return 0;
}
```

Input	output
19 5 119	a^b mod n : 66
66 77 119	a^b mod n : 19
56 24 119	a^b mod n : 84

2> RSA algorithm

```
#include<bits/stdc++.h>

using namespace std;

bool isPrime(int num)
{
   if(num <=1)
          return fulse;
```

```
    for(int i=2; i<=sqrt(num); ++i)
    {
        if( num % i == 0)
            return false;
    }
    return true;
}

vector<int>   keyGeneration( int p, int q)
{
    int phi, n, e, d;
    vector< int> keys;
    phi = (p-1) * (q-1);
    n = p*q;

    for(int i =2; i< phi; ++i)              gcd=1
    {
        if(multiplicative Inverse (i, phi)!=-1)
        {
            e = i;
            break;
        }
    }
    d = multiplicativeInverse( e, phi); //private

    keys.push-back( e);
    keys.push-back(n);
    keys.push-back(d);
    return keys;
}
```

```
int encryption( int msg, int e, int n)
{
    int cipher;
    cipher = squareAndMultiply( msg, e,n);
    return cipher;
}

int decryption( int cipher, int d, int n)
{
    int msg;
    msg = squareAndMultiply(cipher, d, n);
    return msg;
}

int main()
{
    int p,q,e,d,n;
    cout<<"Please enter Two numbers: ";
    cin>> p >>q;
    vector<int> keys;
    keys = keyGeneration(p,q);

    e= keys[0];
    d = keys[2];
    n= keys[1];
    int msg, cipher;
    cout<<"Enter Your msg: ";
    cin>>msg;
```

```
cout<< "Encrypted msg:" << cipher
    <<(cipher = encryption( msg, e,n)) <<endl;

cout<<"Decrypted msg:"
    << decryption( cipher, d, n)<< end;

return 0;
```

Input

```
Please enter Two numbers: 7,17
Enter your msg: 19
```

out put

```
Encrypted msg: 66

Decrypted msg: 19
```