SIDDAGANGA INSTITUTE OF TECHNOLOGY, TUMKUR-572103

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CRYPTOGRAPHY AND NETWORK SECURITY LAB (7RCSL01)

Student Name: Nitin Krishna H	USN:1SI18CS068	Batch No:A4	Date:03/12/2021

Evaluation:

Write Up (10 marks)	Clarity in concepts (10 marks)	Implementation and execution of the algorithms (10 marks)	Viva (05 marks)	Total (35 marks)

Sl.No	Name of the Faculty In-Charge	Signature
1.	Mr Bhaskar G	
2.	Mrs Thejaswini S	

Question No: 10

Write a program to generate large random number using BBS random number generator algorithm and check whether the generated number is prime or not using RABIN-MILLER Primality testing algorithm.

Algorithm:

BBS Random Number Generator Algorithm:

First, choose two large prime numbers p and q, that both have a remainder of 3 when divided by 4.

P=Q=3 mod 4

$$
\begin{aligned}
X_0 &= s^2 \bmod n \\
\textbf{for } i &= 1 \textbf{ to } \infty \\
X_i &= (X_{i-1})^2 \bmod n \\
B_i &= X_i \bmod 2
\end{aligned}
$$

RABIN-MILLER Primality testing algorithm:

```
TEST (n)
1. Find integers k, q, with k > 0, q odd, so that
   (n − 1 = 2^k q);
2. Select a random integer a, 1 < a < n − 1;
3. if a^q mod n = 1 then return("inconclusive");
4. for j = 0 to k − 1 do
5. if a^(2^j q) mod n = n − 1 then return("inconclusive");
6. return("composite");
```

PROGRAM

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

int randInRange(int low,int high)
{
	return (rand()%(high-low+1))+(low+1);
}

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

int genPrime3mod4()
{
	while(true)
	{
		int num = randInRange(10000,100000);

	if(num%4!=3)
		continue;

		if(isprime(num))
			return num;
	}
}

int bbs(int p,int q)
{
	cout<<"BlumBlumShub"<<endl<<"--------------"<<endl;
	cout<<"p="<<p<<"\nq="<<q<<endl;

	long long n=(long long)p*q;//step 1 : n=p*q
   cout<<"n="<<n<<endl;

	//step 2 : CALCULATING s
	//s should be relatively prime to n
	//s should not be divisible by both p and q
	long long s;
	do{ s = rand(); }while( s%p==0 || s%q==0 || s==0);
	cout<<"s="<<s<<endl;

	//BBS algo
	int	B=0;
```

```
        long long x=(s*s)%n;
    for(int i=0;i<10;i++)
        {
                x = (x*x)%n;
                B = B<<1|(x&1);
        }
        return B;
}

int powModN(int a,int b,int n)
{
        int res=1;
        for(int i=0;i<b;i++)
                res = (res*a)%n;
        return res;
}

string rabinMiller(int n)
{
        cout<<"\nRabinMiller("<<n<<")\n----------"<<endl;
        //step 1: choosing k and q
        //k>0 and q is odd such that n-1 = 2 ^ k * q
        int k=0;
        int q=n-1;
        while(q%2==0)
        {
                q=q/2;
                k++;
        }
        cout<<n-1<<"=2^"<<k<<"*"<<q<<endl;
        cout<<"k="<<k<<"\nq="<<q<<endl;

        //step 2 : select random a
        int a = randInRange(1,n-1);
        cout<<"a="<<a<<endl;

        //step 3 : if a^q mod n = 1 then inconclusive
        if(powModN(a,q,n)==1)
                return "inconclusive";

        //step 4
        for(int j=0;j<k;j++)
                if(powModN(a,pow(2,j)*q,n)==n-1)
                        return "inconclusive";

        //step 5
        return "composite";
}

int main()
```

```
{
	srand(time(NULL));

	//generate two primes
	int p = genPrime3mod4();
	int q = genPrime3mod4();

	//generate random number using bbs algo
	int randNum = bbs(p,q);
	cout<<"Random number generated by BBS= "<<randNum<<endl;

	//test primality using rabin miller algo
	cout<<rabinMiller(randNum)<<endl;

	return 0;
}
```

OUTPUT

```
nitin@nitinkrishna:~/Documents/pdf notes/pdf notes 7th sem/CNS lab/labs/lab10/labset10/Rabinmiller$ g++ rabinmiller.cpp
nitin@nitinkrishna:~/Documents/pdf notes/pdf notes 7th sem/CNS lab/labs/lab10/labset10/Rabinmiller$ ./a.out
BlumBlumShub
--------------
p=88463
q=55987
n=4952777981
s=1924564823
Random number generated by BBS= 928

RabinMiller(928)
-----------------
927=2^0*927
k=0
q=927
a=189
composite
nitin@nitinkrishna:~/Documents/pdf notes/pdf notes 7th sem/CNS lab/labs/lab10/labset10/Rabinmiller$ ./a.out
BlumBlumShub
--------------
p=60343
q=84979
n=5127887797
s=1729709956
Random number generated by BBS= 729

RabinMiller(729)
-----------------
728=2^3*91
k=3
q=91
a=619
composite
```