Bansi Bera

Dot Net Technology – 2160711

Lab Manual

Semester 7th

Academic Year 2020-21 Odd

VVP Engineering College,
Rajkot

Gujarat Technological
University

Table of Contents

1. **DIFFIE HELLMAN KEY EXCHANGE 1**

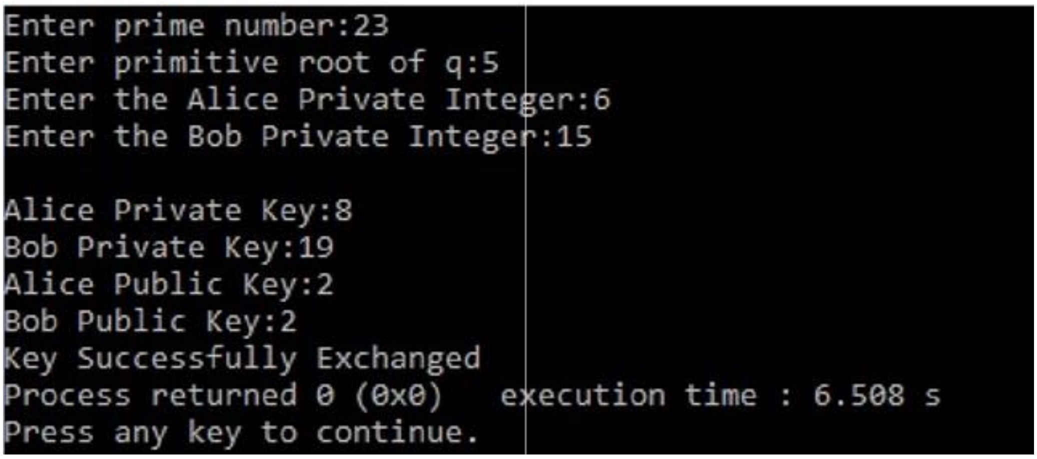
Practical 7

DIFFIE HELLMAN KEY EXCHANGE

```
#include<iostream>
#include<cstdio> using
namespace std;
int SquareMultiply(int a,int b,int c)
{    int i,n=a;
int binary[20];
  for(i=0;b>0;i++)//Convert decimal exponent to binary
  {
    binary[i]=b%2;
b=b/2;
  }
  for(i=i-2;i>=0; i--)//Trace binary number
  {
    if(binary[i]==0)//If current binary digit is 0 then
    {
      a=a*a;//Calculate square
a=a%c;//And mod output with n
    }
    if(binary[i]==1)//If current binary digit is 1 then
    {
      a=a*a;//calculate        square
a=a%c;//And  mod  output  with  n
a=a*n;//Multiply output
      a=a%c;//And again mod output with n
    }
  }
```

```
 return a;//Return
}
void DiffieHellman(int q,int a,int x,int y)
{
   int YA,YB,K1,K2;
    YA=SquareMultiply(a,x,q);//Calculate Alice Private Key which is only known to Alice
YB=SquareMultiply(a,y,q);//Calculate Bob Private Key which is only known to Bob
cout<<"\nAlice Private Key:"<<YA;     cout<<"\nBob Private Key:"<<YB;
   K1=SquareMultiply(YB,x,q);//Calculate Alice Public Key known to Alice and Bob
K2=SquareMultiply(YA,y,q);//Calculate Bob Public Key known to Alice and Bob
cout<<"\nAlice Public Key:"<<K1;     cout<<"\nBob Public Key:"<<K2;
if(K1==K2)//If both public key are same then
      cout<<"\nKey Successfully Exchanged";//display successful
   else
      cout<<"\nKey not exchanged successfully";//else does not successful
} int
main()
{
     int q,a,x,y;
     cout<<"Enter prime number:";//Get Prime number
cin>>q;
     cout<<"Enter primitive root of q:";//Get primitive root
cin>>a;
     cout<<"Enter the Alice Private Integer:";//Get Alice Private Integer
cin>>x;
     cout<<"Enter the Bob Private Integer:";//Get Bob Private Integer
cin>>y;
     DiffieHellman(q,a,x,y);//Call DiffieHellman for process of key exchange
     return 0;
}
```

OUTPUT:



```
Enter prime number:23
Enter primitive root of q:5
Enter the Alice Private Integer:6
Enter the Bob Private Integer:15

Alice Private Key:8
Bob Private Key:19
Alice Public Key:2
Bob Public Key:2
Key Successfully Exchanged
Process returned 0 (0x0)   execution time : 6.508 s
Press any key to continue.
```