T.Y. B.Sc. C.S. Sem-V	Roll No: **713**
	Date:07/10/2020

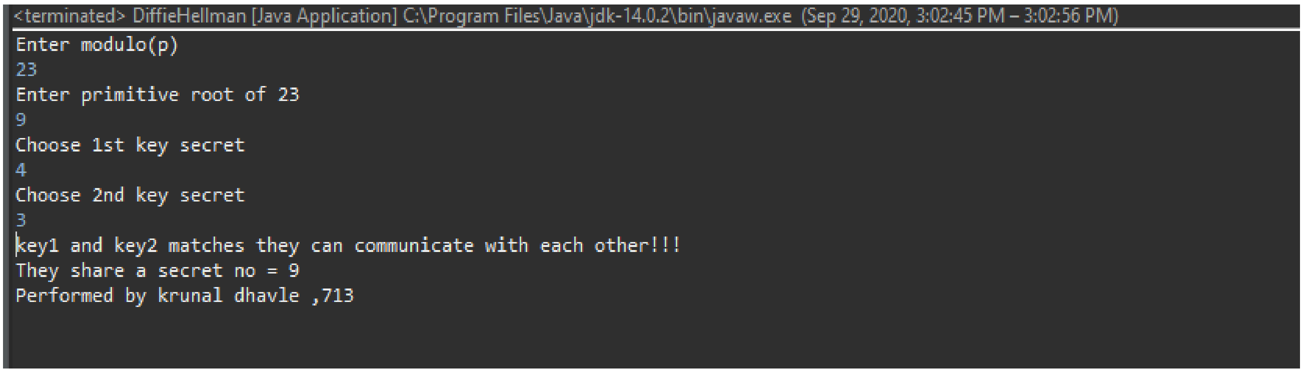
Practical no 6

AIM: Write a program to implement the Diffie-Hellman Key Agreement algorithm to generate symmetric keys.

CODE:-

```
package prac6;
import java.util.*;
public class DiffieHellman {

	public static void main(String[] args) {
	 // TODO Auto-generated method stub
	  Scanner sc=new Scanner(System.in);
	  System.out.println("Enter modulo(p)");
	  int p=sc.nextInt();
	  System.out.println("Enter primitive root of "+p);
	  int g=sc.nextInt();
	  System.out.println("Choose 1st key secret");
	  int a=sc.nextInt();
	  System.out.println("Choose 2nd key secret");
	  int b=sc.nextInt();
	  sc.close();
	  int A = (int)Math.pow(g,a)%p;
	  int B = (int)Math.pow(g,b)%p;

	  int S_A = (int)Math.pow(B,a)%p;
	  int S_B =(int)Math.pow(A,b)%p;

	  if(S_A==S_B)
	  {
	  System.out.println("key1 and key2 matches they can communicate with each other!!!");
	  System.out.println("They share a secret no = "+S_A);
	  System.out.println("Performed by krunal dhavle ,713");
	  }

	  else
	  {
```

```
                                        System.out.println("key1 and key2 matches they cannot
communicate with each other!!!");
                                        System.out.println("Performed by krunal dhavle ,713");
                                        }

                                      }

}
```



```
<terminated> DiffieHellman [Java Application] C:\Program Files\Java\jdk-14.0.2\bin\javaw.exe (Sep 29, 2020, 3:02:45 PM – 3:02:56 PM)
Enter modulo(p)
23
Enter primitive root of 23
9
Choose 1st key secret
4
Choose 2nd key secret
3
key1 and key2 matches they can communicate with each other!!!
They share a secret no = 9
Performed by krunal dhavle ,713
```