**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");  }  }  } |

