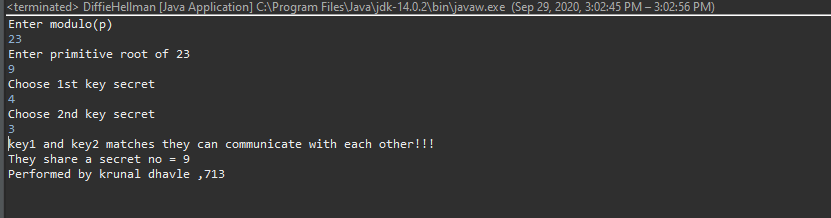
**Practical no 6**

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

**CODE:-**

**Method 1:-**

|  |
| --- |
| 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");  }  }  } |



**Method 2 :-**

**Bob.java**

|  |
| --- |
| package prac6;  import java.io.\*;  import java.net.ServerSocket;  import java.net.Socket;  import java.util.Scanner;  public class Bob {  public static void main(String[] args) throws IOException {  ServerSocket ss = new ServerSocket(5000);  Socket s = ss.accept();  DataInputStream in = new DataInputStream(s.getInputStream());  int n = in.readInt();  int g = in.readInt();  Scanner sc = new Scanner(System.in);  System.out.println("Enter the value of y");  int y = sc.nextInt();  System.out.println("n=" +n);  System.out.println("g=" +g);  int d =(int)Math.pow(g, y);  int B =d%n;  System.out.println("The calculated value of B is " +B);  System.out.println("bob sends the value of B " +B+ " to alice");  int A = in.readInt();  int b = (int)Math.pow(A,y);  double K2 = b%n;  System.out.println("the calculated value of k2 is " +K2);  DataOutputStream out = new DataOutputStream(s.getOutputStream());  out.writeInt(B);  System.out.println("performed by krunal 713");  }  } |

**Alice.java**

|  |
| --- |
| package prac6;  import java.io.\*;  import java.net.Socket;  import java.util.Scanner;  public class Alice {  public static void main(String[] args) throws IOException {  Socket cs = new Socket("localhost" ,5000);  Scanner sc = new Scanner(System.in);  System.out.println("Enter the value of n and g ");  int n = sc.nextInt();  int g = sc.nextInt();  System.out.println("n=" +n);  System.out.println("g=" +g);  DataOutputStream out = new DataOutputStream(cs.getOutputStream());  out.writeInt(n);  out.writeInt(g);  System.out.println("Enter the value of x : ");  int x = sc.nextInt();  int c =(int)Math.pow(g,x);  int A = c%n;  System.out.println("the calculated value of A is " +A);  out.writeInt(A);  System.out.println("Alice sends the value of a " +A + "to bob");  DataInputStream in = new DataInputStream(cs.getInputStream());  int B = in.readInt();  int a = (int)Math.pow(B, x);  double K1 = a % n;  System.out.println("the calculated value for k1 is " +K1);  System.out.println("performed by krunal 713");  }  } |