**NAME: FURKHAN MUJIBODDEN SHAIKH**

**CLASS: BECSEII**

**AIM: WRITE A PROGRAM TO IMPLEMENT DIFFIE-HELLMAN KEY EXCHANGE ALGORITHM**

**----------------------------------------------------------------------**

**import java.net.\*;**

**import java.io.\*;**

**public class ClientProgram {**

**public static void main(String[] args)**

**{**

**try {**

**String pstr, gstr, Astr;**

**String serverName = "localhost";**

**int port = 8088;**

**// Declare p, g, and Key of client**

**int p = 23;**

**int g = 9;**

**int a = 4;**

**double Adash, serverB;**

**// Established the connection**

**System.out.println("Connecting to " + serverName**

**+ " on port " + port);**

**Socket client = new Socket(serverName, port);**

**System.out.println("Just connected to "**

**+ client.getRemoteSocketAddress());**

**// Sends the data to client**

**OutputStream outToServer = client.getOutputStream();**

**DataOutputStream out = new DataOutputStream(outToServer);**

**pstr = Integer.toString(p);**

**out.writeUTF(pstr); // Sending p**

**gstr = Integer.toString(g);**

**out.writeUTF(gstr); // Sending g**

**double A = ((Math.pow(g, a)) % p); // calculation of A**

**Astr = Double.toString(A);**

**out.writeUTF(Astr); // Sending A**

**// Client's Private Key**

**System.out.println("From Client : Private Key = " + a);**

**// Accepts the data**

**DataInputStream in = new DataInputStream(client.getInputStream());**

**serverB = Double.parseDouble(in.readUTF());**

**System.out.println("From Server : Public Key = " + serverB);**

**Adash = ((Math.pow(serverB, a)) % p); // calculation of Adash**

**System.out.println("Secret Key to perform Symmetric Encryption = "**

**+ Adash);**

**client.close();**

**}**

**catch (Exception e) {**

**e.printStackTrace();**

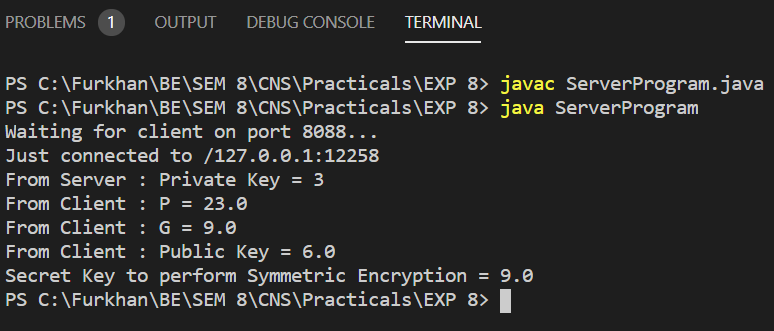
**}**

**}**

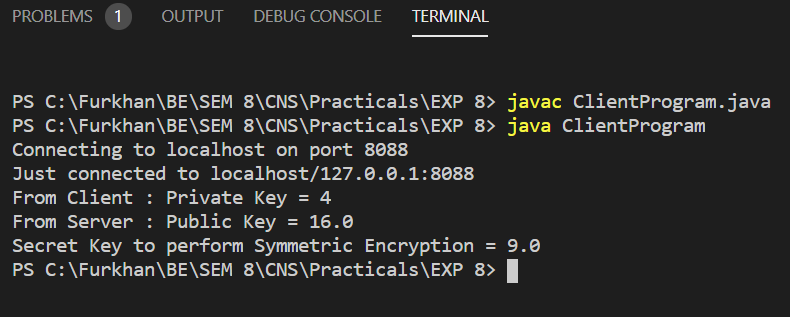
**}**

**OUTPUT:**

**1. SERVER PROGRAM**

****

**2. CLIENT PROGRAM**

****