Practical No – 05

Key Exchange using Diffie-Hellman

Aim: Implement the Diffie-Hellman key exchange algorithm to securely exchange keys between two entities over an insecure network.

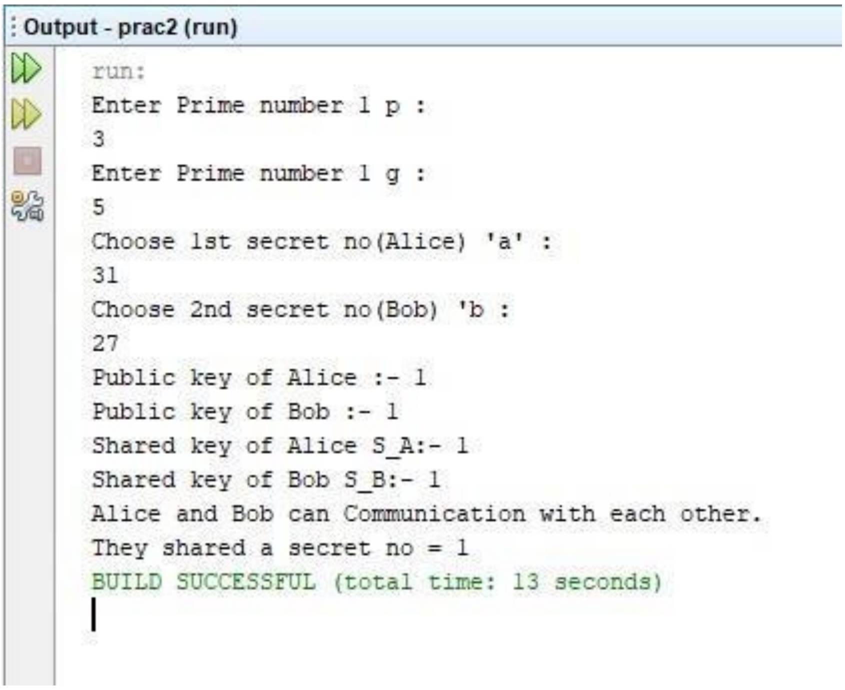
Source Code :

```
import java.util.*; public
class DH { public static void main(String
args[]) {
    Scanner sc = new Scanner(System.in);
    System.out.println("Enter Prime number 1 p : ");
    int p = sc.nextInt();
    System.out.println("Enter Prime number 1 g : "); int
    g = sc.nextInt();
    System.out.println("Choose 1st secret no(Alice) 'a' : "); int
    a = sc.nextInt();
    System.out.println("Choose 2nd secret no(Bob) 'b : ");
    int b = sc.nextInt(); int A = (int) Math.pow(g, a) % p;
    //Publiv Key of Alice int B = (int) Math.pow(g, b) % p;
    //Public key of Bob
    System.out.println("Public key of Alice :- " + A);
    System.out.println("Public key of Bob :- " + B);
    int S_A = (int) Math.pow(B, a) % p; //Alice int
    S_B = (int) Math.pow(A, b) % p; //Bob
    System.out.println("Shared key of Alice S_A:- " + S_A);
    System.out.println("Shared key of Bob S_B:- " + S_B);


    if(S_A == S_B){
      System.out.println("Alice and Bob can Communication with each other.");
```

```
        System.out.println("They shared a secret no = " + S_A);
     }
     else{
        System.out.println("Alice and Bob cannot Communication with each other!!!");
     }
  }
```

Output :



```
run:
Enter Prime number 1 p :
3
Enter Prime number 1 g :
5
Choose 1st secret no(Alice) 'a' :
31
Choose 2nd secret no(Bob) 'b :
27
Public key of Alice :- 1
Public key of Bob :- 1
Shared key of Alice S_A:- 1
Shared key of Bob S_B:- 1
Alice and Bob can Communication with each other.
They shared a secret no = 1
BUILD SUCCESSFUL (total time: 13 seconds)
```