

LAB-7

Name:Nisoka

Reg.No:19BCD7022

DIFFIE-HELLMAN KEY EXCHANGE

CODE:

```
import java.util.*;

// create class DiffieHellmanAlgorithmExample to calculate the key for two persons

class Main {

    // main() method start

    public static void main(String[] args)

    {

        long P, G, x, a, y, b, ka, kb;

        // create Scanner class object to take input from user

        Scanner sc = new Scanner(System.in);

        System.out.println("Both the users should be agreed upon the public keys G and P");

        // take inputs for public keys from the user

        System.out.println("Enter value for public key G:");

        G = sc.nextLong();

        System.out.println("Enter value for public key P:");

        P = sc.nextLong();

        // get input from user for private keys a and b selected by User1 and User2

        System.out.println("Enter value for private key a selected by user1:");

        a = sc.nextLong();

        System.out.println("Enter value for private key b selected by user2:");

        b = sc.nextLong();

        // call calculatePower() method to generate x and y keys

        x = calculatePower(G, a, P);

        y = calculatePower(G, b, P);

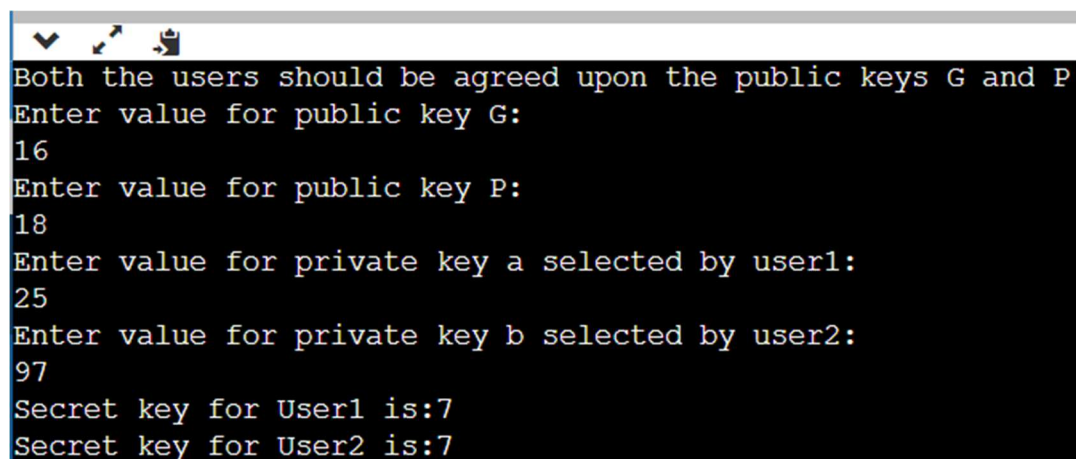
        // call calculatePower() method to generate ka and kb secret keys after the exchange of x and y keys
```

```

// calculate secret key for User1
ka = calculatePower(y, a, P);
// calculate secret key for User2
kb = calculatePower(x, b, P);
// print secret keys of user1 and user2
System.out.println("Secret key for User1 is:" + ka);
System.out.println("Secret key for User2 is:" + kb);
}
// create calculatePower() method to find the value of  $x^y \bmod P$ 
private static long calculatePower(long x, long y, long P)
{
    long result = 0;
    if (y == 1){
        return x;
    }
    else{
        result = ((long)Math.pow(x, y)) % P;
        return result;
    }
}
}

```

OUTPUT:



```

Both the users should be agreed upon the public keys G and P
Enter value for public key G:
16
Enter value for public key P:
18
Enter value for private key a selected by user1:
25
Enter value for private key b selected by user2:
97
Secret key for User1 is:7
Secret key for User2 is:7

```