

Assignment 10

// This program calculates the Key for two persons using the Diffie-Hellman Key exchange algorithm

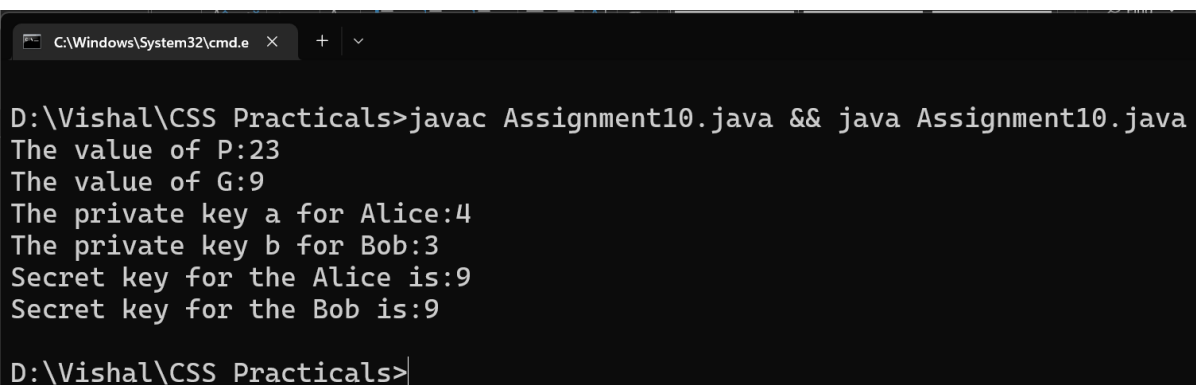
```
class Assignment10 {  
    // Power function to return value of  $a^b \bmod P$   
    private static long power(long a, long b, long p)  
    {  
        if (b == 1)  
            return a;  
        else  
            return (((long)Math.pow(a, b)) % p);  
    }  
    public static void main(String[] args)  
    {  
        long P, G, x, a, y, b, ka, kb;  
        // Both the persons will be agreed upon the public keys G and P  
  
        // A prime number P is taken  
        P = 23;  
        System.out.println("The value of P:" + P);  
        // A primitive root for P, G is taken  
        G = 9;  
        System.out.println("The value of G:" + G);  
        // Alice will choose the private key a  
        // a is the chosen private key  
        a = 4;  
        System.out.println("The private key a for Alice:" + a);  
        // Gets the generated key  
        x = power(G, a, P);  
        // Bob will choose the private key b  
        // b is the chosen private key  
        b = 3;
```

```
        System.out.println("The private key b for Bob:" + b);

        // Gets the generated key
        y = power(G, b, P);

        // Generating the secret key after the exchange
        // of keys
        ka = power(y, a, P); // Secret key for Alice
        kb = power(x, b, P); // Secret key for Bob

        System.out.println("Secret key for the Alice is:" + ka);
        System.out.println("Secret key for the Bob is:" + kb);
    }
}
```



A screenshot of a Windows command prompt window. The title bar shows 'C:\Windows\System32\cmd.exe'. The command prompt displays the following output:

```
D:\Vishal\CSS Practicals>javac Assignment10.java && java Assignment10.java
The value of P:23
The value of G:9
The private key a for Alice:4
The private key b for Bob:3
Secret key for the Alice is:9
Secret key for the Bob is:9
D:\Vishal\CSS Practicals>
```