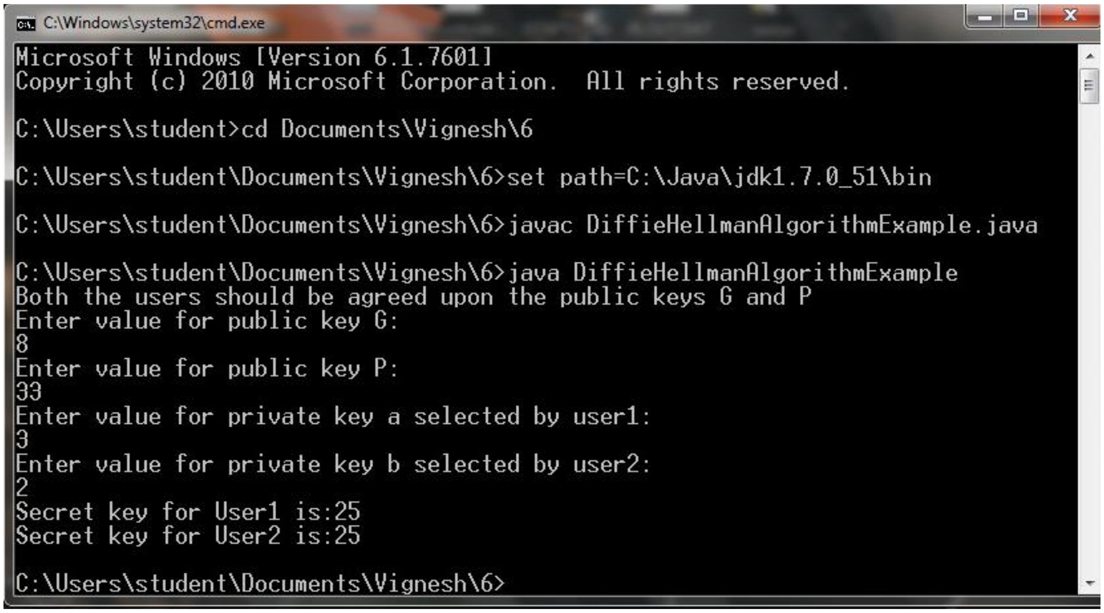
PROGRAM:

DiffieHellman.java

```
import java.util.*;
class DiffieHellmanAlgorithmExample
{
        public static void main(String[]args)
        {
                longP,G, x,a, y,b, ka,kb;
                Scannersc=newScanner(System.in);
                System.out.println(" Both the users should be agreed upon the
                public keys G and P");
                System.out.println("Enter value for public key G:");
                G=sc.nextLong();
                System.out.println("Enter value for public key P:");
                P=sc.nextLong();
                System.out.println("Enter value for private key a selected by user
                1:");
                a=sc.nextLong();
                System.out.println("Enter value for private key b selected by user
                2:");
                b=sc.nextLong();
                x = calculatePower(G, a, P);
                y = calculatePower(G, b, P);
                ka = calculatePower(y, a, P);
                kb=calculatePower(x,b,P) ;
                System.out.println("Secret key for User1 is:" + ka);
                System.out.println("SecretkeyforUser2is:"+kb);
        }
        private static long calculatePower(long x, long y, long P)
        {
                Long result=0;
                if(y==1)
                {
                        returnx;
                }
                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: 8
Enter value for public key P: 33
Enter value for private key a selected by user 1: 3
Enter value for private key a selected by user 2: 2
Secret key for user 1 is: 25
Secret key for user 2 is: 25



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2010 Microsoft Corporation.  All rights reserved.

C:\Users\student>cd Documents\Vignesh\6

C:\Users\student\Documents\Vignesh\6>set path=C:\Java\jdk1.7.0_51\bin

C:\Users\student\Documents\Vignesh\6>javac DiffieHellmanAlgorithmExample.java

C:\Users\student\Documents\Vignesh\6>java DiffieHellmanAlgorithmExample
Both the users should be agreed upon the public keys G and P
Enter value for public key G:
8
Enter value for public key P:
33
Enter value for private key a selected by user1:
3
Enter value for private key b selected by user2:
2
Secret key for User1 is:25
Secret key for User2 is:25

C:\Users\student\Documents\Vignesh\6>
```