Experiment No. 3

Aim: Write a program to implement the Diffie-Hellman Algorithm.

Program:

```
from random import randint
P=int(input("The Value of P is :"))
G=int(input("The Value of G is :"))
a = int(input("The Private Key a for Alice is :"))
x = int(pow(G,a,P))
b = int(input("The Private Key b for Bob is :"))
y = int(pow(G,b,P))
ka = int(pow(y,a,P))
kb = int(pow(x,b,P))
print('Secret key for the Alice is : %d'%(ka))
print('Secret Key for the Bob is : %d'%(kb))
```

Output:

```
PS C:\Users\student\Desktop\CSS> python diffie.py
The Value of P is :5
The Value of G is :7
The Private Key a for Alice is :45
The Private Key b for Bob is :18
Secret key for the Alice is : 4
Secret Key for the Bob is : 4
PS C:\Users\student\Desktop\CSS>
```