

Name : Prem Vinod Bansod
Roll no : 41310
Assignment No : 03 (ICS)

Code:

```
from random import randint

if __name__ == '__main__':

    # A prime number P is taken
    P = 11

    # G is a primitive root for P
    G = 2

    print("The Value of P is :%d"%(P))
    print("The Value of G is :%d"%(G))

    # Alice private key a
    a = 8
    print("The Private Key a for Alice is :%d"%(a))

    # Alice generated key(public Key)
    x = int(pow(G,a,P))

    # Bob private key b
    b = 4
    print("The Private Key b for Bob is :%d"%(b))

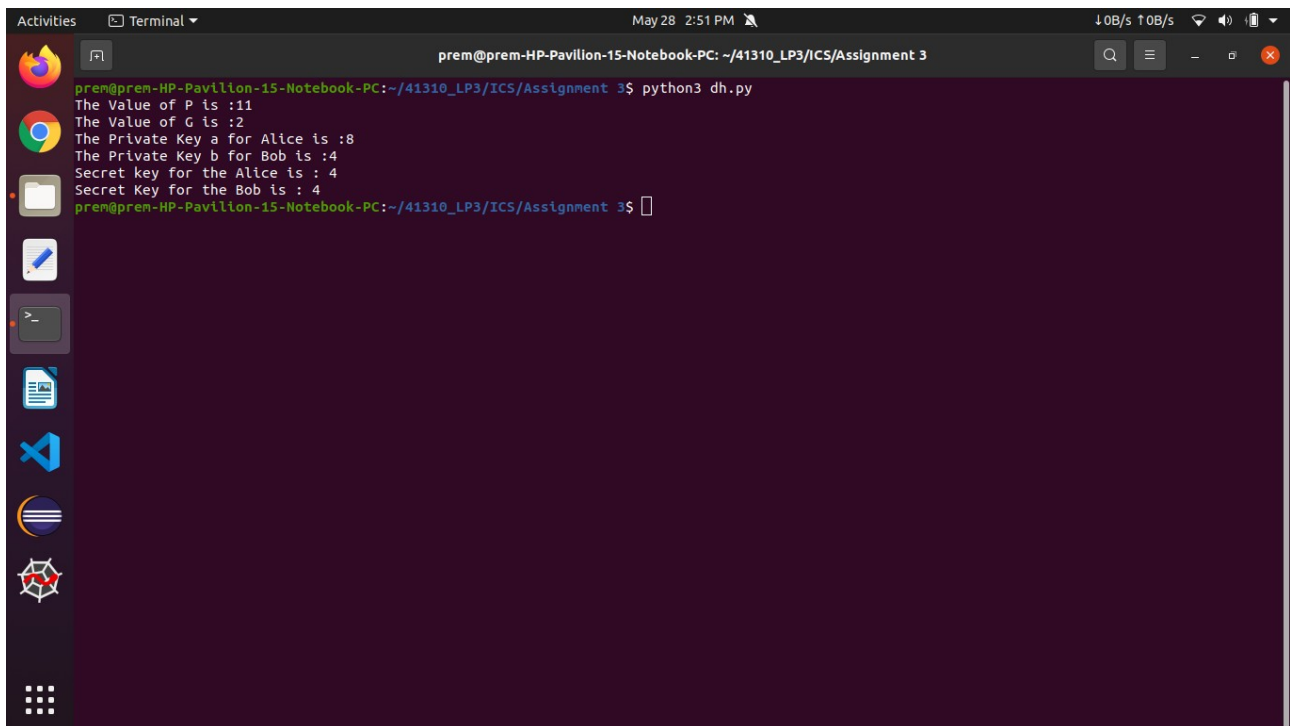
    # Bob generated key(public Key)
    y = int(pow(G,b,P))

    # Secret key for Alice
    ka = int(pow(y,a,P))

    # Secret key for Bob
    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:



A terminal window titled "Terminal" with a dark background. The window shows the execution of a Python script named "dh.py". The output of the script is displayed in green text. The window's title bar includes the date and time "May 28 2:51 PM" and system status icons. The left sidebar of the terminal shows various application icons.

```
premise@premise-HP-Pavilion-15-Notebook-PC: ~/41310_LP3/ICS/Assignment 3
premise@premise-HP-Pavilion-15-Notebook-PC:~/41310_LP3/ICS/Assignment 3$ python3 dh.py
The Value of P is :11
The Value of G is :2
The Private Key a for Alice is :8
The Private Key b for Bob is :4
Secret key for the Alice is : 4
Secret Key for the Bob is : 4
premise@premise-HP-Pavilion-15-Notebook-PC:~/41310_LP3/ICS/Assignment 3$
```