26/11/2020 **Mohd. Aftab Alam**
02013302717

EXPERIMENT 7

Aim: Write a program to perform Encryption/Decryption using Diffie-Hellman Key Exchange Techniques.

Theory & Algorithm:

Diffie Hellman was the first public key algorithm ever invented, in 1976. Alice and Bob want to be able to generate a key to use for subsequent message exchange. The key generating exchange can take place over an unsecure channel that allows eavesdropping. The ingredients to the protocol are: p, a large prime and g, a primitive element of Z_n. This means that all numbers n=1, ... , p-1 can be represented as $n = g^i$. These two numbers do not need to be kept secret. For example, Alice could send them to Bob in the open.

The protocol runs as follows:

1. Alice choses a large random integer x and sends Bob

   $X=g^x \bmod p$

2. Bob choses a large random integer y and sends Alice

   $Y=g^y \bmod p$

3. Alice computes

   $k=Y^x \bmod p$

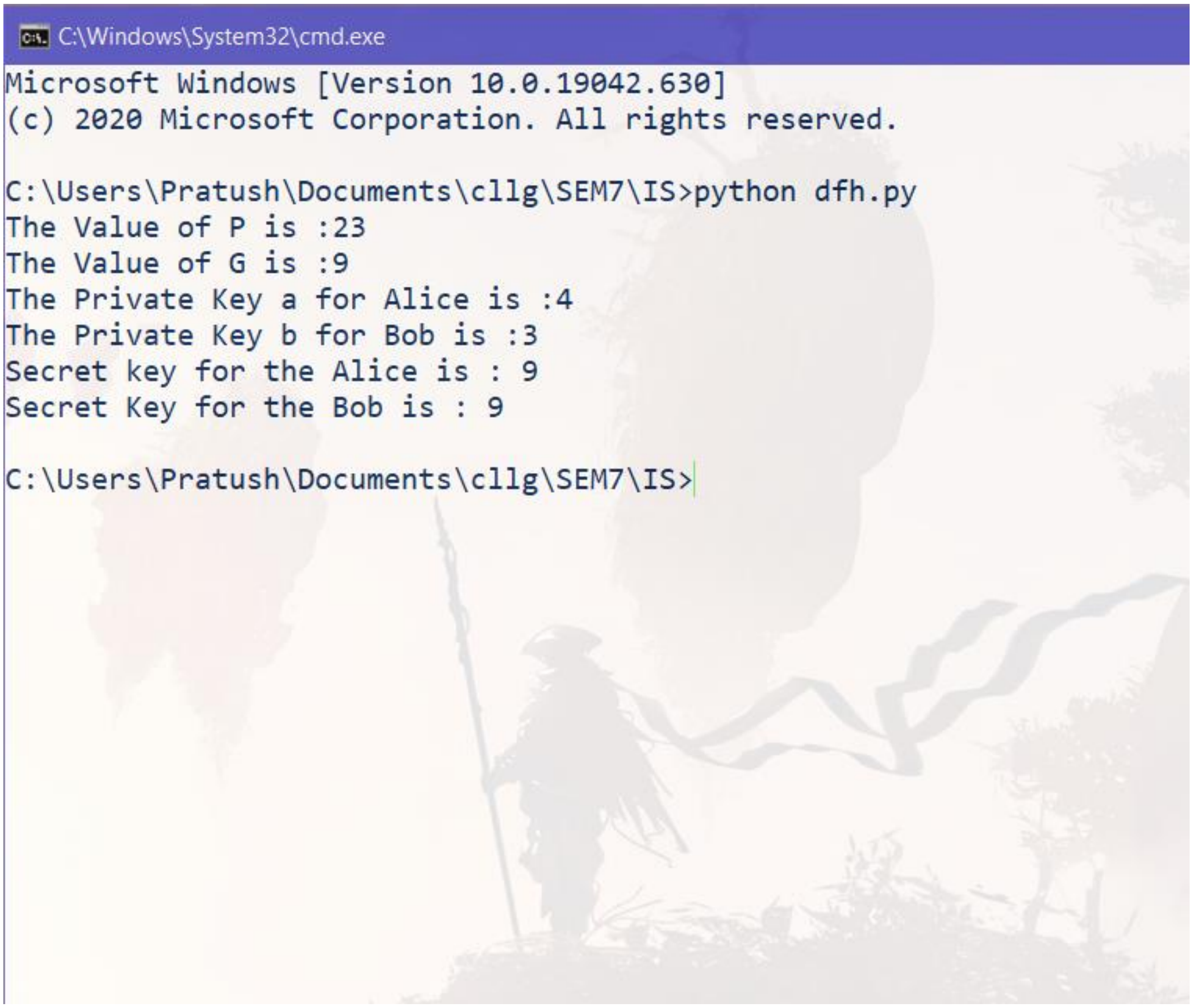
4. Bob computes

   $k=X^y \bmod p$

Code:

```
from random import randint
if __name__ == '__main__':
        P = 23
        G = 9
        print('The Value of P is :%d'%(P))
        print('The Value of G is :%d'%(G))
        a = 4
        print('The Private Key a for Alice is :%d'%(a))
        x = int(pow(G,a,P))
        b = 3
        print('The Private Key b for Bob is :%d'%(b))
        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:



```
Microsoft Windows [Version 10.0.19042.630]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\Pratush\Documents\cllg\SEM7\IS>python dfh.py
The Value of P is :23
The Value of G is :9
The Private Key a for Alice is :4
The Private Key b for Bob is :3
Secret key for the Alice is : 9
Secret Key for the Bob is : 9

C:\Users\Pratush\Documents\cllg\SEM7\IS>
```