

Name: Vishal Salvi

UID: 2019230069

Batch: c

Class: TE Comps

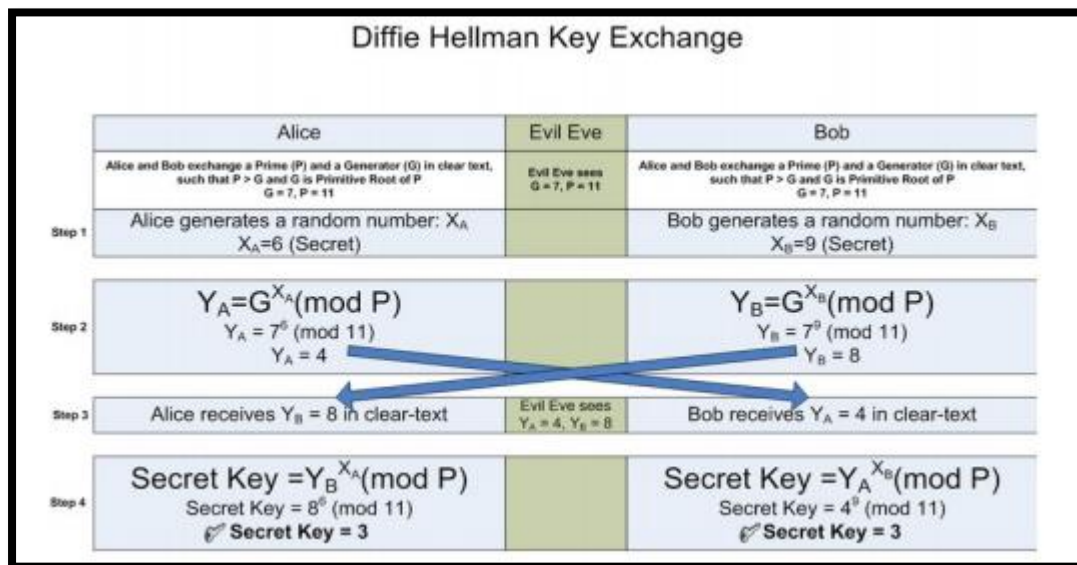
Experiment No 2

Aim: To implement Diffie – Hellman key exchange Algorithm.

Theory:

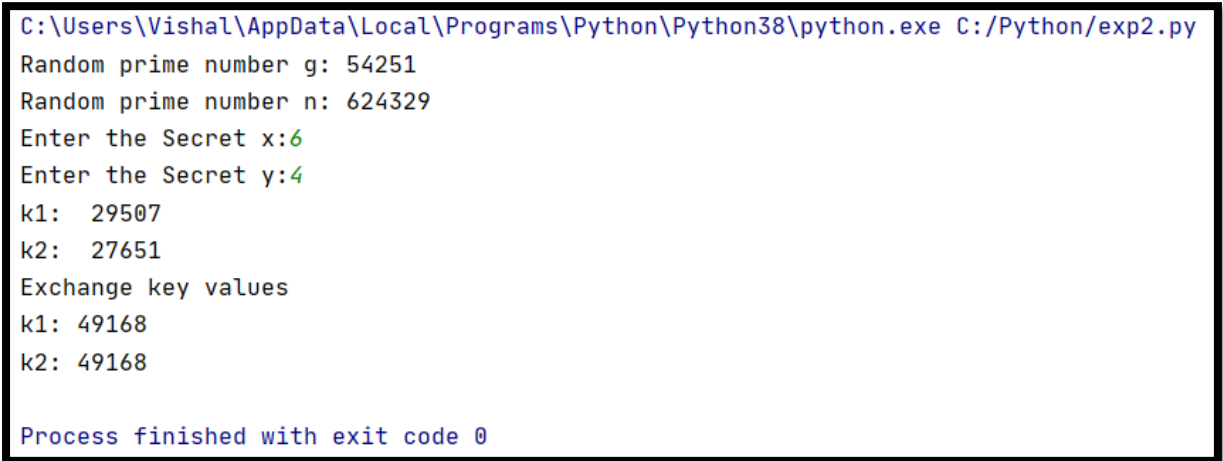
Diffie –Hellman Key exchange algorithm:

The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher. Although Diffie–Hellman key agreement itself is an anonymous (non-authenticated) key-agreement protocol, it provides the basis for a variety of authenticated protocols, and is used to provide perfect forward secrecy in Transport Layer Security's ephemeral modes (referred to as EDH or DHE depending on the cipher suite).



Code:

```
from sympy import *
g=randprime(10000,100000)
n=randprime(10000,1000000)
print("Random prime number g:",g)
print("Random prime number n:",n)
x=int(input("Enter the Secret x:"))
y=int(input("Enter the Secret y:"))
k1=(n**x)%g
print("k1: ",k1)
k2=(n**y)%g
print("k2: ",k2)
print("Exchange key values")
k1_key=(k2**x)%g
k2_key=(k1**y)%g
print("k1:",k1_key)
print("k2:",k2_key)
```

Output:

```
C:\Users\Vishal\AppData\Local\Programs\Python\Python38\python.exe C:/Python/exp2.py
Random prime number g: 54251
Random prime number n: 624329
Enter the Secret x:6
Enter the Secret y:4
k1:  29507
k2:  27651
Exchange key values
k1: 49168
k2: 49168

Process finished with exit code 0
```

Observation:

Diffie Hellman (DH) key exchange algorithm is a method for securely exchanging cryptographic keys over a public communications channel.

Conclusion:

Due to its advantages, the Diffie Hellman key Exchange has proved to be a useful key exchange system. While it is really tough for someone snooping the network to decrypt the data and get the keys, it is still possible if the numbers generated are not entirely random.