LABORATORY

CEL62: Cryptography and System Security
Winter 2021

Experiment 2:	**Implementing Diffie Helman**

Note: Students are advised to read through this lab sheet before doing experiment. On-the-spot evaluation may be carried out during or at the end of the experiment. Your performance, teamwork/Personal effort, and learning attitude will count towards the marks.

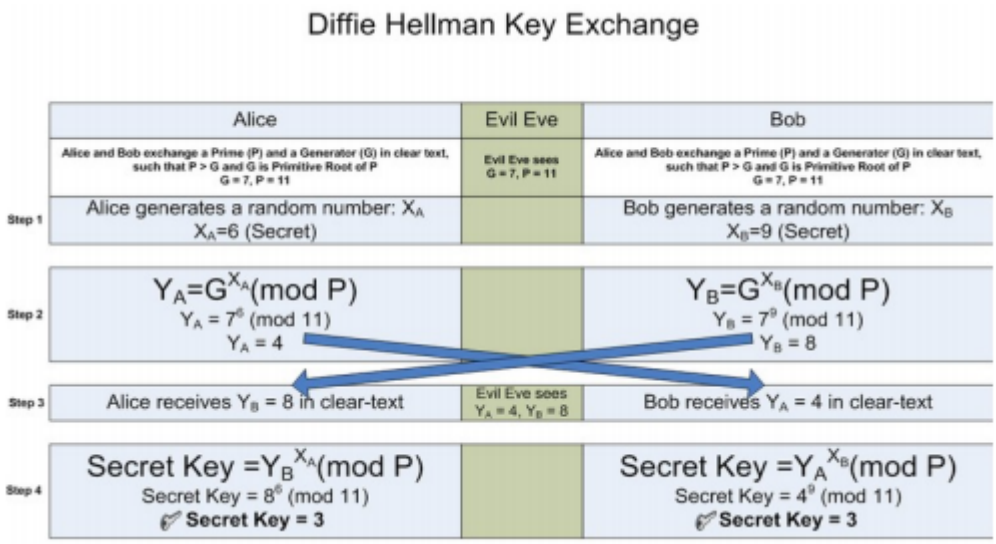
NAME : SHREYAS PATEL

ROLL NO : 42

Experiment 2 : Traditional Crypto Methods and Key Exchange

OBJECTIVE :
Implement Diffie Hellman key exchange algorithm in Scilab/C/Python/R.

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).



a. Diffie Hellman
   i. Enter the Prime Number g:
   ii. Enter second Prime Number n:
   iii. Enter the Secret x:
   iv. Enter the Secret y
   v. K_1:
   vi. K_2:

CODE :

```
import math
```

```
def diffie_hiemann(g,n,x,y):
    a = pow(n,x,g)
    b = pow(n,y,g)
    temp = a
    a = b
    b = temp
    k1 = pow(a,x,g)
    k2 = pow(b,y,g)
    print("The keys are " + str(k1) + " and " + str(k2))
if a == 6:
    print("Diffie-Hiemann Method:")
    print("Enter g and n:")
    g = int(raw_input())
    n = int(raw_input())
    print("Enter x and y:")
    x = int(raw_input())
    y = int(raw_input())
    diffie_hiemann(g,n,x,y)
```

OUTPUT :

```
Enter your choice of method to be used:
6
Diffie-Hiemann Method:
Enter g and n:
23
45
Enter x and y:
3
8
The keys are 1 and 1
```

OBSERVATIONS : This algorithm makes algebraic calculations to turn the keys of both the users to one key which they actually want to share.

CONCLUSION : Through this experiment I came to know the use of these algorithms in cryptography.