Experiment No 2

Nikita Chitre

UID: 2018130006

Batch A

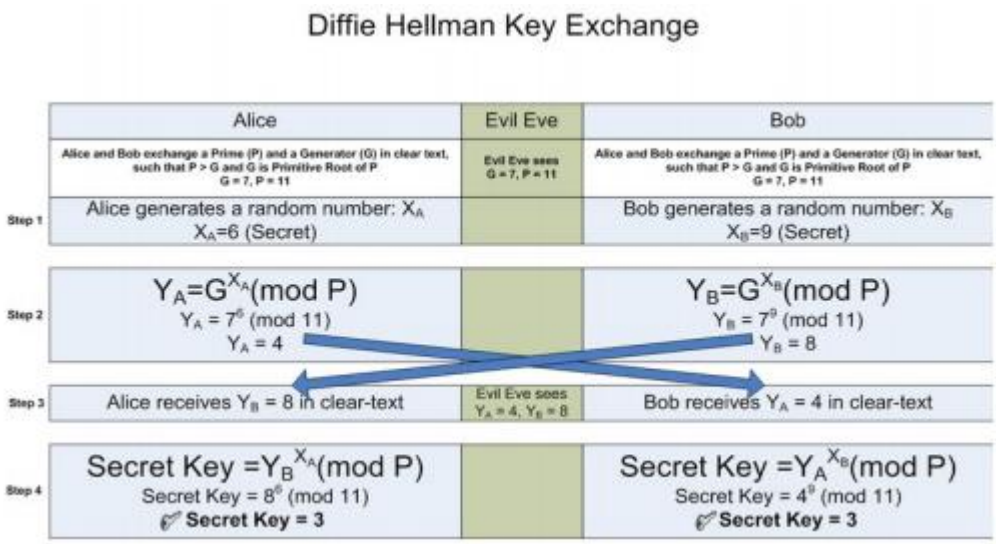
22-01-21

Aim:- To implement Diffie Hellman

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:-

```
def diffie_hellman():
   import random
   import math
   flag = 0
   primes = [i for i in range(50,700) if checkPrime(i)]
   while(flag==0):
      n = random.choice(primes)
      g = random.choice(primes)
      if(n>g and math.gcd(g,n)==1):
         flag = 1


   a = random.randint(5,500)
   b = random.randint(5,500)
   x = int(pow(g,a,n))
   y = int(pow(g,b,n))
   #secret key
   sa = int(pow(y,a,n))
   sb = int(pow(x,b,n))


   print('\t\tAlice\t\t\t\tBob')
   print('\t\tg = : '+str(g)+'\t\t\tg = : '+str(g))
   print('\t\tn = : '+str(n)+'\t\t\tn = : '+str(n))
   print('\t\tSecret key: '+str(a)+'\t\t\tSecret key: '+str(b))
   print('\t\tExchanged Key Bob to Alice: '+str(y)+'\t\tExchanged Key Alice to Bob:
'+str(x))
   print('\t\tSecret: '+str(sa)+'\t\t\tSecret: '+str(sb))


diffie_hellman()
```

Output:-

Alice	Bob
g = : 51	g = : 51
n = : 293	n = : 293
Secret Key a: 67	Secret key b: 91
Exchanged Key Bob to Alice: 183	Exchanged Key Alice to Bob: 291
Symmetric Key: 252	Symmetric Key: 252

Observations:-

- The secret key is never exchanged. The public key is exchanged which is calculated using the two prime numbers and the secret key.
- The final secret key generated at both the ends is symmetric in nature.

Conclusion:-

- Diffie Hellman key exchange is method of exchanging keys over a public channel using secret key and generator which is not shared.
- Vulnerable to middle man attack.