

Experiment 03: Implement and design of Diffie-Hellman Algorithm

Learning Objective: Implement and design of Diffie-Hellman Algorithm

Tools: PyCharm

Theory:

The Diffie–Hellman (DH) Algorithm is a key-exchange protocol that enables two parties communicating over public channel to establish a mutual secret without it being transmitted over the Internet. DH enables the two to use a public key to encrypt and decrypt their conversation or data using symmetric cryptography.

Diffie-Hellman is generally explained by two sample parties, Alice and Bob, initiating a dialogue. Each has a piece of information they want to share, while preserving its secrecy. To do that they agree on a public piece of benign information that will be mixed with their privileged information as it travels over an insecure channel. Their secrets are mixed with the public information, or public key, and as the secrets are exchanged the information they want to share is commingled with the common secret. As they decipher the other's message, they can extract the public information and with knowledge of their own secret, deduce the new information that was carried along. While seemingly uncomplicated in this method's description, when long number strings are used for private and public keys, decryption by an outside party trying to eavesdrop is mathematically infeasible even with considerable resources.

Code:

```
1
2 ▶ if __name__ == '__main__':
3     P = 23
4     G = 9
5     print('The Value of P is :%d' % (P))
6     print('The Value of G is :%d' % (G))
7
8     # Alice will choose the private key a
9     a = 4
10    print('The Private Key a for Alice is :%d' % (a))
11
12    # gets the generated key
13    x = int(pow(G, a, P))
14
15    # Bob will choose the private key b
16    b = 3
17    print('The Private Key b for Bob is :%d' % (b))
18
19    # gets the generated key
20    y = int(pow(G, b, P))
21
22    # Secret key for Alice
23    ka = int(pow(y, a, P))
24
25    # Secret key for Bob
26    kb = int(pow(x, b, P))
27
28    print('Secret key for the Alice is : %d' % (ka))
29    print('Secret Key for the Bob is : %d' % (kb))
30
```

Output:

```

C:\Users\Mech\PycharmProjects\css\venv\Scripts\python.exe C:\Users\Mech\PycharmProjects\css\main.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

Process finished with exit code 0
  
```

Conclusion: After performing the experiment I was able to implement and design of Diffie-Hellman Algorithm.

For Faculty Use

Correction Parameters	Formative Assessment [40%]	Timely completion of Practical [40%]	Attendance / Learning Attitude [20%]	Total
Marks Obtained				