Experiment 03: Implement and design of Diffie-Hellman Algorithm

<u>Learning Objective:</u> Implement and design of Diffie-Hellman Algorithm

Tools: PyCharm

Theory:

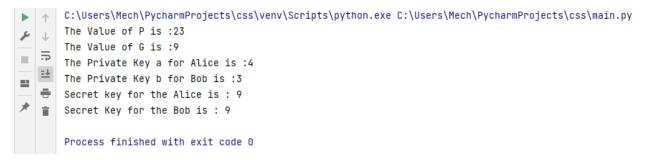
The Diffie—Hellman (DH) Algorithm is a key-exchange protocol that enables two parties communicating over public channel to establish a mutual secret without it being transmitted over the Internet. DH enables the two to use a public key to encrypt and decrypt their conversation or data using symmetric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

Diffie-Helman 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:

```
__name__ == '__main__':
P = 23
  G = 9
  print('The Value of P is :%d' % (P))
  print('The Value of G is :%d' % (G))
  # Alice will choose the private keu a
   a = 4
  print('The Private Key a for Alice is :%d' % (a))
  # gets the generated key
  x = int(pow(G, a, P))
  # Bob will choose the private key b
  print('The Private Key b for Bob is :%d' % (b))
  # gets the generated key
   y = int(pow(G, b, P))
   # Secret key for Alice
  ka = int(pow(y, a, P))
  # Secret key for Bob
   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:



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

For Faculty Use

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