

**Assignment #04 – Public/Private Keys: Diffie-Hellman**

**Due: Monday, 27-Jun-2022 (before 11:59 p.m. ET)**



## Public/Private Keys: Diffie-Hellman

Based on the following information calculate the key for both Alice and Bob, assuming you are Bob. As Bob, the receiver, you should choose a prime number to use as the variable B.

The roles are:

- Sender: Alice
- Receiver: Bob
- Eavesdropper: Eve

Show each of your steps in the process of calculating the key.

Private Information for Alice

- $A = 19$  (not shared with anyone)

Private Information for Bob

- $B =$  prime number of your choosing (not to be shared with Alice or Eve)

Information Shared by Alice

(And available to Bob and Eve)

- $N = 50$
- $P = 41$

Submit your assignment which includes declaration of the value you chose for B and the key which you and Alice will be using based on the steps and calculations you document in a Word, .PDF, or text file.

This assignment is due to be completed before 11:59 p.m. ET/USA on Monday, 27-Jun-2022.

Email Professor Patrick at [PaSlattery@CityTech.CUNY.edu](mailto:PaSlattery@CityTech.CUNY.edu) with any questions or concerns.

Thank you.