Network Security Fall 2018 Project 1

August 30, 2018

Due Date: Friday September 14 11:59 PM
Submission: Source Code & File
Demo: September 25 Office Hours
Group Size: 2
Total Points: 100

Statement of Project: Implement DH Key exchange algorithm for the simple client-server communication as implemented in the provided files server.py & client.py. The current code demonstrates the sending of a file from the server to the client and sets up the appropriate socket connections. The students will NOT need to create the connections, they cam piggy back on the connections created and achieve the public key exchange for DH algorithm. Once the shared key has been established the students should *encrypt* the file being transferred from the server to the client and transfer the *encrypted file*. On the client side the file should be *decrypted* using the same shared key. Finally the server should also send the *hash* of the encrypted file and the client should verify that it received the same file by hash comparison. Note that Python provides functions to compute the hash of inputs. The students should use a variation of the SHA or MD5 hash as implemented in Python.

Note: Please submit the names of the project members along with the submission. There is a 5 point bonus for documenting the code properly.