Feb 20

EE 5453 – Assignment #4

Due date: Feb 27, 11:59 PM

--

This is a group assignment. Work with your group. One submission per group is sufficient.

Problem #1

This is an extension of assignment #3. Extend your previous system:

(a) So that the client and server can agree on two symmetric keys using Diffie-Hellman key exchange: one for confidentiality and one for integrity.
(b) Now, use those two keys to accomplish confidentiality and integrity of files exchanged in either direction between the client and the server.

Learn more about implementing DH online using libraries available for your programming language.