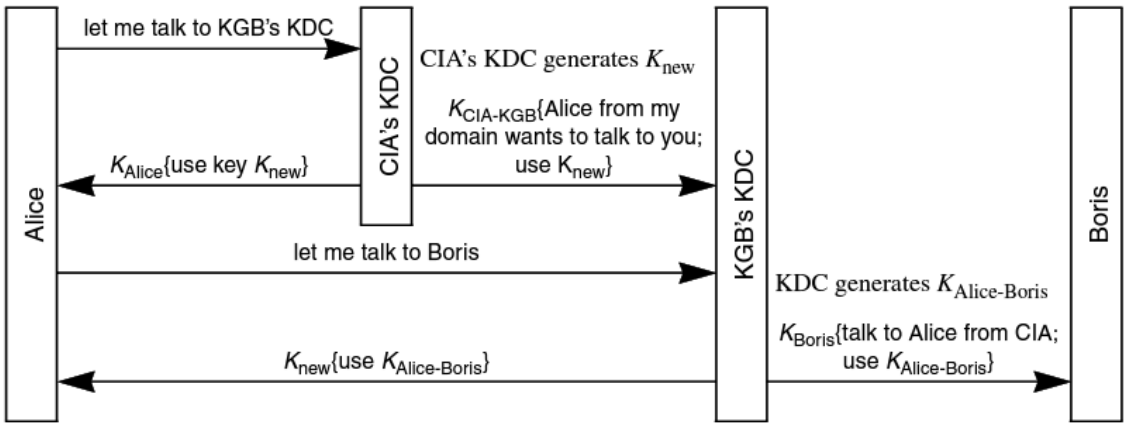
Note: Due Monday, April 8 at midnight;
Each problem is worth equal points (10 points).

8 common problems for everyone, 10 problems in total:

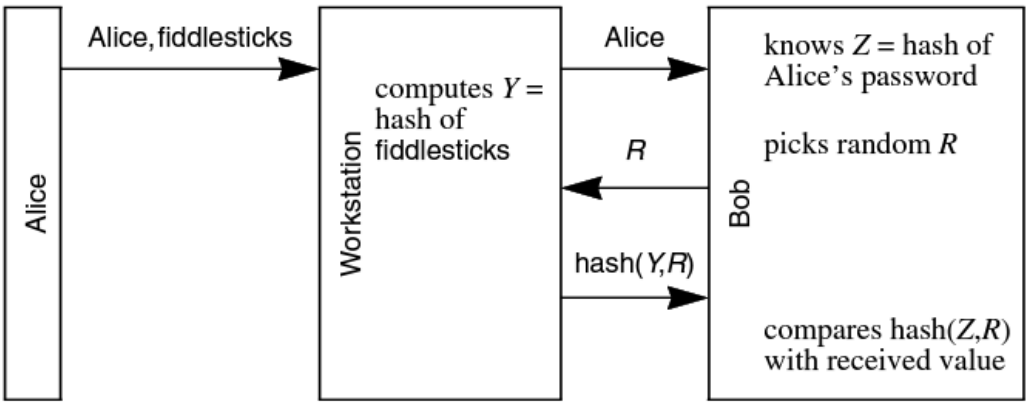
Problems 10.2, 15.6, 15.7, 16.4, 16.6 all from textbook.

Problem 6: When we talked about defenses against Man-in-the-Middle (MitM) Attack, we stated that encrypting the Diffie-Hellman value with the other side's public key prevents the attack. Why is this the case, given that an attacker can encrypt whatever it wants with the other side's public key? In addition, describe at least one other defense mechanism against the MitM attack and explain why it is secure.

Problem 7: Extend the following scenario of two KDC Domains to a chain of three KDCs. In other words, assume that Alice wants to talk to Boris through a chain of three KDCs (Alice's KDC, a KDC that has shared keys with both Alice's KDC and Boris's KDC, and finally, Boris's KDC). Give the sequence of events necessary to establish communication.



Problem 8: In the class, we asserted that it is extremely difficult, without public key cryptography, to have an authentication scheme which protects against both eavesdropping and server database disclosure. Consider the following authentication protocol (which is based on Novell version 3 security). Alice knows a password. Bob, a server that will authenticate Alice, stores a hash of Alice's password. Alice types her password (say fiddlesticks) to her workstation. The following exchange takes place:



Suppose Eve can eavesdrop the communication between Alice's workstation and Bob the server. Is this an example of an authentication scheme that isn't based on public key cryptography and yet guards against both eavesdropping and server database disclosure?

Additional problems for 471 students only:

Problems 10.4, 15.8 all from the textbook.

Additional problems for 571 students only:

Problems 10.3, 15.2 all from the textbook.