CSC 439/539: Advanced Information Security, Spring 2013
Sample Questions on Module 2: Key Distribution and Management

1) Illustrate the working (using a sequence diagram, as in the slides) of the Needham-Schroeder protocol for secure key distribution and authentication.
2) What are the components of a public-key certificate? How is the notion of "trust" used in the context of a public-key certificate?
3) How would you use a "Nonce" to authenticate a user? Explain with an example.
4) What are the different classes of public-key certificates? Explain with an example for each class.

5) Assume users A and B are in the same network and both of them trust a certificate authority CA. Let the public-key certificate obtained by user A from the CA be represented simply as PUB-CERT-A and this public-key certificate should be seen only by user B and not visible to anybody else. Explain how you would send a message M from user A to user B for each of the following cases:

a) User B needs to make sure the message came from user A and not anybody else.
b) User B needs to make sure that the integrity of the message was maintained during transmission.
c) User B needs to make sure both (a) and (b) simultaneously.

6) Assume users A and B in two different networks. User A owns a public-key certificate (PUB-CERT-A) that is digitally signed by a certificate authority (CA-1) whose public-key certificate (PUB-CERT-CA-1) is digitally signed by another certificate authority (CA-2). User A trusts CA-1 and User B trusts CA-2.

(a) Explain how you would send a message M from user A to user B such that it provides integrity, confidentiality and authentication.
(b) What would be the sequence of steps executed by receiver B to extract the message M?

7) Briefly discuss the key assumptions, three important advantages and three weaknesses of Kerberos.

8) Explain the use of a Ticket Granting Ticket and Client-to-Server Ticket in Kerberos.

9) Let there be three servers (a file server, web server and database server) in a network. If Kerberos is used as the authentication protocol, how many times does a client needs to contact the Authentication Server and Ticket Granting Server to communicate with each of these three file servers? Justify your answer.

10) Complete the following sequence diagram for Kerberos: