Tasks to be accomplished in Weeks 6 and 7 (10/9 - 10/22):

1. Read textbook Chapter 4.
2. In Discussion Board forum for this time period, answer the following questions by clicking on the reply link for the questions:
   a. What are the suitable scenarios for adopting Kerberos and X.509 respectively (comparing the two authentication mechanisms)?
   b. The original three-way authentication procedure for X.509 illustrated in Figure 4.6c contains a security flaw. Identify the security flaw and suggest a fix to it. (Problem 4.3 on textbook page 126)
3. Take an open-book quiz in Blackboard Course Documents from 9am of October 20 to 10pm of October 22. You must complete your quiz within one hour in a single session. Make sure you don’t leave the quiz Web page during your quiz session, and you click on the Submit button at the end of your session. If accidents happen and you cannot access your quiz again, send me an email and I will reset the quiz for you. All the quiz questions are conceptual, and they check your understanding of the topics covered in the recent two weeks and whether you have completed the assigned tasks for the time period.

Important concepts/terms worth attention:

Kerberos, X.509, time-stamp, replay attack, nonce, tickets, ticket-granting tickets, ticket granting service, session key, certificate notation, certificate chaining, signed certificate