Homework Assignment 7
ECE 151 / CMPSC 171 - Spring 2014
Due Tuesday, May 27, 5pm
Note: Monday, May 26, is Memorial Day (a Holiday)

1. Consider the **Kerberos Authentication System**, given in Lecture 13, Slides 7 and 8.

(a) Why is the nonce (timestamp) t used in message 6?

(b) Why is the nonce (timestamp) t encrypted?

2. Consider the **Diffie Hellman Key Exchange Algorithm**, given in Lecture 13, Slide 22 as corrected, with the values $n = 19$, $g = 4$, $x = 3$ and $y = 6$.

(a) Show the specific numbers that Alice and Bob send to each other in Steps (1) and (2) of the algorithm.

(b) Show that Alice and Bob construct the same shared secret key in Steps (3) and (4) of the algorithm.

3. Consider an **access control matrix** *M* and the corresponding **access control list** A and **capability list** C.

(a) Explain the relationship between M and A, and the relationship between M and C.

(b) Explain how a server uses an access control list for an object O to allow/disallow access to the object O by a subject (cllent).

(c) Explain how a server uses a capability list for a subject (client) S to allow/disallow access to an object by the subject S.

4. (a) In a **distributed object-based system**, describe the purpose of the **stub** on the client-side and the **skeleton** on the server-side.

(b) Explain what is meant by **marshalling** and **unmarshalling** of messages.

5. Describe two different ways in which the **EJB component model** supports interactions between EJBs.