Homework Assignment 6
ECE 151 / CMPSC 171 - Spring 2014
Due Monday, May 19

Note: Problems 1 through 5 are due on Monday, May 19. Problem 6 (which is a Programming Assignment with a Demo) is due on or before Friday, May 30.

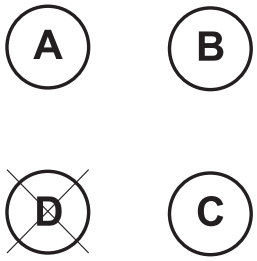
1. Consider the following example of **group multicast**, where there are two senders P1 and P2.

Process P1	Process P2	Process P3	Process P4
sends m1			
receives m1	receives m1	receives m1	receives m1
	sends m2		
receives m2	receives m2	receives m2	receives m2
sends m3			
	sends m4		
receives m3	receives m3	receives m4	receives m3
receives m4	receives m4	receives m3	receives m4

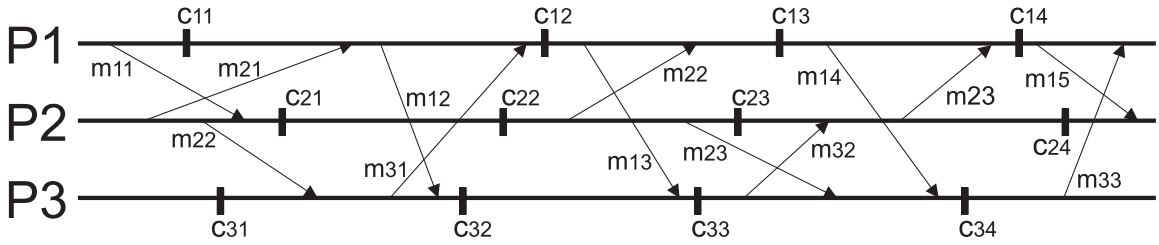
(a) Does this example satisfy **FIF0 multicast**? Explain why or why not.

(b) Does this example satisfy **FIFO atomic multicast**? Explain why or why not.

2. Consider a group of four processes, as shown in the figure below, where process A detects that process D has failed. Create diagrams that show the messages that processes B and C exchange with the other processes until the processes in the new view have installed that view, so that **virtual synchrony** is maintained. Note that Slide 13 in Lecture 11 shows such diagrams only for process 6. To maintain virtual synchrony, further diagrams would be required for the other processes. Show all such diagrams for the following example.



3. The following diagram comprises three processes, messages sent and received by those processes, and checkpoints taken by those processes. Show all of the **recovery lines (consistent snapshots)**. Explain why each of them is a consistent snapshot.



4. Consider the **RSA algorithm** invented by Rivest, Shamir and Adelman for **public key cryptography**.

(a) Given the values $p = 5$ and $q = 13$, find the smallest legitimate value of d and the corresponding value of e.

(b) Using the RSA algorithm and the values of d and e that you found, show the computations performed by the sender to encrypt the message "ABC" where A is represented by 1, B is represented by 2 and C is represented by 3, and the corresponding computations performed by the receiver to decrypt the encrypted message.

5. Consider the **Needham-Schroeder protocol** for **authentication**, as corrected with the additional nonce RB1, given in Lecture 12, Slide 30.

(a) Why is the additional nonce RB1 necessary?

(b) The KDC puts B (Bob) into its reply message and A (Alice) into the ticket. Why does the KDC do so?

(c) In the KDC's message to Alice, the ticket is encrypted with the shared secret key $K_{A,KDC}$. Why is it necessary to encrypt the ticket?

6. For this problem, you will implement the **2-Phase Commit (2PC) protocol** in C/C++ using TCP sockets, or in Java using Java sockets, for one client (coordinator) and two participants.

You may work in groups of two for this problem. You will demonstrate your implementation of the 2PC protocol to the TAs as three processes running on three different computers. The demos will take place during the week of May 26. Please schedule a time for your demo with the TAs. At that time, you will also turn in your code and a short report, describing your program and how to run it.