Recommended exercises on some topics that were not addressed by questions on the homework:

- Suppose that Alice and Bob want to use public-key cryptography to communicate with each other. (a) Explain how Alice may encrypt a message for Bob, and how Bob would decrypt it (i.e., which keys would they use?). (b) Explain how Bob may sign a message for Bob, and how Bob would verify the signature. See textbook or slides for answer.

- What is a digital certificate? See textbook or slides for answer.

- Consider Dijkstra's self-stabilizing solution for K>N where we have N = 4 machines and K = 5. Suppose that the state of machines 0, 1, 2, 3 and 4 is presently 2, 4, 2, 2, 0, respectively.

  (a) Which machine(s) have privilege in the above state? machines 1, 2, 4 have privilege

  (b) Suppose that a privileged machine with the smallest identifier (among the privileged machines makes a "move" (i.e., takes the action specified by the algorithm). List the state of all the machines after this move. In the new state, which machine(s) have privilege?

  New states: 2, 2, 2, 2, 0 (only machine 1 changes state due to condition specified in part (b)).

- Distance-vector routing: Readings for distance vector routing is listed at Lecture 27 (although the material was covered in class previously).

  Suppose that a network consists of 5 nodes, with identifiers A, B, C, D and E. Suppose that the distance vectors at nodes A and B are as shown below at a certain point of time.

  Table at node A

To	Next-Hop	Cost
B	B	2
C	D	8
D	D	2
E	-	infinity

  New table at A:

To	Next-Hop	Cost
B	B	2
C	B	5
D	D	2
E	B	8

  Table at node B below

To	Next-Hop	Cost
A	A	2
C	C	3
D	D	9
E	C	6

Subsequently, node B sends its distance vector to node A. Assume that the cost of link BA is 2. Determine the distance vector at node A after it updates its distance vector on receipt of the message from B.

- The following questions relate to Paxos by Lamport:

Assume that A1 has already seen the prepare corresponding to this accept message with proposal number 10.

(a) Suppose that an acceptor A1 has most recently responded to ~~*prepare*~~ accept message containing proposal number 10 and value 3. In each case below, determine whether A1 will respond if it receives the specified message, and is so, what would be the contents of its response:

(i) A1 receives a prepare message containing proposal number 8 and value 5. No response because number 8 is smaller than 10.

(ii) A1 receives a prepare message containing proposal number 11 and value 5. Respond by sending (11, (10,3) because 11 is the number of the message for which the response is sent, and (10,3) is the largest numbered proposal that A1 has accepted

correction: proposal number 25 (not 20)

(b) Suppose that proposer P1 sends a *prepare* message with proposal number ~~20~~ and value 9, and receives responses from a quorum (majority) of acceptors. Acceptor A1's response to P1 contains a proposal with sequence number 22 and value 17; Acceptor A2's response to P1 contains a proposal with sequence number 23 and value 6; remaining responses do not contain a proposal. accept ~~(20,~~ 6) because 6 is the value returned with largest proposal number.

accept(25,6)

Which proposal number and value would P1 include in its *accept* messages?

See lecture 19 for Paxos. The Lectures page also provides a link to slides used for this lecture.

- Determine whether the various executions shown in the figures in the file below satisfy **causal consistency**. See Lecture 15 and material in assigned reading for the definition of causal consistency.

See course notes