ECE428/CS425/CSE424: Distributed Systems **Spring 2011**

Homework 4 **Due: by 2 pm on 04/12/2011**

Total points: 60

Problem numbers below refer to 4th edition of the textbook.

(1) (10 points) Problem 18.6 from the textbook.

No. Sequential consistency requires that W(y)1 at P1 occur in the interleaving before R(y)1 at P2 and W(x)2 at P2 occur in the interleaving before R(x)2 at P1. This can happen only if the ordering of the operations is violated in one of the processors, violating sequential consistency.

(2) (10 points) Problem 18.18 from the textbook.

W(a)1 at P_1 must happen before R(a)1 at P_2. In fact, P_1's two writes should happen before P_2's operations. For similar reason, P_2's operations should happen before P_3. Hence, the following should be the order of events:

W(a)0 → W(a)1 → R(a)1 → W(b)2 → R(b)2 → R(a)0

However, the last R(a)0 does not make sense since W(a)1 happened after W(a)0.
Hence, the given history is not causally consistent.

(3) (10 points) This question relates to Dijkstra's self-stabilizing mutual exclusion algorithm.

a. What condition(s) must hold before a node enters the critical section when using this algorithm?

For node 0, the previous node's variable should be equal to the node 0's variable.
For other nodes, the previous node's variable should not be equal to a node's variable.

b. When using this algorithm is it possible for the state of the nodes to be corrupted in such a manner that multiple nodes may enter critical section?

Yes. If the states of the nodes are such that all of them have the same value, then it is possible for all of them to enter the critical section.

(4) (10 points) Describe an advantage and a disadvantage of symmetric key cryptography compared to public key cryptography.

Advantage: Symmetric key cryptography is computationally cheaper than public key cryptography.
Disadvantage: Symmetric key cryptography needs different symmetric keys to communicate with different users to avoid one user from being able to read the messages meant for another user.

(5) (20 points) Consider that node A needs to route its messages to another node D in a large network, wherein there are many different routes available for forwarding data from A to D. Suppose that we want node D to be able to detect tampering of its message by an attacker, such that the attacker may compromise at most 1 node in the network. Suggest 2 mechanisms that may be used for this purpose.
For each of the two mechanisms, describe whether the mechanism can always detect message tampering under the specified conditions, or only detect tampering with a probability smaller than 1.

1) **The node A can send a message over multiple routes and node D can compare the messages received over the multiple routes. If at least one of the messages differs from the rest, then the receiver can detect that the message has been tampered.**

   Provided that the routes are node-disjoint, tampering by a single node will always be detected.

2) **Send data along one path and its hash along a node disjoint path. This scheme will detect the tampering with a probability less than 1.**