**NAME:** _____ (First name first) **SCORE:** _____

**COSC 6360** **QUIZ #3** **OCTOBER 23, 2017**

**Closed book.** You can have with you one single-sided 8½ by 11 sheet of notes.

**1.** A system of physical clocks consists of two clocks, namely, one that is fast and gains five minutes every hour and another that slow and loses five minutes every hour. Assuming that the clocks are managed by Lamport's physical clock protocol, what will be the time marked by each clock at 3 pm given that:

**a.** Both clocks indicated the correct time at noon;

**b.** The processors on which the clocks resides stopped exchanging messages at 2 pm; and

**c.** Message transmission delays are negligible. (2×5 points)

**The fast clock will indicate** 3:15 pm **plus or minus a few seconds at 3 pm.**

**The other clock will indicate** 3:05 pm **plus or minus a few seconds at 3 pm.**

| True time | Fast clock | Other clock |
|---|---|---|
| 12 noon | 12 noon | 12 noon |
| 1 pm | 1:05 pm | 12:55 pm |
| 2 pm | 2:10 pm → | 2:10 pm |
| 3 pm | 3:15 pm | 3:05 pm |

2. What is the major disadvantage of ***logical clocks*** over ***physical clocks***? (10 points)

Logical clocks have *anomalous behaviors* in the presence of *outside interactions.*

**3.** Give two examples showing how conventional cryptosystems can complement public key cryptosystems (20 points)

- We can use a conventional cryptosystem to encrypt our secret key(s).
- We can use a public cryptosystem to establish a conventional session key before exchanging messages.

4. What should we try to know about a server before connecting to it ***for the first time*** through SSH? (10 points)

Its *public key* (otherwise, we cannot authenticate it).

**T = ___/50**

**5.** Why are ***RAID level 2*** and ***RAID level 4 never*** used (2×10 points)**?**

- RAID level 2 is never used because omission correction, not error correction, is all what we need.
- RAID level 4 is never used because storing all parity data on the same drive introduces an update bottleneck.

6. According to Shah et al., why was the BitTorrent tit-for-tat policy ill-suited to streaming applications? (10 points)

The BitTorrent tit-for-tat policy makes too many peers to wait for too long before joining the swarm.

**7.** Consider the dynamic voting algorithm used in Pirogue.

**a.** What would be the standard quorum for a cluster with ***four nodes***? (5 points)

Three out of four nodes.

**b.** What would then happen if two of the servers fail at ***exactly the same time***? (5 points)

The cluster would be down.

**c.** Can you think of a solution that would avoid this outcome in fifty percent of the cases? (10 points)

We could introduce a tie-breaking rule.

**T = ___/50**