CMSC 818k **Fall 2007**

Final Exam

Closed everything; Take-Home *Due in my office or mail q by 11:59PM Dec 18*

⊕ *Do not forget to write your name on the first page.*
⊕ *Be* **neat** *and* **precise**. **I will not grade answers I cannot read.**
⊕ *If you have written something incorrect along with the correct answer, you should* **not** *expect to get all the points. I will grade based upon what you* **wrote**, *not what you* **meant**.
⊕ *You should draw simple figures if you think it will make your answers clearer.*
⊕ *If you do not have a calculator, leave your answer in the simplest form you can.*
⊕ *Good luck and remember, brevity is the soul of wit.*

- You have **120 minutes** to do this exam.
- Do either part (a) or part (b) for each question. Cross out the one you skip.
- Maximum possible points: 120.

Name: _____

Problem	Points
1	
2	
3	
4	
5	
6	
Total	

1. (a) Explain secret splitting, and secret sharing.
   (b) Explain blinding, and the electronic voting scheme discussed in class.

2. (a) Discuss how Dynamo maintains consistency.
   (b) Describe the shortcuts Dynamo takes in its version of classsic distributed-system ideas, and why they are appropriate.

3. (a) Describe your favorite systems "idea" paper (does not have to be from this course), why you like it, and how it is important to other work (different idea from the one you chose last time).

   (b) Prove P == NP

4. (a) Describe the life of an update in Oceanstore.
   (b) Discuss the problems Oceanstore would face if it had no trusted nodes.

5. (a) Describe the details of a byzantine fault-tolerant algorithm (w/ picture).
   (b) Where does the 3n + 1 byzantine requirement come from?

6. (a) Describe the Confused Deputy problem, and how to address it.
   (b) Discuss the problem of confinement w/ capability systems, and text.pdf how to address it.