Name _____

Midterm — March 13, 2007

ECE 428 / CS 425 / CSE 424

Spring 2007

Academic Honesty Policies:

- This exam is open book and open note. No other external sources may be used other than nonelectronic aids (notes and books) you bring with you into the exam.
- You must not give or receive assistance to any other person taking this exam, nor may you talk about the exam with your classmates who have not taken it until the midterm is returned to you. **Some students will take a conflict exam later.**
- Electronics are NOT allowed, and must remain off for the duration of the test. The three exceptions to this rule are:
  - Medically necessary life support devices
  - Simple calculators that cannot display characters
  - Watches that cannot store, transmit, or receive alphanumeric data

  This rule prohibits the use of devices including, but not limited to, general purpose computing devices (laptops, PDAs, graphing calculators, etc.), telephones of any kind (cellular, VoIP, wireless, wired, or satellite), pagers, radios, and music players are not permitted and must remain off at all times during the exam. Storage or communications of any data regarding the class on any electronic device is prohibited.

General Instructions:

- Show your work for all problems. Correct answers with no (or incorrect) work shown may result in partial credit.
- Draw a box around all final answers less than one sentence long.
- You must not write your answer in red.
- If there is any confusion as to the question being asked, request clarification from the proctor. If you need to make additional assumptions to complete the problem, state them.
- Unless otherwise specified, *why* is a technical question.
- If you cannot fit your work in the space provided, use the back side of the same page to complete your work to the extent practicable. **Do not write on the back of this sheet.**

Question	1	2	3	4	5	EC	Total
Possible	7	10	12	10	11	2	50 (+2)
Score							

Name _____

1. (7 Points) In the context of this class thus far, for each of the following terms, specify the general topic area it is used in, and briefly (one sentence) define it.

a. Synchronization Delay

b. Fairness

c. Serial Equivalence

d. Distance Vector Routing

e. Distributed Hash Table

f. Data Authentication

g. Weak Collision Resistance

Name _____

2. (10 Points) Will Chandry-Lamport work (that is, provide a consistent cut) in the following network?

- all pairs of processes are connected by a pair of unidirectional channels (one in each direction)
- each channel is synchronous, so messages are received without loss, and with bounded delay
- nodes cannot fail
- channels may reorder packets
- each received packet is processed in the order received.

If so, explain why; if not, give a counterexample and design an extension to Chandry-Lamport that works in this network.

Name _____

3. (12 Points) When we proved the impossibility of consensus in an asynchronous distributed system where a single node failure is possible, we proved that even *weak consensus* was impossible. Any consensus result (strong or weak) requires that whenever two output bits are set, they must be set to the same value, that both 0 and 1 are possible results of the algorithm. In *weak consensus*, we only require a single node to set its output bit. In *strong consensus*, we will require *each* nonfailed node to set its output bit. Where explicitly stated in the subsections below, we'll also consider an additional type of failure, *link failures*; messages attempted over failed links will never be delivered. For each of the following situations, state whether strong consensus is possible and whether weak consensus is possible. If it is possible, give an algorithm (or name one described in class). If it is not possible, give a proof (you may build on results shown in class).

a. (2 Point) Synchronous, failures possible

b. (2 Point) Asynchronous, failures impossible

c. (4 Points) Synchronous over nonfailed links, link failures possible, but node failures impossible

d. (4 Points) Synchronous over nonfailed links, link failures possible, node failures possible

Name _____

4. (10 Points) Conceptually explain why SM(m) requires fewer non-attacking users than OM(m) to exclude the same number of attackers. I'm looking for an intuition, not (only) mathematical expressions. For example, the following argument (in addition to being wrong) does not capture the spirit of this question:

> *OM(m) requires 4m normal users, and SM(m) requires only 3m, so therefore OM(m) requires more.*

The following argument (though it is wrong) captures the spirit of this question:

> *OM(m) involves lynching the traitors, which requires more work than SM(m), which simply identifies them for exclusion.*

Name _____

5. (11 Points)

a. (7 Points) Consider a Chord network for $r = 5$ containing N2, N5, N13, N15, N16, N19, and N31. Show the finger tables of nodes N13 and N19. Show the recursive calls involved in N15 searching for key K6.

b. (2 Points) What global routing metric, if any, is minimized by a distance vector routing protocol?

c. (2 Points) What global routing metric, if any, is minimized by BGP?

Name _____

EC. (2 Points) **Hint: These questions take more time per point than the others. Do not attempt this problem until you have finished the others. No partial credit on individual questions.**

a. (1 Point) Prove the homomorphism of the DLOG hash, that is, that $H(a + b) = H(a)H(b)$.

b. (1 Point) What is the necessary and sufficient condition under which batch verification of the DLOG hash provides data authentication? Prove your answer (and that it is both necessary and sufficient) under the discrete log assumption (that is, that calculating a discrete logarithm is difficult).