Assignment 8: April 8 through April 16

For Recitation, Thursday, April 8 (R17: Why Cryptosystems Fail)

For recitation, read Anderson's "Why cryptosystems fail" (#22). It is pretty easy reading, but read it with care; the author provides many interesting examples and insights.

The second **Design Project** will be available today on the Web. Form a team of three as soon as possible, and send an e-mail message to your recitation instructor before next Thursday listing the members of your team. All students in a team *must* have the same recitation instructor, since he will grade your Design Project 2 paper. Note that the student page of the 6.033 Web site contains an up-to-date list of potential team members.

For Lecture, Monday, April 12 (L18: Certification)

Last lecture on security. Start on the reading assignment for tomorrow and take some time to think about Design Project 2.

For Recitation, Tuesday, April 13 (R18: E-Mail Pseudonym Server)

Each year we assign a timely paper of relevance to computer systems and society. For recitation, read "The design, implementation and operation of an email pseudonym server" (handout #25) by David Mazières and Frans Kaashoek. We handed out this paper during last Wednesday's lecture. The topic of this paper also relates to design project 2 from 1997.

Note the following extra feature: today there will be a panel discussion in Kresge auditorium on this very subject, including Scott Charney of the United States Justice Department, Prof. Kaashoek, and David Mazières. Mr. Charney is expected to take a somewhat negative view of the service described in the paper. The panel discussion is part of the Laboratory for Computer Science 35th anniversary celebration, and Kresge is expected to be packed full (it is an invitation-only affair), but the discussion is to be carried live on the M.I.T. cable system and the M.I.T. online video system. So locate a convenient access point for the cable broadcast and plan to watch at 4:00pm. Watching the panel is not a required assignment, but it is so timely and pertinent that we highly recommend it.

No reading report due this week. Study for the quiz.

Also, you might want to spend some time thinking about Design Project 2.

For Lecture, Wednesday, April 14 (L19: Fault Tolerance)

This lecture begins a new topic of fault-tolerant computing systems. In preparation, read "Chocolate" by

Plauger (#25) and "Engineering: history and failure" by Petroski (#24). These two papers are very short, but provide you with some good insights.

For Recitation, Thursday, April 15 (R19: More Fault Tolerance)

The reading for today is "High-availability computer systems" by Gray and Siewiorek, reading #26. This paper is a heavy duty paper; read it with care. It introduces some terminology and tries to build an appreciation of the difficulty in attaining continually available systems.

In addition, read "The space shuttle primary computer system" by Spector and Gifford, reading #28. This paper is quite long; you can skim much of the paper, but as you do so slow down enough to figure out the following things: How are they using redundancy? What is force-fight voting? What are alibis? You should have sent your recitation instructor e-mail listing your three-person Design Project 2 team by today.

For Quiz 2, Friday, April 16

Quiz 2 will be held from 2-3pm on Friday, April 16, 1999. The quiz will cover all the material up to and including the April 13th recitation. The quiz will be open book and open notes meaning that you can use any course materials from this year. The quiz will be held on the third floor of Walker and in 34-101. See the chart below to determine which location you should go to for the quiz.

Last Name	Location
A-R	Walker
S-Z	34-101

There is no quiz review as we had for quiz 1, but TAs will hold extra office hours. Look for an announcement closer to the date of the quiz.

If you have a problem regarding the scheduling of the quiz, email Professor Kaashoek at *kaashoek@mit.edu*.

System aphorism of the week

KISS: Keep It Simple, Stupid.
