ECS 227: Modern Cryptography
Course Information

6 January 2000

Instructor

Phil Rogaway
Engineering II, #3063
Office: (530) 752-7583
Home: (530) 753-0987
E-mail: `rogaway@cs.ucdavis.edu`
WWW: `www.cs.ucdavis.edu/~rogaway/`
Office Hours: When I set official official office hours for this course they never seem to get used. So just drop by at by any time, or you can make an appointment.

Lectures

TR 1:40 pm – 3:00 pm in 80 Soc Sci

Course Web page

http://www.cs.ucdavis.edu/~rogaway/classes/227/winter00 You can easily navigate there from my homepage, http://www.cs.ucdavis.edu/~rogaway. I'll stock our course Web page with notes, homeworks and some pointers. I'll try to provide notes by the lecture following the completion of any topic.

Expectations

(1) Attend class regularly (and think while you're there).
(2) Read and understand the materials I hand out.
(3) Do the homeworks I give out. There will be about five homework sets, each of about 1–4 problems. Some of the problems might require significant thought. Make the writeups elegant. Please don't turn in incorrect solutions. You can collaborate, but if you work in a group you should turn in one writeup per group.
(4) I will ask you to select one paper that we did not cover in class, read and understand it, and do a short writeup about that paper (typeset; 2–3 pages).
(5) At the end of the term, during finals week, I will meet with each student for 30 minutes for an "individualized" discussion/final. I won't ask you anything hard, and I am really assessing how well I've done as much as I am how much you've gotten out of the class. Students have told me in the past that they are intimidated by this meeting. Don't be; it's really not a big deal.

This is a non-required graduate class, so I expect students to be here because they're genuinely interested in learning the material.

Prerequisites

Typical background might be a graduate-level course in algorithms (eg., ecs222A), an undergraduate-level course in theory (eg., ecs120), and some upper-division math classes, including probability. You can succeed in this course with a weaker or different background than what's above. In particular, a strong mathematics background but no computer science is probably fine. Top undergraduates are welcome as well.

Material

This course gives a "rigorous" approach to cryptography. The emphasis is on theorems and, even more, on formal models and meaningful definitions. At the same time that we aim for rigor, I want to convey the *practical* value of modern cryptography. Here is a rare subject in that you can do work of significant mathematical/theoretical content which, at the same time, is highly applicable to solving real-world problems. As evidence, note that cryptographers are, currently, extremely employable!

I will decide what material to cover as time goes on, according to student feedback and my own activities/interests during the quarter. In addition, I prefer to cover somewhat different material each time I teach this course, so if you've taken this class before, you might profit by coming once again. Topics might include:

- Symmetric encryption
- Asymmetric encryption
- Message authentication codes
- Digital signatures
- One-way functions
- Bit commitment
- Interactive proofs
- Zero-knowledge
- Entity authentication
- Key distribution
- Secret sharing
- Secure function evaluation

Research in cryptography

You may treat this class as an "invitation" for doing research in cryptography—a most unusual and wonderful subject. Welcome!