ECS 227: Modern Cryptography
Course Information

7 January 1999

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: T 4:30–5:30, or by appointment, or without one.

Lectures

Thursdays from 6:10 pm – 9:00 pm in 267 Olson.

Course Web page

http://www.cs.ucdavis.edu/~rogaway/classes/227/fall99/

You can easily navigate their from my homepage. I'll try to provide notes within a couple days after completing each lecture or topic. The notes may be quite "rough."

Expectations

(1) Attend class regularly (and think while you're there). (2) Read and understand as much of the distributed papers as is feasible for you. (3) Do the homeworks I give out — as many as you can solve. There won't be many —at most 20— but some of the problems might require significant thought. Make the writeups elegant. Please don't turn in incorrect solutions. (4) 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!