ECS 227: Modern Cryptography
Course Information

26 September 1996

Instructor

Prof. Phil Rogaway
Engineering II, #3063
Office: (916) 752-7583
Home: (916) 753-0987
E-mail: `rogaway@cs.ucdavis.edu`
WWW: `http://wwwcsif.cs.ucdavis.edu/~rogaway/`
Office Hours: W 9:30–10:30, or by appointment, or without one.

Lectures

Tuesday and Thursday from 4:40 pm – 6:00 pm in 144 Olson.

Course Web page

http://wwwcsif.cs.ucdavis.edu/~rogaway/classes/227/fall96/handouts.html. I'll try to provide notes within a couple days after completing each lecture or topic. Some (all?) of the notes may be pretty "rough." You can navigate to the course Web page from my own home page (go to "teaching"), or from the CS Department's home page (go to "CSIF" — "Online class notes").

Expectations

You should submit to being photographed; attend class regularly (and think while you're there!); read and try to understand distributed papers; do any homeworks I give out. There won't be many (perhaps four), but some of the problems on the homeworks could take significant thought.

At the end of the term, during finals week, I plan to meet with each student for 30 minutes for an "individualized" discussion/final exam. I won't ask you anything terribly hard, but I would like to see evidence that you've been following the class and understanding the basic notions and results. If you have been, there's absolutely no need to study or concern yourself with our little chat.

This is a non-required graduate class, so I expect students to be here because they're genuinely interested in learning the material. Students who evidence conscientious performance will probably get an "A". Other students might not.

Prerequisites

An appropriate level of background would 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. I encourage top undergraduates to take this class.

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 within industry. They can even demand rather extreme consulting fees.

I will decide what material to cover as time goes on, according to student interests and my own activities during the quarter. In addition, I prefer to cover somewhat different material each time this course is taught. There is enough material in modern cryptography for several quarters, but I'll try to talk about a good fraction of the following:

1. Symmetric encryption
2. Asymmetric encryption
3. Message authentication codes
4. Digital signatures
5. One-way functions
6. Bit commitment
7. Interactive proofs
8. Zero-knowledge
9. Identification
10. Entity authentication
11. Key distribution
12. Secret sharing
13. Secure function evaluation