ECS 227: Modern Cryptography
Course Information

9 January 1995

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: Wednesday 2-3, or by appointment, or drop by without one.
Course Web page: accessible off of my home page, will be set up as a repository of homeworks, handouts, etc..

Lecture

Tuesday and Thursday from 4:40 pm – 6:00 pm in 123 Wellman, UC Davis.

Expectations

Students should submit to being photographed, or bring one in one from home, or explain why your image must not be captured on film. In addition, students should:

1. Participate: attend class regularly, think and take part in class discussions, study the papers given out, and scribe, if requested (at most two lectures).
2. Do the homeworks. (There won't be much, but it will take some thought.)
3. Do a final project
   (a) Expository or semi-original or original.
   (b) Due the last day of class. (Prefer earlier.) No late projects!
   (c) Well-written, thoughtful. Terse: 2–8 pages.
   (d) Topic must be approved in advance, by the end of week 7.
4. Visit me during the last week of class for a friendly, at most 30 minute oral quiz/discussion. I'm not going to ask you anything very hard— I just want evidence that you've been paying attention and understanding the basic notions we've been talking about.

Note that there is no final for this class.

This is a non-required graduate class. Thus I expect students to be here because they're interested in learning the material. Students who evidence conscientious performance on the above four items will get a grade of “A”. Other students might not.

Prerequisites

“Ideal” prerequisites are a graduate-level course in algorithms (eg. ecs222A), an undergraduate-level course in theory (eg. ecs120), and some upper-division math, including probability. You can succeed in this course with a weaker background. I encourage good 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.

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, so don't expect that we'll cover all of the following topics:

1. Complexity theoretic foundations
2. Symmetric encryption
3. Asymmetric encryption
4. Message authentication codes
5. Digital signatures
6. The random oracle model
7. One-way functions
8. Pseudorandom generators
9. Pseudorandom function families
10. Bit commitment
11. Interactive proofs
12. Zero-knowledge
13. Non-interactive proofs
14. Identification
15. Session key distribution
16. Secure function evaluation
17. Byzantine agreement