ECS 227: Modern Cryptography

TR 4:40–6:00 pm (beginning 1/9/96). 123 Wellman (UC Davis). CRN 87063.

Phillip Rogaway
Eng II, #3063, (916) 752-7583, `rogaway@cs.ucdavis.edu`

In this course we'll look at the ideas underlying modern cryptography and cryptography-inspired complexity theory. This is a field which draws its basic problems from computer security, but its outlook and methods rest with theoretical computer science and allied areas of mathematics. We'll address "classical" problems —like how Alice might send a secret message to Bob— as well as more "modern" problems —like how a friendly alien can prove a theorem to a distrustful earthling. I won't assume any particular background material— say an undergraduate algorithms/theory of computation course, plus a suspicious disposition. Sample topics (complete with English-language translations):

- One-way functions. (It's easier to break a glass than to reassemble the pieces.)
- Pseudorandom generators and functions. (Making lots of randomness out of a little bit.)
- Public Key Encryption. (Bob wants to send a confidential message to Alice, but Eve is listening in.)
- Interactive proof systems. (How *much* can a really smart space alien teach us, even if she likes to kid around?)
- Zero-knowledge. (How *little* information can you convey in a proof and still get full credit?)
- Secure computation. (Is it possible to play high-stakes poker over the Internet?)