CS 427 / 519: Cryptography

Instructor: Dr. Mike Rosulek, <rosulekm@eecs.oregonstate.edu>

TA: Peter Rindal, <rindalp@oregonstate.edu>

Meets: MWF 1, in LINC 314

Website: http://eecs.oregonstate.edu/~rosulekm/cs427
Please check often for announcements, homeworks, etc.

Office hours: Mike: MW 2-3, or by appointment, in my office (KEC 3063)
TA office hours to be announced

Prerequisites: MTH 232, programming fluency (in a language of your choice). CS 321 or 325 helpful but not required.

Textbook: We will use *The Joy of Cryptography,* a free textbook that I have written. For a second opinion, I recommend the following:

- *A Course in Cryptography*, Rafael Pass & abhi shelat (free online).
- *Cryptography, an Introduction*, Nigel Smart (free online).
- *Introduction to Modern Cryptography*, Jonathan Katz & Yehuda Lindell (dead tree).

Software: We'll do computations on very large ($\sim 2^{1000}$) integers, which requires some special libraries. Examples in class will use `pari/gp`, a free open-source library for number theory & abstract algebra. It's installed on `nome` and `flip`, and can be downloaded from http://pari.math.u-bordeaux.fr.

Course Overview

Historical cryptography was an arms race between the ingenuity of the "good guys" in designing ciphers and the "bad guys" in breaking them. Modern cryptography, however, allows us to *mathematically prove* statements about security. A major theme in this course learning how to talk about security in such a *rigorous* and *precise* way. In this course you should expect to learn how to:

- State and interpret the standard formal definitions for the most common cryptographic security properties (privacy and authentication).
- Formally prove security properties of sound cryptographic constructions, and break the security of unsound ones.
- Choose the appropriate cryptographic primitive for a task (block ciphers, hash functions, MACs, public-key encryption, etc.) while avoiding common pitfalls.

Along the way, you will also learn how the most common cryptographic constructions work.

Grad Increment

Students enrolled in CS 519 will be assigned additional problems on each homework. These problems will often be more theoretical in nature (*e.g.*, understanding security definitions as objects worthy of study in their own right). In their final projects, grad students will engage with the academic literature.

Assessment

10% **Reading responses:** Read the assigned readings *before the scheduled class,* then on Canvas respond to question prompts, and write any questions you have. These responses will be graded for good-faith effort, and will inform our classtime activities.

30% **Problem sets:** Expect roughly 6 homework assignments, with a mixture of math, programming, computation, security proofs, attacks, problem solving. Submissions must be typed and submitted on Canvas. **No late homeworks!** If you don't already have my approval to submit a late homework, expect a score of zero.

40% **Exams:** There will be a midterm exam and final, each worth 20%.

20% **Small project:** Undergrads will find an example of cryptography being used inappropriately or implemented incorrectly, *in a real-world system,* and write a report on the incident. Grad students will read an academic paper (or two) and write a summary/evaluation. More guidelines will be provided later.

Other Policies

Cheating: Academic dishonesty (including plagiarism and cheating) will not be tolerated. Consult the university's student conduct code for more details. I will follow the guidelines given there, and seek out the maximum allowable penalty for violations that occur in this course.

If you have a question about what constitutes academic dishonesty, please ask me.

Disabilities: Accommodations are collaborative efforts between students, faculty, and Disability Access Services (DAS). Students with accommodations approved through DAS are responsible for contacting the faculty member in charge of the course prior to or during the first week of the term to discuss accommodations. Students who believe they are eligible for accommodations but who have not yet obtained approval through DAS should contact DAS immediately at 737-4098.