Advanced Cryptography
University of Michigan, Winter 2017

Course Information and Syllabus

Instructor: Chris Peikert
GSI: Navid Alamati

1 General Information

Cryptography, or "secret writing," is nearly as old as written communication itself. Yet only over the past few decades has it grown from a "black art" into a science with rigorous mathematical foundations and methodologies. These have taken cryptography far beyond its roots in simple secret codes, to a discipline with far-reaching influence on computing as a whole.

This class is a graduate-level, theory-oriented introduction to the foundations of modern cryptography. The emphasis is on essential *concepts*, precise *attack models* and *security definitions*, and *construction and proof techniques*. Topics include:

- symmetric-key cryptography, including: information-theoretic security, pseudorandom generators and functions, encryption and authentication;
- public-key cryptography, including: number theory, encryption, digital signatures, and identity-based encryption;
- basic protocols, including: secret sharing, commitment, and zero knowledge.

As time permits, we may also touch upon special topic areas such as secure multiparty computation, private information retrieval, fully homomorphic encryption, or digital money.

1.1 Times

Lectures: Mon/Wed 9-10:30am, Beyster 1690

Discussion: Fri 1:30-2:30pm, Beyster 1690

Office hours: Chris: Mon 10:30-11:30am, Beyster 3601. Navid: Fri 2:30-3:30pm (Learning Center).

1.2 Materials

All online resources, homework uploads and downloads, Q&A, etc. can be found at the following locations:

- Canvas: `https://umich.instructure.com/courses/114824`.
- Piazza: `https://piazza.com/umich/winter2017/eecs575/home`.

The required textbook is *Introduction to Modern Cryptography* (2nd edition) by Jonathan Katz and Yehuda Lindell. As appropriate, supplementary lecture notes will be posted on the course Canvas page.

Extra resources include the following excellent textbooks:

- *Foundations of Cryptography*, Vol. 1 and 2 by Oded Goldreich. A very comprehensive treatment of the theoretical foundations of cryptography; a very good reference for those interested in understanding the material in greater depth.
- *A Course in Cryptography*, by Rafael Pass and abhi shelat, freely available at `http://www.cs.cornell.edu/courses/CS4830/2010fa/lecnotes.pdf`.

1.3 Prerequisites

This course is mathematically rigorous, hence the main prerequisite is *mathematical maturity*. Specifically, students should be comfortable with reading and writing formal definitions and proofs, devising and analyzing algorithms and reductions between problems, and working with probability.

Helpful prior courses—none of which are formal prerequisites, but the more the better—include:

- EECS 475 (Introduction to Cryptography),
- EECS 477 and/or 586 (Algorithms),
- EECS 574 (Computational Complexity),
- EECS 598 (Randomness and Computation),
- Any Mathematics courses on discrete probability or number theory.

The instructor reserves the right to limit enrollment to students who have the necessary background.

2 Course Policies

2.1 Grading

Grades will be determined roughly as follows:

(50%) Homework assignments (6–7) and peer review, due approximately every two weeks. Collaboration and external sources are allowed; see academic honesty policy for details.

(25%) Take-home exam #1, Feb 6–13. *No collaboration or external sources are allowed.*

(25%) Take-home exam #2, April 10–17. *No collaboration or external sources are allowed.*

All submitted work will be graded on *correctness*, *clarity*, and *conciseness*, and must be *typed*, preferably in LaTeX (templates will be made available). It is good practice to start any longer solution with an informal (but accurate) "proof summary" that describes the core idea(s). This will help the reader—and you!—understand your solution better.

There are no predetermined score thresholds for grades A/B/C/etc. Your primary focus should be on *learning the material*, not your grade.

2.2 Academic Honesty

For the take-home exams, your submissions must exclusively represent your own work: *absolutely no collaboration or consultation with external sources is permitted.* Specifically, you may refer only to materials that you and your fellow students prepare prior to the release of each exam, and to any materials or clarifications provided by the instructors.

On homework assignments, collaboration and consultation with external sources is allowed and encouraged, subject to the following conditions:

1. You must first understand the problem on your own and make an initial reasonable attempt to solve it.
2. You must write you own solution, and list your collaborators/sources for each problem.
3. You may not submit a solution that you cannot explain orally.

There is no hard-and-fast list of (dis)honest conduct. When in doubt, err on the side of caution, or ask the instructor. Dealing with academic dishonesty is unpleasant for everyone involved, so please follow these policies!

3 Schedule

The course will be broken loosely into units, each covering a number of topics within a certain broad theme. The approximate plan is as follows; note that the pace and/or content may change as needed, or to reflect levels of interest.

- **Overview, information-theoretic security:** Overview of course. Shannon/perfect secrecy.
- **Symmetric cryptography:** Computational security. Pseudorandom generators, functions, permutations, and practical/theoretical constructions. Encryption, chosen-plaintext and chosen-ciphertext attacks. Message authentication. Hash functions.
- **Asymmetric cryptography:** Number theory and cryptographic assumptions. Public-key encryption. Digital signatures. Identity-based encryption.
- **Protocols.** Commitment. Identification schemes. Secret sharing and threshold cryptography. Interactive proofs and zero knowledge.
- **Special topics.** Possible topics: Fully homomorphic encryption and applications. Advanced zero knowledge. Secure multiparty computation.

Special Dates

Note the following special dates:

- **Jan 16, Feb 27, Mar 1.** No class (MLK Day, Spring Break).
- **Feb 6–13.** Take-home exam #1, due by start of class Feb 13.
- **Apr 10–17.** Take-home exam #2, due by start of class Apr 17.