1 General Information

Cryptography, or "secret writing", is nearly as old as written communication itself. Yet only over the past few decades has it matured into a science with rigorous mathematical foundations and methodologies. This scientific approach has transformed cryptography into a discipline with far-reaching influence on computing and society.

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, authentication, authenticated encryption;
- public-key cryptography, including: number theory, encryption, digital signatures, and identity-based encryption;
- basic protocols, including: secret sharing, commitment, and zero knowledge;
- applications, including: encrypted data management, secure messaging, and privacy-enhancing technologies.

Though this class will focus on the theory of cryptography, it will also discuss how this theory connects to practice. Particular attention will be paid to the *contexts*, both technical and social, in which cryptography is used in today's world.

1.1 Email Contact and Times

Paul's email is paulgrub@umich.edu. Alexandra's email is aveliche@umich.edu. To contact the course staff via email, please include **[EECS575FA22]** in the subject of the email. This makes it *vastly* easier to manage course emails, and increases the likelihood of receiving a timely reply!

Times for the course are as follows:
Lectures: Mon/Wed 9–10:30am, Dow 1005
Discussion: Fri 1:30–2:30pm, Dow 1005
Office Hours: Paul: Wednesday 10:30–11:30am, in BBB 4709. Thursday, by appointment only. Alexandra: 5–6pm Mondays and 2:30–3:30pm Fridays, outside BBB 3956. (With notice, Alexandra's OH may also be held in the BBB Learning Center.)

1.2 Materials

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

- Lecture notes: https://github.com/pag-crypto/EECS575-fall22 (including PDFs with in-class markups)
- Canvas: https://umich.instructure.com/courses/546123
- Piazza: https://piazza.com/class/l79a7bug761mw

- Gradescope: https://www.gradescope.com/courses/429591

There is no required textbook for this course, but purchasing the optional textbook (*Introduction to Modern Cryptography*, 3rd edition, Katz and Lindell) is strongly recommended. We will be following Chris Peikert's excellent lecture notes for this course, with modifications and additions. Extra resources include the following textbooks:

- Foundations of Cryptography, Vol. 1 and 2 by Oded Goldreich.
- A Course in Cryptography, by Rafael Pass and abhi shelat. Freely available here
- A Graduate Course in Applied Cryptography, by Dan Boneh and Victor Shoup. Draft available at https://toc.cryptobook.us/

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),
- EECS 498/598 (Encrypted Systems),
- Any Mathematics courses on discrete probability or number theory.

2 Course Policies

This class will be taught in person by default. Students are expected to attend class and participate in person. (Certain students have been given permission to attend the class remotely, due to extenuating circumstances.) Because of the ongoing COVID-19 pandemic, some adjustments have been made to course policies:

- Lectures and discussions will be recorded, and the recordings will be available on Canvas. The course staff will try to make the recordings available as quickly as possible. Attendance and participation is required, and will factor into the final grade. Please be courteous and abide by all campus policies regarding remote courses.[1]

[1] In particular: "Course lectures may be audio/video recorded and made available to other students in this course. As part of your participation in this course, you may be recorded. If you do not wish to be recorded, please contact the instructor the first week of class to discuss alternative arrangements," and "Students are prohibited from recording/distributing any class activity without written permission from the instructor, except as necessary as part of approved accommodations for students with disabilities. Any approved recordings may only be used for the student's own private use."

- PDFs of slides, including the instructor's markups, will be made available on the course Github and on Canvas.
- The course's "main" office hours will be in person. For students who cannot attend, either due to illness or visa-related time zone difficulties, some additional office hours may be available by appointment.
- For students, wearing a face covering over their mouth and nose during class is recommended. If you feel sick, do not come to class. Again: ***If you feel sick, do not come to class.***

These plans are subject to change on short notice.

2.1 Grading

Grades will be determined roughly as follows:

(50%) Homework assignments (6–7) and peer review, due approximately every two weeks, and class participation. Collaboration and external sources are allowed; see academic honesty policy for details. Regrade requests are due 1 week after assignment grades are released.

(25%) Take-home exam #1, October 4–11. *No collaboration or external sources are allowed.*

(25%) Take-home exam #2, November 29–December 6. *No collaboration or external sources are allowed.*

Some of the lectures in this course are not yet typeset. Students who wish to earn extra credit can write LaTeX scribe notes for these lectures. More points will be awarded for higher-quality notes. Inquire with the instructor for more information.

All submitted work will be graded on *correctness*, *clarity*, and *conciseness*, and **must** be typeset 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 your own solution, and list your collaborators/sources for each problem.
3. You may not submit a solution that you cannot explain orally.

4. Solutions from previous iterations of EECS 575 cannot be used as external sources.

Students must also abide by the College of Engineering's honor code. 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!

The most important course policy. The final, and undoubtedly most important, course policy is: *you must treat the course staff, other students, and yourself with respect and compassion.*

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. Authenticated encryption.
- **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.
- **Applications and special topics:** Secure messaging. Private information retrieval. Blockchains and cryptocurrencies. Lattice-based cryptography.

Special Dates

Note the following special dates:

- Days without class and/or OHs: September 5, October 17, November 23.
- October 3–10. Take-home exam #1 (Date still tentative.)
- November 28–December 5. Take-home exam #2 (Date still tentative.)