Course Syllabus
Introduction to Cryptology I
Math 173A, Summer Session I 2023
Online course

Instructor. Christopher Davis, daviscj@uci.edu

Teaching Assistants. Byron Osterweil, osterweb@uci.edu and Xu Zhuang, xzhuang8@uci.edu

Lecture. MWF 9:00-10:50am, Online. The lectures will be recorded and made available on the course website.

Discussion section. MWF 11:00-11:50am, Online

Office Hours. The instructor and TA will hold weekly office hours over Zoom. See our course website for details.

Class Website. `https://canvas.eee.uci.edu/courses/55830`

Prerequisites. Math 2B and Math 3A and Math 13.

Primary Textbook. Hoffstein, Pipher, and Silverman, *Introduction to Mathematical Cryptography*, second edition. Available free to download on campus (or using VPN) through SpringerLink. If you wish to purchase a physical copy, I recommend the (currently) $40 MyCopy Softcover version available through that same link.

About the class. Cryptology is the science of secret writing. The field has been around since at least the time of Julius Caesar, but in the 1970s it underwent a revolution. Now, two parties who have never met can transmit secret messages to each other, even if they can only communicate over insecure lines. The high point of this course is the explanation of how advanced mathematics enables this seemingly impossible feat.

Learning Outcomes 173A. The primary learning outcomes for Math 173A are that students will be able to:

- Identify whether a cryptosystem is a public key or a private key cryptosystem;
- Predict how a piece of ciphertext was encrypted using frequency analysis;
- Decrypt Vigenère ciphertext using frequency analysis;
- Implement a Diffie-Hellman key exchange, based on the discrete log problem;
- Implement the RSA public key cryptosystem, based on prime factorization;
- Find a solution to a discrete log problem using a collision algorithm;
- Determine whether two mathematical tasks are of comparable computational complexity;
- Assess whether a computation (especially involving prime numbers or modular arithmetic) is feasible with currently available software;
- Factor a product of large primes $N = pq$ when provided additional information (such as the value of $\phi(N) = (p-1)(q-1)$, or an "oracle" function that can compute square roots modulo N).

Weekly Schedule 173A. All sections refer to the course textbook by Hoffstein, Pipher, and Silverman.

- Week 1: Sections 1.1–1.5, 5.2, Lab 0 due Wednesday
- Week 2: Sections 2.1–2.4, Homework 1 due Monday, Online quiz 1 due Monday, Lab 1 due Wednesday
- Week 3: Sections 2.5–2.7, Homework 2 due Monday, Online quiz 2 due Monday, Lab 2 due Wednesday
- Week 4: Sections 3.1–3.3, Homework 3 due Monday, Midterm during the beginning of class Monday, Lab 3 due Wednesday
- Week 5: Sections 3.4–3.6, Homework 4 due Monday, Online quiz 3 due Monday, Lab 4 due Wednesday
- Week 6: Homework 5 due Monday, Online quiz 4 due Monday, Lab 5 due Wednesday, Final exam during the beginning of class Wednesday

Grade breakdown. The final grade will be calculated using the following weights:

- 20% Homework
- 20% Labs
- 20% Quizzes
- 20% Midterm
- 20% Final

The class will not be curved in a traditional sense. However, if one of the quizzes or exams proves to be more difficult than anticipated, the scores may be adjusted upwards. A total course grade of 93-100 will correspond to A, 90-93 will be A-, 87-90 will be B+, ..., 60-63 will be D-, and 0-59 will be F. A grade of A+ will be given only in extreme circumstances.

Homework. There will be weekly homework due by the end of the day on Mondays. You are encouraged to work together, but your written submission should be in your own words. Your lowest of the 5 homework scores will be dropped.

Labs. There will be weekly labs due by the end of the day on Wednesdays. These labs will primarily be completed on the website Deepnote. You are allowed to work in a group of up to 3 students on the labs, but each student should submit the file on Canvas. (It is fine for the groupmates to all submit the same file.) Your lowest of the 5 lab scores will be dropped.

Quizzes. There will be online Canvas quizzes due by the end of the day on Mondays. The quiz content will be based on the homework that is due that week. You are allowed to use internet resources and the textbook during these quizzes, but you should not discuss the problems with your classmates. We will not drop a quiz score, there will be at least two opportunities during the class to earn a "bonus point" on the quiz section. (So you can get 100% on the quiz portion of the class without getting every quiz question correct.)

Midterm. The midterm will be at the beginning of class on Monday, July 17th. It will be based on the first three weeks of class. The exam will be synchronous, with Zoom proctoring followed by pdf upload.

Final. There will be a one-hour Final exam at the beginning of class on Wednesday, August 2nd. The exam will be synchronous, with Zoom proctoring followed by pdf upload.

Makeup exams. In general, no makeup exams will be available. If you must miss an exam due to a verifiable reason, let the instructor know as soon as possible, preferably before the exam begins. Time zone inconvenience or travel plans are not acceptable reasons for missing the test. The reason we are holding the exams at the beginning of class, and the reason we are only having a one-hour final exam, is to attempt to minimize the time-zone inconvenience.

Waitlist. Students on the waitlist are expected to complete assignments by the same deadlines as the officially enrolled students. You should automatically have full access to the Canvas page if you are on the waitlist; let the instructor know if you do not.

Online learning. Taking a course online requires more self-discipline than taking a course in-person. Try your best to remove distractions while attending the lectures. The best way to keep your attention is to actively participate, whether out loud or through the Zoom chat.

If you find yourself confused by something (whether it is something mathematical or some logistic aspect of the course), please ask for clarification on Ed Discussion, so that other students can also benefit from the question.

Class meetings. Class meetings will be synchronous over Zoom. The lectures will be recorded and the recordings will be available on the course website.

Hardware requirements. The midterm and the final exam will be taken at the beginning of the scheduled classtime, and will be proctored over Zoom. Therefore it is required to be able to connect to Zoom using a webcam during these assessments. After the exam is over, you will upload a pdf of your answers. One app that can be used to produce this pdf is the free app CamScanner.

Announcements. Announcements to the class will be sent either using the class mail list or using Canvas messages. It is your responsibility to check these announcements regularly.

Ed Discussion. Ed Discussion is an online question-and-answer forum. Ed Discussion can be used for asking for clarification on material, getting help with homework, checking logistical details about the class, finding classmates to work with. It should not be used for requesting extensions, requesting changes to the course, etc. For those sorts of accommodations, please contact the instructor directly.

Support from the Disability Services Center. University of California, Irvine is committed to providing a barrier free environment for persons with documented disabilities. If you have any questions about accommodations, please contact the Disability Services Center at 949-824-7494 or register online at https://dsc.uci.edu/.

Academic integrity. Following the UCI academic integrity policy is a requirement to pass this class. Please see this website for more information on that policy: `https://aisc.uci.edu/`. The homework assignments can be worked on collaboratively, but the quizzes, the midterm, and the final exam must be taken individually. There will be no tolerance for sharing answers with classmates or submitting work that is not your own (for example, submitting an answer to an alternate version of the question).