CAS CS 538: Fundamentals of Cryptography
Spring 2022

Prerequisites

CAS CS 131 and 237 and CS 357 (formerly 391 G1 "Introduction to Information Security") or permission of instructor.

First, I will be assuming you have a basic knowledge of information security topics: definitions of encryption (symmetric and public-key) and its security (under CPA and CCA attacks), authentication (message authentication codes, digital signatures), hash functions, and key exchange. These topics are taught in CS 357.

Second, I will be assuming that you are comfortable reading and writing mathematical proofs. Every problem set will ask you to do so. We are not going to be writing code in this class; we will be writing proofs instead. Proof writing is taught in CS 131 and follow-up courses.

Third, I will be assuming a reasonable comfort level with probability theory, although if you are really comfortable with mathematical proofs and didn't have a whole course on probability, you will likely be able to catch up on the probability. But at the very least you should know what a sample space is, what conditional probability is, what random variables are, and what independence means both formally and intuitively. These topics are taught in CS 237.

Related Courses

You may wish to consider CAS CS 558 (offered in the Spring), ENG EC 521 (offered in the Fall), and CAS CS 501 B1 (offered in the Fall).

Textbook and Planned Content

The course will be based mostly on material from Boneh and Shoup's draft textbook "A Graduate Course in Applied Cryptography", available for free at `http://toc.cryptobook.us`. We will expect you to do a good deal of independent reading from this book; the lecture will aim to highlight the important points and explain the subtle ones. We suggest downloading the book and using it locally rather than accessing it online, as the file is big and navigating it in your web browser is a lot less pleasant than using a good pdf reader.

The primary focus of this course will be on *definitions*, *constructions*, and *proofs of security* of various cryptographic objects, such as encryption schemes, digital signature schemes, secret sharing, multiparty computation, zero-knowledge proofs, etc. We will try to understand what security properties are desirable in such objects, how to properly define these properties, and how to design objects that satisfy them.

Once we establish a good definition for a particular object, the emphasis will be on constructing examples that *provably* satisfy the definition. Thus, a main prerequisite of this course is mathematical maturity and a certain comfort level with proofs. I will be doing proofs in class, and you will be doing them on the problem sets.

At the end of this course, you should be able to make sense of a good portion of current cryptography research papers and standards.

I expect to cover most of chapters 1–13 as well as selected topics from remaining chapters of the textbook.

Staff, Communication, Piazza, Office Hours

Instructor: Leo Reyzin. TA: Luowen Qian. Office hours: will be posted via a pinned Piazza post.

Homework Q&A, homework, class announcements, etc. will be handled via Piazza `https://piazza.com/bu/spring2022/cascs538`. If you haven't yet, please sign up with Piazza ASAP with an email address that you actually check, so that you don't miss announcements ("I didn't get see the announcement" is not an acceptable excuse). Piazza is also the place to post HW questions. Answer your fellow students' questions!

Please do not send course staff individual email: class-related but nonpublic questions should go to private posts on Piazza rather than to email. Please keep questions public unless they pertain specifically to your situation in the class.

Lectures

Lectures, taught by Leo Reyzin, are in CAS (725 Commonwealth Ave) room B12, Tuesdays and Thursdays 12:30–1:45. There will be lecture material not covered in the textbook. Make every effort to attend unless, of course, you are contagious. We will try to make lecture recordings available if you are out sick, but the quality may not be very high, given the equipment available in the room.

Discussions

Discussions, taught by Luowen Qian, are Wednesdays at 9:05–9:55, 10:10–11, and 11:15–12:05. Their main purpose is to help you understand the course material and do the homework. Please try to attend the discussion to which you are assigned; if you cannot, you may attend another one subject to seat availability (students actually registered have priority).

Homework (60%)

Problem sets will be roughly weekly, due usually (but not always) on Monday nights, worth 60% of your grade. We will collect problem sets via gradescope; your submission must be in pdf format. We recommend typing them up (ideally, using LaTeX) or handwriting them and scanning to pdf (your phone can probably do that, either natively or with one of several available apps; gradescope has instructions at `https://help.gradescope.com/article/0chl25eed3-student-scan-mobile-device`).

Late assignments will not ordinarily be accepted, because we will endeavor to post solution as fast as possible. If we grant an extension to one person, we have to delay revealing solutions for everyone else, which inhibits learning. Thus, you will have to manage your own time well. Please budget time for unexpected minor emergencies, such as computer crashes, colds, quarantines, and noisy roommates. Please **never** organize your work in such a way that a single computer failure will set you back. Use cloud services with automatic saving/backup.

We understand, however, that sometimes circumstances are beyond your control. For just such an occasion, we will replace your lowest homework grade with your final exam grade if it is higher. Do not use the dropped grade option without a good reason—if you use it up early and then get a cold later in the semester, it's too late. Exceptions to this policy will be granted only in serious circumstances (such as hospital stays or family emergencies) that I hope none of you will have.

Exams (40%)

There will be a midterm (15% of the grade), Thursday March 17 in class, and a final exam (25%), **tenatively** scheduled for Thursday May 12, 12–2 (the registrar will publish the definitive final exam schedule during the semester).

Final Grade

Grading will be on a curve. Thus, individual grades on problem sets and exams do not correspond to the usual US high school letter grades. To come up with letter grades, we will add up all the points you earned with the appropriate weights, plot them, and then decide where the letter grades fall. The average in the class usually ends up being around 3.2 (high B or low B+).

Dropping the Class

If you are unsure of your performance in the class, please talk to us. Remember that the last day to drop a class without a 'W' is Thursday, February 24. The last day to drop a class with a 'W' is Friday, April 1. After that, you must receive a real grade for the course. Please talk to us if you are considering dropping the class—quite often students drop for the wrong reasons.

Collaboration Policy

Collaboration policy for this class is as follows.

- You are encouraged to collaborate with one another in studying the notes and lecture material.
- As long as it satisfies the following conditions, collaboration on the homework assignments is permitted and will not reduce your grade:
    1. Before discussing each homework problem with anyone else, you must give it an honest half-hour of serious thought.
    2. You must write up your solutions completely on your own, without looking at other people's write-ups.
    3. In your solution to each problem, you must write the names of those with whom you discussed it.
    4. You may not consult solution manuals, other people's solutions from similar courses or prior years of this course, etc. You may not work with people outside this class (but come and talk to us if you have a tutor) or get someone else to do it for you.
- You are not permitted to collaborate on the midterm and the final exam.

The last point is particularly important: if you don't make an honest effort on the homework but always get ideas from others, your exam scores will reflect it.

Violations of Collaboration Policy

Violations of collaboration policy fall into two categories: ones that are *acknowledged* in your write-up and ones that are *unacknowledged*.

Acknowledged violations (e.g., reading someone else's solution before writing your own and saying so in your own solution) will result in an appropriate reduction in the grade, but will not be considered cheating.

Unacknowledged violations of the collaboration policy—for example, not stating the names of your collaborators, or any other attempt to represent the work of another as your own—will result in **a lower final grade for the course—at least by an entire letter grade, but, depending on the severity, all the way to F**—and will be reported to the Academic Conduct Committee (ACC). I will assume that you understand the BU Academic Conduct Code; read it if you haven't.

If you are uncertain as to whether a particular kind of interaction with someone else constitutes illegal collaboration or academic dishonesty, please ask me *before* taking any action that might violate the rules; if you can't reach me in time, then at the very least include a clear explanation of what happened in your homework write-up to avoid being treated as a cheater. Citing your sources is usually the easiest way out of trouble.