CAS CS 538: Fundamentals of Cryptography

Spring 2021

1 Administrative Stuff

Official Description (slightly out of date)

Basic algorithms to guarantee confidentiality and authenticity of data. Definitions and proofs of security for practical constructions. Topics include perfectly secure encryption, pseudorandom generators, RSA and ElGamal encryption, Diffie-Hellman key agreement, RSA signatures, secret sharing, block and stream ciphers.

Prerequisites

CAS CS 131 and 237 and CS 391 G1 ("Introduction to Information Security") or permission of instructor. The course will require a good comfort level with mathematical proofs and elementary probability theory. Most of the homework assignments will ask you to write proofs. The course will assume that are you familiar with cryptographic concepts taught in CS 391 G1 (such as CPA and CCA security of symmetric and public-key encryption; stream ciphers and block ciphers; MACs and digital signatures; hash functions), even though we will explore them in more depth.

Staff, Communication, Piazza, Office Hours

Instructor: Leo Reyzin. TA: Pratik Sarkar. Office hours: will be posted via a pinned Piazza post together with zoom links.

Homework Q&A, homework, class announcements, etc. will be handled via Piazza `https://piazza.com/bu/spring2021/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!

Do not use anonymous posts on Piazza unless there is some very good reason to do so. You need to get to know your classmates, and it's hard to do so when no one knows your name.

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 228, Tuesdays and Thursdays 9:30–10:45am. If you can attend in person, please do. Use the InClassLfA app to reserve a seat. If you attend remotely, you will find Zoom links on Piazza and on Blackboard.

Lecture will be recorded, but recordings do not substitute for the interactive nature of a live class (in person or via Zoom). To help you succeed in the class, please make every effort to attend either in person or online.

Per university policy, students may not share lecture recordings with anyone not registered in the course and may not repost them in a public platform.

We will make an effort to set up Zoom to record in such a way as not to capture students' video feeds. However, Zoom is not always easy to operate and the recording options are somewhat limited, and so we may occasionally record your video without meaning to. Students have the right to opt-out of being part of the lecture recording. Please contact us (via a private post on Piazza) to discuss options for participating in the course while opting out of the class recording.

Discussions

Discussions, taught Pratik Sarkar, are Wednesdays at 9:05-9:55am, 10:10-11am, and 11:15am-12:05pm, online only. You will find Zoom links on Piazza and on Blackboard. They will not be recorded. Their main purpose is to help you understand the course material and do the homework, so please make every effort to attend. Please try to attend the discussion to which you are assigned; if you cannot, please attend another one.

Cameras On!

Zoom links for lectures and discussions will be posted on Blackboard and Piazza. We expect you to keep your camera on. We like to see your faces! We understand that not everyone has a perfect background or a distraction-free environment, and we do not judge. Bring along the pets, messy rooms, unmade beds, yesterday's dishes, roommates, younger siblings, children, and potentially embarrassing parents. We all have them! Use a zoom background if you would like. If you would really like to keep your camera off, please contact us (via a private post on Piazza) to explain your need.

No Recordings by Students (and How to Request an Exception)

No student may record any classroom or other academic activity in this class. If you have (or think you may have) a disability such that you need to record classroom activities, or need other assistive services, you should contact Disability & Access Services (`https://www.bu.edu/disability/accommodations/`) to request an appropriate accommodation.

Textbook

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.

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 using LaTeX or handwriting them and scanning to pdf (your phone can probably do that, either natively or with one of several available apps).

Late assignments will not ordinarily be accepted, because we will endeavor to post solution as fast as possible. You have to manage your own time well. Please budget time for unexpected minor emergencies, such as computer crashes, colds, 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 drop the lowest homework grade, and then average your remaining homework grades. 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), March 16 in class, and a final exam (25%), Wednesday May 5, 9–11am. The exams will be in real-time, via zoom, with cameras on for proctoring.

Final Grade

Grading will be on a curve. This, 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 Monday, March 1. The last day to drop a class with a 'W' is Friday, April 2. 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.

2 Contents

What this course is about

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. There will be little to no code writing in this class.

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

What this course is *not* about: Alternatives to consider

This course will not teach you how to make your computer secure. Cryptography is only one tool in computer security. The rest of computer security has to deal with such fascinating things as buggy code, poorly managed and ever-too-curious humans, backward compatibility, network protocols, sound emissions from your CPU, privilege escalation, hardware attacks, etc. We will mostly abstract all that away. I will, however, try to point out where the limitations of our models are and what else is needed for actual security.

This course will also not teach you how to implement the techniques we discuss in the most efficient manner. We will, generally, stop at cryptographic algorithms. The underlying number-theoretic algorithms will be discussed only briefly; the most advanced and efficient ones require more time to learn than we will have. For example, if you take only this class, you should be able to program RSA, but many existing implementations will probably be much more efficient that yours.

Finally, this course will not teach you how to design the next great block cipher, such as AES/Rijndael, or the next cryptographic hash function, such as SHA-3/Keccak. Nor will this course teach you how to "break" such designs.

Just because I will not teach these topics does not mean they are not worth your while. There are plenty of books and research papers to read and people to talk to if you are interested in pursuing any of these topics. In addition to our prerequisite CS 391 G1 ("Introduction to Information Security"), which I assume you have taken, you should also consider taking CS 558 ("Network Security") and CS 568 ("Applied Cryptography").