Introduction to Cryptography

Instructor: Rohit Musti, *Current Semester:* Spring 2022

Course Goal

My goal is to provide you (the student) with a working understanding of cryptographic primitives and the confidence to pursue further study or real world application of your knowledge (including, but not limited to, boring your loved ones with enthusiastic descriptions of obscure cryptographic constructions over the dinner table).

Course resources

- Text Book: this is written by Dan Boneh at Stanford. We will not be following it too closely, but it is an excellent resource for reading and learning more about cryptography.
- Anonymous feedback form. I do not collect any data on this form besides any anonymous feedback you have for me. If you wish to contact me non-anonymously, you can use this form too and include your email.
- Course Slack. Please contact instructor directly for information on how to join the slack.
- To contact the instructor directly, please email rohit.musti@hunter.cuny.edu

Course Schedule

Date	Lecture Topic	Notes
February 2, 2022	Course Introduction and History of Cryptography	Lecture 1 Video
February 9, 2022	Semantic Security Stream Ciphers	Lecture 2 Video, HW 0 Assigned: Due February 16, 2022 by the start of class.
February 16, 2022	Semantic Security Review Stream Ciphers Review Block Ciphers	Lecture 3 Video
February 23, 2022	Message Integrity Authenticated Encryption	Lecture 4 Video, HW 1 assigned and is due March 11, 2022 at 5:00 pm EST via Blackboard.
March 2, 2022	Symmetric Key Cryptography Review Public Key Cryptography Introduction (lite)	

March 9, 2022	Public Key Primitives	Lecture 6 video
March 16, 2022	Public Key Encryption	Out Sick
March 23, 2022	Digital Signatures	Lecture 7 video
March 30, 2022	The Block Chain, bitcoin paper,	Lecture 8 video HW 2 assigned and is due April 8, 2022 at 5:00 pm EST via Blackboard.
April 6, 2022	Zero Knowledge Proofs	Lecture 9 Video
April 13, 2022	Multi-Party Computation	Lecture 10 Video HW 3 Assigned, Due April 29 at 5:00 PM
April 20, 2022	*Spring Recess*	
April 27, 2022	delayed	delayed - wifi outage
May 4, 2022	Login Systems	Lecture 11 Video
May 11, 2022	Encrypted Computation	
May 18, 2022	*Final Exam* (date/time not official yet)	

Course Policies

- These policies are subject to change at my discretion as the instructor. However, I will announce all changes and will do my best to avoid making significant changes.
- Course Contract: I, as the instructor, agree to provide you with the resources you need to succeed in this class and you as the student will do your best to succeed. By offering this class, I agree to this contract and by taking the class you agree to this contract and agree to adhere to all course policies.
- Course Honor Code: *I will not lie, cheat, or steal*. I understand that, at times, this class may feel stressful. If you are feeling overwhelmed and concerned about your ability to achieve the grade you are aiming for in this class, please do not hesitate to reach out to me directly and we can work out a plan together.
- *Course Errors:* If you find a mistake in any course materials (including this site, lectures, or assigned homework), I will give you up to a 5% bump on an assignment of your choice. This is a first come first serve policy (i.e. only the first student to spot and report a error will receive the credit). I will award an extra 2% to any student who makes a PR with the fix that is successfully merged into the class.
- *Office Hours:* Because of my schedule, I will not be able to hold weekly office hours at a regularly scheduled time. If

you would like to speak with me directly, please reach out over email and we will find a time that works for both of us. I am hoping to meet all of you over the course of the semester so I can learn more about the experiences you bring to this course and what you are hoping to get out of it. To incentivize this, I will give anyone who meets with me during office hours, an additional 5/5 assignment points. You can also schedule office hours for any topic you wish, even beyond this class, including advice on working as a software/data engineer.
- *Recording Lectures:* Please do not record my lectures. I understand during this zoom era that you may want to screen record the lectures. I hope you recognize that it is uncomfortable to be recorded on video. If you need an accommodation/exception to this policy, just let me know and we'll get that squared away.
- *Special Accommodation:* This class will be digital, but if you need any accommodations to make this course accessible, please do not hesitate to reach out.

Homework/Grading Policies

- *Course Grade Structure:* There are two possible structures for your grade in this class and the choice is yours! Option 1: 100% of your grade is exclusively the sum of the total points you earn on homework assignments divided by the total number of possible points. Option 2: 75% of your grade is the sum of the total points you earn on homework assignments divided by the total possible points and the remaining 25% is your score on the optional final exam. I am building in this flexibility so that students who find the pressure of exams overwhelming do not need to put themselves through it and students who find homework annoying have another mechanism to demonstrate their knowledge!

- *Late Homework:* You are allowed 5 late days throughout the semester. You can apply up to 3 late days to a given homework assignment. These late days cannot be split (i.e. 12 hours on one and 12 hours on another). If you are not able to submit an assignment on time, please speak with me directly.
- *Dropped Assignment:* You are allowed to drop a homework assignment of your choosing from your overall grade calculation. There may be an assignment that I do not allow any one to drop; I will make it clear when I assign an assignment that is "undroppable".
- *Extra Credit:* Extra credit assignments. If you feel that your grade isn't as high as you are hoping it is and you want the opportunity to submit an extra credit assignment, please reach out to me directly. We will discuss which part of the class you find most interesting and design an assignment based on it. I will then make that extra credit assignment available to all of the

students in the class.

Teaching Philosophy and Inspiration

I have been lucky in that, thanks to several amazing teachers, I have felt comfortable in the classroom and was often that student raising their hand asking a million questions. When I transitioned to the teaching side of the classroom, I discovered that I loved answering those questions and soon became addicted to helping students. I hope to foster a community of learners in our digital classroom, where students feel comfortable asking quesitons, challenging me to offer a clearer explanation, and respecting one another. I don't believe in a heavy divide between teacher and student in the classroom. Rather, I see it as my responsibility to guide us through the content and I hope to empower each of you to take an active role in your education. I hope throughout this class you take time to stop and deeply explore ideas you find interesting and compelling. If you are interested in some of the pedagogy behind the classroom, check out *Teaching to Transgress* by bell hooks.