Introduction to Cryptography **Caltech CS152, Fall 2022**

Thomas Vidick, vidick@caltech.edu

Course Organization **Tuesday September 28th, 2022**

The goal of this course is to teach you modern techniques in cryptographic design and analysis, as well as to initiate you to the "cryptographer's mindset". With this goal in mind, you are encouraged to adopt a critical mindset throughout the class, and question any definition that I bring forward. My goal is for each of you to reach the point where you are able to introduce, critically assess, and implement, your own security definitions. Evaluation in the course is based on a variety of assignment types (detailed below) that are designed to make you reflect on the material at all levels, from coding to math-based proofs to critical reading to a final project, all with an emphasis on mathematical rigor. If you are confused by course expectations or grading guidelines you should feel free to raise any questions with the instructor.

Indicative syllabus: See the course webpage http://users.cms.caltech.edu/~vidick/teaching/cs152_Fall22.html for up-to-date information.
Week 1: Introduction, computational security. Pseudorandom generators. Week 2: Pseudorandom functions, one-way functions. Week 3: Encryption and authentication. Week 4: Public-key encryption, digital signatures. Week 5: Lattice-based cryptography. Homomorphic encryption. Week 6: Hash functions. Week 7: Blockchain. Week 8: Interactive proofs. Zero-knowledge. Week 9: Quantum cryptography.

Prerequisites: Ma 1b. CS 21, CS 38 or equivalent recommended.

Resources: The course textbook is "Introduction to modern cryptography" (second edition), by Katz and Lindell. In addition, I will assign readings from resources available online, including draft textbooks by Boneh and Shoup and Barak (links available on the course webpage).

Office hours and recitation: You are strongly encouraged to come to my office hours or to those held by the TAs. My office hours are Tuesdays 5:30-6:30pm in my office, 207 ANB. You can come to office hours to discuss assignments, but not only for that. You can come to discuss anything related to the course: the material covered in class, the material not covered in class, your interest in the class, etc. You are also welcome to come in for advice on how to do well in the class.

Communication: Course communication will be made in class and through Piazza.

Course TAs: The TAs are Hanna Chen and Junxuan (Helen) Shen. Their office hours are Thursdays 5-6pm in 205 ANB

Assignments and evaluation: Each student is required to complete the following:

- Pre-class quizzes: 10% of grade. Before each class you will have to answer a simple multiple-choice question to test your understanding of the previous class's material. There will be 16 such quizzes, and you are allowed to skip 4 of them while still receiving full grade. The goal of the quizzes is to make sure every student is following the class, and that no one falls behind.
- Three take-home assignments: 40% of grade. These will be due bi-weekly, to be handed by Friday 5pm, with the first assignment due Friday 10/08. Assignment consists of 4-6 exercises each, whose solution is to be handed in on paper (handwritten or latexed solutions are equally good). Grading will take into account clarity and rigor of exposition: make sure your solutions are presented appropriately and include complete proofs whenever required.
- Three reading assignments: 15% of grade. These will be handed out bi-weekly (in alternation with the problem sets). Each assignment will require you to read one or two simple papers with historical

significance in the field of cryptography, and turn in one or two pages of reflections on the paper (you will be given guiding questions). The goal of these assignments is to encourage you to take a historical perspective and reflect on deeper questions that go beyond the math. The goal is not to test or trick you, and grading will be generous. I hope you enjoy the readings!

- Three programming assignments: 10% of grade. These assignments will be taken from the challenges at `http://cryptopals.com/`. The goal of the assignments is to introduce you to the complexities and risks of actual implementation of simple cryptosystems. They can be solved using any language of your choice (with python being a convenient option).
- Final exam: 25% of grade. The final will be similar to a take-home assignment, possibly slightly longer (not more than 50% extra work). It will contain problems on all the material covered in class. In addition, it may include one or two more open-ended questions of a similar flavor to the reading assignment questions. These questions will be assigned a numerical point value lower than the problem questions.

Collaboration policy:

- The quizzes and reading assignments should be completed on your own: no collaboration. We will discuss those in class, and you are welcome to bring any questions you have there.
- The problem sets can be solved in collaboration with other students in the class (and I encourage it). But you should read and think about each problem alone for at least a few minutes before collaborating. *You must produce the final write-up for submission alone, without relying on notes of any kind from your discussions; your solution must depend solely on your own understanding.* Questions about homework problems are welcome on Piazza and in Office Hours, as long as they don't reveal parts of a solution. There is a 24h pre-deadline moratorium on questions on Piazza; please make sure to respect this.
- The programming assignments can be discussed in groups as long as no computer (or printed, or even hand-written, code) is present. In addition you are encouraged to work through them in pairs, and may turn in the same code for both members of the pair. However, different pairs may not directly exchange code and are subject to the "50-foot rule" from CS11.
- The final exam is strictly no collaboration. You are allowed to use all materials given in class (including solutions to homework exercises), but no more.

In all cases where collaboration is allowed, you should indicate on your solution the name of your collaborator(s).

Sources: It is ok to look up definitions online or wherever you find convenient. It is not ok to use solutions found online, in whole or in part. If by accident you find a solution to an assigned problem, or a problem that is close to an assigned problem, you should immediately put it aside. **Do not violate the honor code**. In case of uncertainty **ask.**