Course overview and additional reading resources | Coursera

Course Overview

Cryptography is an indispensable tool for protecting information in computer systems. This course explains the inner workings of cryptographic primitives and how to correctly use them. Participants will learn how to reason about the security of cryptographic constructions and how to apply this knowledge to real-world applications. The course begins with a detailed discussion of how two parties who have a shared secret key can communicate securely when a powerful adversary eavesdrops and tampers with traffic. We will examine many deployed protocols and analyze mistakes in existing systems. The second half of the course discusses public-key techniques that let two parties generate a shared secret key. We will cover the relevant number theory and discuss public-key encryption and basic key exchange. Throughout the course participants will be exposed to many exciting open problems in the field and work on fun (optional) programming projects. In a second course (Crypto II) we will cover more advanced cryptographic tasks such as zero-knowledge, privacy mechanisms, and other forms of encryption.

Homework and Grading

- There will be a weekly problem set that includes an optional programming component. Participants are expected to solve these assignments on their own, but can discuss clarification questions on the course forum.
- Participants can attempt each of the problem sets four times. After each submission the system will provide explanations about correct and incorrect anwers. When participants attempt to solve the problem set again, many of the questions will be different.
- The programming assignments are optional. Participants are free to use any language of their choice to solve the programming assignments. Our sample code will be given in Python although that code is not required to complete these optional assignments.

- A passing grade be given to participants who obtain more than 70% of the maximum score on the problem sets and final exam. The programming assignments are optional.
- In-video quizzes are not graded and are only there to help participants with self assessment.
- Many of the modules contain links to research papers for further readings. These are intended for participants interested in learning more about the material covered. These further readings are optional.
- There will be a final exam (no midterm) that is similar in style to the problem sets, but covers the material of the entire course.

Links to free resources to supplement the lectures:

- Background on discrete probability: [html]
- A course in applied cryptography: [html]

- Computational number theory: [pdf]