Winter 2017 CS 485/585 - Introduction to Cryptography

About

- **Instructor**: Fang Song @ FAB 120-07. Email: fsong“AT”pdx.edu.
- **Lectures**: Tu/Th 2:00 - 3:50 pm @ Fourth Ave Building 47.
- **Office hours**: Tuesday/Wednesday 4:00 - 5:00pm, or by appointment.
- **Course webpage**: http://www.fangsong.info/teaching/w17_4585_icrypto/. Please check regularly for updates and announcements.
- A **resource page** http://www.fangsong.info/teaching/w17_4585_icrypto/resource/ with useful materials related to the course.

Course Description

Cryptography is usually described as the *art* of secret writing. The revolution of *modern* cryptography, however, has been transforming cryptography into a science based on a mathematically rigorous framework. Beyong the significance in protecting information in our society, modern cryptography is also full of intellectual and mathematical beauty. This course will explore the key concepts in modern cryptography, including private-key cryptography such as perfect secrecy, block ciphers, crytographic hash functions and message authentication, as well as public-key cryptography such as public-key encryption and digital signatures. We will also touch some exciting advanced topics such as secure computation, fully homomorphic encryption, and the threats and opportunities that the new paradigm of quantum computing brings in cryptography. We will take a conceptual and theoretical approach: the focus is on the *ideas* rather than *implementations*, and on how to define and reason about security of cryptographic constructions in a mathematically sound manner. The ultimate goal will be to build a cryptographic way of thinking.

Text

- (Required) Introduction to Modern Cryptography (2nd edition) by Jonathan Katz and Yehuda Lindell. Chapman and Hall/CRC Press, Nov 2014. Katz is maintaining a webpage with errta and other updates about the book.
- We will refer to Boneh and Shoup’s onging book occasionally: A Graduate Course on Applied Cryptography.
- For thoery-oriented students, Goldreich’s two volume text on theory of cryptography is the place to go: Foundations of Cryptography.

Prerequisites

CS 350 or equivalent. It is crucial that you are comfortable with (preferably enjoy) reading and writing mathematical proofs. It’s helpful if you are familiar with (randomized) algorithms, basic probability theory and linear algebra. I will review some of the basics in class, but the terms “big-O notation, randome variables, expectation, matrices and eigenvalue” for example should not be totally alien to you. If you are uncertain about your background please don’t hesitate to talk with me. Programming skills are not required for this course.

Main topics

- Part I: **Overview**. History, dawn of modern cryptography, the idea of provable security, and Shannon’s perfect secrecy.
- Part II: (Modern) **Private-key** (aka *symmetric*) cryptography.
  - Computational security for encrytion, CPA & CCA, proof by reduction;

  - Pseudorandom generators and stream ciphers, psuedorandom permutations and block ciphers;
  - Data integrity, message authentication codes;
  - Hash functions, random oracle, applications;
  - Practical and theoretical constructions of private-key primitives.
- Part III: **Pubic-key** (aka *asymmetric*) cryptography.
  - Diffie-Hellman key exchange, and the public-key evolution;
  - Public-key encryption. Factoring and Discrete-log based PKE, trapdoor permutations, hybrid encryption;
  - Digital signature. DSA, hash-based signatures.
- Part IV: **Selected** topics. Zero-knowledge proofs, secure computation, fully homomorphic encryption, quantum computing and quantum-safe cryptography.

Policy

- **Grading Policy**: Homework 40% (10 each with lowest one dropped), Quizzes 20%, Participation 10%, Final exam 30%.
- **Homework**: You must turn in hard copies of your assignments before the lecture on the due date. The solutions must be intelligible. I encourage you to type your homework with Markdown or Latex (and submit the printouts). *Late homework* is acceptable, but there will be a penalty of 50% (<1 day), 80% (1-2 days), and 100%(>2 days). Out of the 5 homework assignments, the one with the lowest grade will be dropped in final grade. No exceptions.
- **Collaboration** in small group (3 people max.) on homework problems is *highly encouraged*. However, each person must write up their solutions independently. For each problem that you have collaborated with others, you must list the names of your collaborators.
- **Quiz and exam**: Quizzes are closed book. You are allowed to bring in two double-sided pages of notes for the final exam.
- **Academic integrity**: Students will be responsible for following the PSU Student Conduct Code.