Winter 2018 CS 485/585 - Introduction to Cryptography

About

- **Lectures**: Tu/Th 16:40 - 18:30 @ Fourth Ave Building 10.
- **Instructor**: Fang Song (fsong "AT" pdx.edu). **Office hours**: Tu/Th 10:30 - 11:30am, or by appointment @ FAB 120-07.
- **Teaching assistant**: Nate Launchbury (njl2 "AT" pdx.edu). **Office hours**: Monday 9:30 - 11:00am.
- **Course webpage**: http://www.fangsong.info/teaching/w18_4585_icrypto/. Please check regularly for updates and announcements.
- **Useful materials**: on RESOURCE page (http://www.fangsong.info/teaching/w18_4585_icrypto/resource/).

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 (http://www.cs.umd.edu/~jkatz/imc.html) 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 (https://crypto.stanford.edu/~dabo/cryptobook/). Current version 0.4 (posted Sep. 30, 2017).
- For thoery-oriented students, Goldreich's two-volume text on theory of cryptography is your destination: Foundations of Cryptography (http://www.wisdom.weizmann.ac.il/~oded/foc-book.html).

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.

Prerequisites

CS 350 or equivalent. It is crucial that you are comfortable with (preferably enjoy) reading and writing mathematical proofs. Basic probability theory is extremely important to succeed in this course. It's also helpful to familiarize yourself with design and analysis of (randomized) algorithms, and linear algebra. I will review some the basics in class, but the terms "big-O notation, random 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. lattice-based PKE, trapdoor permutations, hybrid encryption;
  - Digital signature. DSA, hash-based signatures.
- Part IV: **Selected** topics. Zero-knowledge proofs, fully homomorphic encryption, quantum-safe cryptography, etc.

Policy

- **Grading Policy**: Homework 40%, Quiz 20%, Final Exam 30%, Participation 10%.
- **Homework**: Start working on your homework early! The more iterations you go through a problem, the more likely you will get some idea of approaching it. Do not expect to finish it the night before due. You must turn in hard copies of your assignments before the lecture on the due date, and your written 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 30% (<1 day), 50% (1-2 days), 80% (2-3 days), and 100%(>3 days). Some problems are markded for Graduate students (registered in 585), which are required for graduate students, and counted as bonus points for undergraduate students.
- **Collaboration**: I highly encourage you form study groups (of 3 people maximum) as early as possible. You may discuss in groups on homework problems, however, everyone 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. In the final exam, You are allowed to bring in two pages (double-sided, letter-size) of notes.
- **Academic integrity**: Students will be responsible for following the PSU Student Conduct Code (http://www.pdx.edu/dos/codeofconduct).
- **Students with disabilities**: If you need academic accommodations, please register with the Disability Resource Center (https://www.pdx.edu/drc/) and notify the instructor immediately to arrange for support services.