CMSC 28400: Introduction to Cryptography, Autumn 2021

Instructor: David Cash, davidcash@uchicago.edu

Logistics

Website: https://people.cs.uchicago.edu/~davidcash/284-autumn-21/index.html

Discussion Q/A site: See link on Canvas. Invitations have been sent to students enrolled by Monday Sept 27.

Lectures: Tues/Thurs 12:30pm-1:50pm in Ryerson 251

David's office hours: Wednesdays 1:00pm-3:00pm on Zoom (link on Canvas)

Teaching assistants and office hours:

- Akshima akshima@uchicago.edu, Fridays 3:00pm-5:00pm, on Zoom (link on Canvas)
- Andrew Chu andrewcchu@uchicago.edu, Wednesdays 3:00pm-5:00pm, at JCL 354
- Alex Hoover alex8@uchicago.edu, Tuesdays 2:00pm-3:00pm, at JCL 257

Source books and notes. The main material for this course will be instructor notes. All additional material for this course will be either free online, or freely available as a pdf download via the University of Chicago library. The title of each source is a clickable link.

- Understanding cryptography: A textbook for students and practitioners by Christof Paar and Jan Pelzl
- Introduction to Modern Cryptography (course slides) by Mihir Bellare.
- A Graduate Course in Applied Cryptography by Dan Boneh and Victor Shoup
- Handbook of Applied Cryptography by Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone
- Cryptography Made Simple by Nigel Smart

Content and Prerequisites

This course is about cryptography from a theoretical and practical perspective. It will cover how cryptography works, how security is analyzed theoretically, and how cryptography is broken in practice. Topics will include classical cryptanalysis, symmetric-key encryption, block ciphers, message authentication codes, asymmetric encryption (RSA- and discrete-log-based), and digital signatures.

This course assumes familiarity with mathematical proofs and basic number theory and probability (at the level of CMSC 27100; refreshers will be distributed as needed) and programming (at the level of CMSC 15400). This course does not assume any prior knowledge of computer security, cryptography, or advance mathematical like group theory beyond what was covered in CMSC 27100.

The recommended programming language is Python, but submissions written in another language may be accepted with permission from the course staff.

Course Structure

Lecture. Lecture summaries and links to associated materials will be posted on Canvas and the course website.

Assignments. There will be two types of assignments: *Problem Sets* will be mostly theoretical, pen-and-paper assignments usually due on Thursdays at class. *Projects* will be involve problem solving via programming, and tend to be longer running (about two weeks). There will be three projects during the quarter. Some assignments will be team-based.

Exams. There will be one in-class exam, tentatively Week 6. The exact date will be determined in advance. The final exam will be cumulative and held at the time and place scheduled by the university.

Course grades. Final grades for the quarter will be a weighted average of assignments Problem Sets (35%), Projects (25%) Midterm (15%), and Final (25%).