

CS4830 - Introduction to Cryptography

Location : Gates Hall G01

Lecture Times : Mon, Wed and Fri. 1:25pm-2:15pm

--- HOME --- --- SYLLABUS --- --- RESOURCES ---

This syllabus is subject to update.

Week	Foundational Concepts	Interesting Application/Story-time	Homework
<u>8/26, 8/28</u>	Introduction to the course Introduction to encryption, one-time pad	Historical aspects Bonus project ideas	• Watch "The Imitation Game" (optional) • Think about/sign up for bonus projects, and project team formation (optional) • Break a Vigenère cipher and a substitution cipher Lab Instructions Released: see link • Required Reading: Section 1 of the textbook

8/31, 9/2, 9/4

Encryption, one-time pad, perfect secrecy

Coin flipping (various topics)

- Optional: Talk to Elaine about your intended bonus project direction. We will use a combination of office hours and part of class time on Friday for this (15 min per group). Elaine may assign you a grad-student mentor for your bonus project. Schedule a meeting with your grad-student mentor if you have one.

9/7 (labor day, no class), 9/9, 9/11

Computational Hardness and one-way functions

Private coin protocols (pepsi or coke?)

Zero-knowledge proofs

- [How to explain ZKP to your children](#) (optional)

- Required Textbook Reading: Chapter 2 (Computational Hardness); Chapter 4 (Zero-knowledge Proofs)
- Break a Vigenère cipher and a substitution cipher
- Lab Instructions Released: see [link](#)

9/14, 9/16, 9/18

One-way functions, basic number theory

Secret sharing

- [Lecture notes on secret sharing by Bill Gasarch](#)

- Required Textbook Reading: Chapter 2 (One-way functions); Section 6.1 Secret Sharing
- Implement secret sharing

9/21, 9/23, 9/25

Indistinguishability and Pseudorandomness

Wiki introduction to [Euler's Totient Function](#)

Secure dating, i.e., "he loves me, he loves me not"

- Required Textbook Reading: Chapter 2
- Implement secret sharing

Reading: Rafael Pass
and abhi shelat "A
course in
cryptography", page 9

Secure voting with a
PEZ machine

9/28, 9/30, 10/2

Encryption

- Optional reading

- Required Textbook Reading: Chapter 3
 - Written homework 1
- Released: see [link](#) ([.tex file link](#))

Cryptography pitfalls
Reading:

10/5, 10/7, 10/9

Encryption

- Implementation pitfalls
- An Empirical Study of Cryptographic Misuse in Android Applications
- Talk by Nate Lawson
- Talk by Steve Weis

- Written homework 1
- Released: see [link](#) ([.tex file link](#))

10/12 (fall break, no
class), 10/14, 10/16

Review

10/14 was a review session for the midterm. No
new material was covered.

Oblivious RAM
([slides link](#))

10/19, 10/21, 10/23

- Binary-tree ORAM
- Path ORAM

Oblivious RAM

- **Midterm (Monday 10/19 in class)**
- Implement Path ORAM

<u>10/26, 10/28, 10/30</u>	Public-key Encryption		- Implement Path ORAM - Required Reading: Textbook Section 3.10.0 (Public Key Encryption) - Optional Reading: Proof in Textbook Section 3.10.1
<u>11/2, 11/4, 11/6</u>	Public-key Encryption and Authentication Code		- Required Reading: 3.11 (El-Gamal Public Key Encryption Scheme) - Implement Path ORAM - Bonus mini-research project
<u>11/9, 11/11, 11/13</u>	Digital Signatures	Merkle-hash trees	- Implement Path ORAM - Slides deck: link
<u>11/16, 11/18</u> , 11/20 (recitation no scribe)	Consensus Protocol (Byzantine Agreement)	Garbled circuits	Written homework 2
11/23 (pre-thanksgiving, no class), 11/25 (thanksgiving, no class), 11/27 (thanksgiving, no class)	•	Thanksgiving	
<u>11/30, 12/2</u> ,	Bitcoin and Review	Bonus project	

12/4(recitation no
scribe)

- The rise and
rise of bitcoin

presentations

- Written homework 2

12/17 (Final)

- **Final (9:00AM 12/17 Gates Hall G01)**

Instructor and TAs

Instructor:

- Elaine Shi

Email: runting at gmail dot com . Please begin your subject line with "[cs4830]", otherwise your email may be filtered by my email filter.

Office Hours: Wed 5pm - 6pm

Office Location: 437 Gates Hall

TAs:

- Antonio Marcedone

Email: [MySurname]@cs.cornell.edu

Office Hours: Tue 5pm - 6pm

Office Location: G15 Gates Hall

- Zikai Alex Wen

Email: zw385 [at] cornell.edu
Office Hours: Fri 10.10-11.10
Office Location: G13 Gates Hall

[About](#) | [Sitemap](#)

[Log in](#)

You can do it, too! Like what you see? Go ahead, create your own free website. Just sign up on <http://www.jimdo.com> and get started!