CSE 5351: Introduction to Cryptography

Ten H. Lai
Spring 2018
TuTh 3:55-5:15 PM, Caldwell 171
Syllabus

• Instructor: Ten H. Lai (Steve)
• Office: DL 581
• Office hours: TuTh 11:30am-12:30pm
• Email: lai.1@osu.edu
• Home page: http://web.cse.ohio-state.edu/~lai

• Grader: Jiayuan Wang, wang.6195@osu.edu, Dreese 474, 2:30-3:30 pm
Textbook (Required)

• Jonathan Katz & Yehuda Lindell
  Introduction to Modern Cryptography
  Chapman & Hall/CRC, 2015
  Second edition
Grading plans and exam schedule

• Homework: 15% or 15%
• Midterm exam: 32% 42%
• Final exam: 33% 43%
• Attendance: 20% 0%

• Midterm: Thursday, March 8, class time
• Final exam: Monday Apr 30, 6:00pm-7:45pm
Class attendance

- Class attendance is essential for understanding the materials --- and you earn credit!
- Attendance will be taken at random times.
- If you have to miss a class for a legitimate reason, please email me in advance.
- Please be on time for class!
This course is about …

• Theory/principle and some practical constructions of various cryptographic primitives and protocols.
• Chapters 1-8 and 10-12, with many sections skipped
• Notes on cryptographic protocols
Topics (1)

• Introduction
  – Overview
  – Classical cryptography
  – Shannon’s perfectly-secret encryption

Classical crypto

Perfect Secrecy (1949)

Modern crypto
Topics (2)

• Private-key cryptography
  – Private-key encryption
  – Message authentication codes
  – Hash functions and applications (e.g. bitcoins)
  – Practical constructions
Topics (3)

• Public-key cryptography
  – Basic Number theory (mathematical background)
  – Public-key encryption
  – Digital signature schemes

• Some Basic cryptographic protocols
Prerequisites

• Stat 3460 or Stat 3470

• CSE 2331 or CSE 5331 or Math 4573 or Math 4580

• Some maturity in **mathematical reasoning**
Mathematics background

• Basic Probability (important for understanding the concepts; will not be reviewed)
• Modular arithmetic (will be reviewed/taught)