

---

# Introduction to Cryptography

**CSE 598A Fall 2007**

Adam Smith

Office hours: Mondays 3-5pm

Office: IST 338K

Phone: x3-0076

# What this course is about

---

- Cryptography
  - The science of communicating and computing in the presence of an adversary
- Basic:
  - encryption,
  - authentication,
  - signatures
- Interactive protocols:
  - identification,
  - playing poker over the telephone (how do you shuffle and deal?),
  - distributing computation among mutually distrusting parties

# Focus: mathematical rigor

---

- Precise **definitions, assumptions, proofs** of security
  - Conceptual toolkit for approaching nebulously defined problems
- Specific **constructions** used in practice
  - Things you've heard of: RSA encryption, Diffie-Hellman, AES
  - Things you may not have: Fiat-Shamir signatures, zero-knowledge proofs for NP, Feistel networks
- **Foundations**
  - Relations between different assumptions
  - Provably secure constructions
  - Cryptanalysis: basic attacks and design principles

This is a theory course

- you have to read and write proofs
- solve problems
- mostly board lectures

# What this course is **not** about

---

- Computer security
  - Crypto is one (important) aspect of security
  - CSE 543 is a broader survey of security
- Hacking
  - But the material will make you a better hacker
- Details of practical implementations
  - You will acquire the tools to understand and design implementations of cryptographic schemes
  - Learn to think critically about crypto

# Course Info

---

- Prerequisites
  - **Discrete math** (e.g. CSE 260, Math 311)
  - **Probability** (e.g. STAT 418)
  - Algorithms (e.g. CSE 465, 565)
- Related courses offered this semester at Penn State
  - Security (CSE 543)
  - Factoring and primality (MATH 467)
  - Information Theory (EE 561)
  - Quantum computing
  - Distributed computing
  - Data privacy (joint with stat's)
  - **Theory seminar** (CSE 597x): Tuesdays 11am -12:30pm

# Evaluation

---

- Homework 60%
- In-class Quizzes 40%
- Homework policy:
  - Collaboration **ok**, copying **NOT OK**
  - partial credit hard to get
    - 15% rule
  - randomized grading (law of large numbers)
  - Extra credit problems
  - Online questions and reading checks
  - Please type your solutions (no mercy for bad handwriting)

# Lectures

---

- Tuesdays & Thursdays, 4:15-5:30pm, IST 333
- Exceptions:
  - September 6: no lecture. Substitute in evening Sep. 4 or 18?
  - October 9 and November 6: room change (TBD)
  - Oct 18 and 23: guest lectures (TBD)
- Auditors
  - Send me your Penn State email i.d. so that I can add you to the Angel mailing list for the class.

# Textbook

---

- Jonathan Katz and Yehuda Lindell.  
*Introduction to Modern Cryptography*.  
CRC Press, 2007.
- Not yet at bookstore
  - I have 15 copies of the first two chapters + appendices
    - Please share!
  - Chapter 1 is available online
- When we follow the book (75% of class) I expect you to **read** assigned chapters and **prepare questions**

# Homework

---

- Complete background survey on Angel
- Read KL Chapters 1, 2

---

Questions?

# Today: Encryption

---

- Historical ciphers
- Perfect secrecy
  - One-time pad
- Limitations of perfect secrecy