

---

# Introduction to Cryptography

**CSE 546 Spring 2009**

Adam Smith

Office hours: After class, 4-5pm, Tue/Thu.

Office: IST 338K

Phone: x3-0076

[asmith@cse.psu.edu](mailto:asmith@cse.psu.edu)

# Lecture I

---

# What this course is about

---

- Cryptography
  - The science of communicating and computing in the presence of an adversary
- Securing basic communication channels:
  - encryption,
  - authentication,
  - signatures
- Interactive protocols:
  - identification,
  - playing poker over the telephone
  - 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)
  - **Computability** (e.g. CSE 464/468)
  - Algorithms (e.g. CSE 465, 565)
- Related courses offered this semester at Penn State
  - Security (CSE 443/543)
  - Factoring and primality (MATH 467)
  - Information Theory (EE 561 / IST 597)
  - **Theory seminar** (CSE 597x): Tuesdays 11am -12:30pm
  - Number theory / algebra classes in math

# Topics you should be familiar with

---

- Probability
  - Probability distributions, random variables
  - Expectation
  - Counting permutations and combinations
- Algorithms / complexity
  - Asymptotic notation (big-oh)
  - NP
  - NP-completeness
  - Reductions between problems
- Reading/writing proofs

# Lectures

---

- Tuesdays & Thursdays, 2:30-3:45pm, IST 333
- Exceptions (more TBD?):
  - March 31
  - April 2
- Auditors
  - Send me your Penn State email i.d. so that I can add you to the Angel mailing list for the class.

# Evaluation

---

- maximum of
  - 30% exams + 50% homework + 20%project,
  - 30% exams + 40% homework + 30%project)
- Exams (2 midterms + final)
  - Midterm 1: Tue, Feb 24, 8-10pm at 109 Walker
  - Midterm 2: Fri, Apr 3, 8-10pm at 109 Walker
- Homework policy:
  - Collaboration **ok**, copying **NOT OK**
  - partial credit hard to get
    - 20% rule
  - Extra credit problems
  - Please type your solutions (no mercy for bad handwriting)

# Textbook

---

- Jonathan Katz and Yehuda Lindell.  
*Introduction to Modern Cryptography*.  
CRC Press, 2007.
  - At bookstore
- Useful reference:
  - Oded Goldreich. *Foundations of Cryptography*, Vols 1 and 2.
- When we follow the KL book (75% of class) I expect you to **read** assigned chapters and **prepare questions**

# Homework

---

- Read KL Chapters 1, 2
- Homework to hand in approx every 2 weeks.

# Project

---

- Examples:
  - Theory project: summarize existing work on a particular problem, explain one or several interesting ideas and propose (or solve!) some open problems
  - Programming project: Implement some latest/greatest protocol, evaluate performance.
  - [Your suggestion here. Be creative.]
- Teams (up to 3) are ok. Expected quality scales with the number of team members...
- You'll have to propose a project within about 4 weeks (1/3 of the way through the semester)

---

Questions?

# Highlights

---

- Things you can do:
  - Public-key cryptography
    - two locks on a chest
  - Zero-knowledge proofs
    - Coke v. Pepsi reloaded
  - Poker over the telephone
    - (How do you shuffle and deal?)
- Big Ideas:
  - Careful definitions: how can we formalize concepts like “secure”?
  - Proofs via reductions
  - Hardness as a tool: “One man's misfortune is another man's gain”
  - Pseudorandomness: what makes a bit stream “random”?

# Today: Encryption

---

- Symmetric encryption: setting
- What should “security” mean?