Lecture 00: Cryptography

Apologies

- Sorry for not being here for the first class
- I am traveling and, if everything works out as planned, I should be here for the next lecture
- Do not worry. You are in extremely capable hands today
- Alex Block, your teaching assistant for the course, who also conducts research with me in Cryptography, is taking the first class

Course Content

- Introduce Foundational Topics in Cryptography
  - Mathematical Foundations
  - Some Applications and Coding

About Prof. Maji

- He is a Theoretical Cryptographer
- Visit webpage to find more about research
  - `https://www.cs.purdue.edu/homes/hmaji/`

What is Cryptography?

- Controlling Access to Information
  - Who learns what?
  - Who can Influence what?

Relation to Other Topics

- Part of Information Security
- Significant Intersection with
  - Complexity Theory
    - One Way Functions
  - Information Theory
    - Quantification, Storage, Communication of Information
  - Number Theory, Linear Algebra
    - RSA; Error Correcting Codes
  - Combinatorics, Graph Theory

Course Outline

- Theoretical Cryptography: Provable Security
- Practice: Under the Concerns of Implementation
- Grand Aim: Initiate into the state-of-the-art research topics in Cryptography

Topics

- Private-key Cryptography
- Pseudorandomness
- Message Authentication Codes
- Hashing
- Public-key Cryptography
- Digital Signatures
- Zero-knowledge
- Multi-party Computation

Prerequisites

- Basic Algorithms (CS 58000)
- Mathematical Maturity
- Read the course website and the course policy

Course Instruction

- Board-work
- Lecture notes (in next couple of days)
- Pointers to a lot of reading materials
- General Pointers to books and other related courses
  - No official course book
  - The course syllabus is flexible and student interest will influence it

Grading

- 40% Homework (3 – 4)
- 25% Midterm (in class)
- 30% Final Exam
- 5% Class Participation

How to Use this Course?

- For Grades
  - Submit Homework, perform in Exams, and Participate in Class
- For Research
  - Solve extra-credit problems, read additional materials, discuss with instructor by scheduling appointments, and target to find a research topic of choice

Office Hours

- Office hour with Instructor: By Appointment Only
- Office hour with TA: One hour that is agreeable to the TA and all students (please discuss now)

Concluding Remarks

- What is expect of you: Knowledge of "Algorithms"-equivalent course, some Mathematical Maturity and Class Participation
- We will collaboratively learn from each other
- Read the course webpage

Emergency Preparedness — A Message from Purdue

- To report an emergency, call 911. To obtain updates regarding ongoing emergency, sign up for Purdue Alert text messages, view www.purdue.edu/ea.
- There are nearly 300 Emergency Telephones outdoors across campus and in parking garages that connect directly to the PUPD. If you feel threatened or need help, push the button and you will be connected immediately.
- If we hear a fire alarm during class we will immediately suspend class, evacuate the building, and proceed outdoors. Do not use the elevator.

Emergency Preparedness — A Message from Purdue (Cont.)

- If we are notified during class of a Shelter in Place requirement for a tornado warning, we will suspend class and shelter in [the basement].
- If we are notified during class of a Shelter in Place requirement for a hazardous materials release, or a civil disturbance, including a shooting or other use of weapons, we will suspend class and shelter in the classroom, shutting the door and turning off the lights.
- Please review the Emergency Preparedness website for additional information. http://www.purdue.edu/ehps/emergency_preparedness/index.html