

Lecture 00: Introduction

What to Expect from this Course?

- We shall learn the fundamentals of cryptography
 - Topics: Private-key Cryptography, Pseudorandomness, MACs, Hashing, Public-key Cryptography, Digital Signatures, Multi-party Computation
- Coding is encouraged to develop intuition
 - You can use [sage](#) (similar to Python) for coding. You can use the free platform [cocalc](#) to write and compile sage code
- Lectures are highly interactive

Who am I?

- Name: Hemanta K. Maji
- Research Interests: Cryptography, Theoretical Computer Science
- Office: LWSN 1177
- Office Hours: By **email**

- We shall use [Piazza](#) for this course to ask and answer questions. Everyone is highly encouraged to use this platform

Course Policy II

- Evaluation: (Roughly) Eight homework (40%), one mid-term exam (25%), and a final exam (35%)
- Grading will be done using percentiles.
 - In Fall 2018, the following grades were given: A+, A, A-, B+, B, B-, C, C-, D, F.
 - Roughly 23% of students for A or higher, and
 - Roughly 23% of students got C or below
 - Solving extra-credit problems earns you instructors' goodwill. So, if your total score is close to a grade threshold, then you might get the higher grade if you have sufficient instructors' goodwill

- Homework Submission: All homework must be \LaTeX -ed
 - We shall provide the \LaTeX -files for the questions
 - You can use [Overleaf](#) to typeset your solutions
 - Output pdf files are to be emailed to the TAs
 - We shall experiment using [Gradescope](#) to evaluate your homework solutions
 - Students are highly encouraged to collaborate for homework. Every student must typeset their own solutions. Please mention the name of all the students that you collaborated for each question

- Please go over the course [policy](#) website for all additional details

Instruction in the Course

- Lecture Notes prepared by me will be uploaded
- Reference Book: [Introduction to Modern Cryptography, Second Edition](#) by Jonathan Katz and Yehuda Lindell
- The lectures and the lecture notes will encourage students to work and think on exploratory problems

Introduction to your TAs

- Hai Nguyen
- Hamidreza Amini
- Office Hours will be uploaded soon

Background Needed

- Basic Mathematics, like, integration, differentiation,
- Asymptotic Notation, and
- Probability Basics.