

Lecture 00: Introduction

What to Expect from this Course?

- We shall learn the fundamentals of cryptography
 - Topics: Private-key Cryptography, Pseudorandomness, MACs, (possibly) Hashing, Public-key Cryptography, Digital Signatures, (possibly) Basics of 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
 - 1 Old video lectures are online on Brightspace
 - 2 Old in-person lectures are online on Brightspace

Who am I?

- Name: [Hemanta K. Maji](#)
- Research Interests: Cryptography, Information Theory, Theoretical Computer Science
- Office: LWSN 1177
- Office Hours: By [email](#)

- We shall use [Ed Stem](#) for this course to ask and answer questions (joining code is available on Brightspace). Everyone is highly encouraged to use this platform
- Historically, my average response time has been (less than) roughly 15 mins

Course Policy II

- Evaluation: (Roughly) Seven/eight homework (40%), one mid-term exam (25%), and a final exam (35%).
- Grading will be done using percentiles.
 - Previously, the following grades were given: A+, A, A-, B+, B, B-, C, and F.
 - Solving extra-credit problems earns you the instructors' goodwill. So, if your total score is close to a grade threshold, then you might get a 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
 - How to submit pdfs for evaluation? TAs will get back to you soon
 - We shall use [Brightspace](#)
 - Students are highly encouraged to collaborate for homework. However, Every student must typeset their own solutions. Furthermore, 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

- Xiuyu Ye
- Office Hours will come up soon on Ed Stem

Background Needed

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