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 typically highly interactive
  1. CS355 video lectures are all online
  2. CS355 in-person lectures are online

Who am I?

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

Course Policy I

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

Course Policy II

- Evaluation: (Tentatively) Seven/eight homework (40%), one mid-term exam (25%), and a final exam (35%).
- Grading will be done using percentiles

Course Policy III

- 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

Course Policy IV

- Please go over the course policy website for all additional details (this semester there might be some changes, I will update you when I introduce these changes)

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 be online and will be uploaded soon (poll for day/time on campuswire)

Background Needed

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