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
- In regular semesters, lectures are highly interactive. This semester, there will be lecture videos, and one lecture for interaction
  1. Video lectures for the entire week will go online on Sunday midnight
  2. Monday lecture is cancelled
  3. Group A attends Wednesday lecture
  4. Group B attends Friday lecture

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 Piazza for this course to ask and answer questions. Everyone is highly encouraged to use this platform
- Historically, my average response time has been roughly 15 mins

Course Policy II

- Evaluation: (Roughly) Eight homework (40%), one mid-term exam (25%), and a final exam (35%). This semester the mid-term and the final may be online
- Grading will be done using percentiles.
    - In Fall 2017, Fall 2018, and Spring 2020: the following grades were given: A+, A, A-, B+, B, B-, C, C-, and 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"
    - Every course offering a couple of students get an *F*

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 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

- Hai H. Nguyen
- Hamidreza Amini Khorasgani
- Office Hours will be uploaded soon (poll for day/time in piazza)

Background Needed

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