Computer Science: CS435, Fall 2024
Introduction to Cryptography

Instructor: Rishab Goyal
Office: CS 4373, Computer Science Department (1210 W. Dayton)
E-mail: rishab.goyal@wisc.edu
Office Hours: Monday, Friday 3:45-5PM (after class), and by appointment.

TA: Abtin Afshar
E-mail: abtin@cs.wisc.edu
Office Hours: Monday 5:00-6:00PM and Wednesday 11:00AM-12:00PM (*).

TA: Saikumar Yadugiri
E-mail: saikumar@cs.wisc.edu
Office Hours: Tuesday 11:00AM-12:00PM and Thursday 5:00-6:00PM (*).

TA: Sanjay Nagarimadugu
E-mail: snagarimadug@wisc.edu
Office Hours: TBD.

Class: Monday, Wednesday, Friday 2:30-3:45PM in Sewell Social Sciences 5206
Midterm: October 18th, 2024, in class.
Final: December 18th, 2024, location TBD.

(*) TAs will host office hours in the CS building, room 1334.

Course Overview

The objective of this course is to introduce modern cryptography and discuss its many applications. The course will cover the fundamentals of cryptography including encryption, authentication, pseudorandomness, average-case hardness, number theory etc. We will focus on the theoretical underpinnings of cryptography, and discuss how computational hardness from number theory problems can be translated into security of various cryptographic systems. A major component of this course will be to precisely capture different security guarantees using theoretical definitions, and show how to rigorously prove formal theorems about designed systems.

This course is designed to be a challenging theory course. *No* prior knowledge of cryptography is required, however mathematical maturity and a strong theoretical CS background will be highly desirable.

Textbook and Readings

The material shared during class will be self-contained. The textbook – "Introduction to Modern Cryptography" by Katz and Lindell – is strongly recommended and will be a useful supplementary resource. Additional supplementary material will be shared using Canvas.

Grading and Evaluation

For evaluation, the course will contain 5 homework assignments (provided biweekly which have to be typeset via LaTeX), 2 exams (an *in-class* mid-term and an *in-class* final). The following explains the "points" distribution.

Homework (best 4 out of 5)	**Mid-Term**	**Final**
$25 * 4$	50	50

There will also be *15 bonus points* for in-class participation (which will be awarded based on class attendance and in-person discussion). Bonus points will be considered only at the time of final grading in case a student is missing the next grade by a small margin. E.g., suppose a student scored 150 points out of 200, and the cut-off for grade AB was 152 points. Then the bonus points will be considered to increase the grade to A from AB, if the student has sufficient bonus points, awarded as class participation.

We emphasize that the *the lowest score* among the 5 homework assignments will be dropped while calculating the final score. The problems in homework assignments and exams will be directly based on concepts discussed in lectures, and sufficient hints will be provided during lectures as an aid. *The final grades will be assigned on a curve based on the entire class performances.* The participation credit will be used to bump up your grade when it is closer to a higher grade's boundary. You can earn participation credit by attending lectures, asking and answering questions during lectures, and answering questions on piazza.

Other Information

- For questions, the students should follow the 4 point approach:
  1. Ask the question during a lecture.
  2. If (1) doesn't fully resolve, then post the question on Piazza. (Typically, (1) and (2) will resolve most questions and they will also be helpful to your classmates.)
  3. Otherwise, contact the TAs.
  4. Lastly, if the question is still unresolved, you should contact the instructor.
- Allowed absences are for religious observance and medical emergencies (with a doctor's note). If you need to reschedule an exam for the former, or will be unable to participate or attend lectures, then please notify the instructor **within the first two weeks of classes**. If you need to reschedule an exam for a medical emergency, then please notify the instructor **as soon as possible**.

Tentative List of Topics

The following is a tentative list of topics that we plan to cover during the course. This will be subject to minor changes depending on how the course progresses and prior familiarity of the class with cryptographic concepts. Remaining lectures are reserved for problem solving days, exam reviews, guest lectures and so on.

History and Perfectly Secure Encryption. (3 sessions)

Pseudorandomness: Generators and Functions. (2 sessions)

Encryption I: Definitions and Constructions. (4 sessions)

Block Ciphers. (1 session)

Hash Functions: Collision Resistance. (2.5 sessions)

Authentication: Definitions and Constructions. (2.5 sessions)

Encryption II: CCA Security. (2 sessions)

Number Theory and Modular Arithmetic. (2 sessions)

Number-Theoretic Cryptographic Assumptions. (1 session)

Using Number Theory: Hash Functions. (1 sessions)

Public-Key Encryption and Signatures. (3 sessions)

These topics will require approximately 24/25 in-person lectures.