Computer Science: CS880, Spring 2025
Graduate Cryptography

Instructor: Rishab Goyal
Office: CS 4373, Computer Science Department (1210 W. Dayton)
E-mail: rishab.goyal@wisc.edu
Office Hours: Monday after class

Class: Monday 2:25-5:25PM in CS 1257
Midterm: (tentative) Monday, March 17 (before Spring break)
Project Presentations: (tentative) Monday, Apr 28, (last class)

Course Overview

The objective of this course is to give a graduate level introduction to cryptography and discuss its many applications. The course will cover the fundamentals of cryptography including encryption, authentication, pseudorandomness, average-case hardness etc. We will focus on the theoretical underpinnings of cryptography, and discuss how different sources of computational hardness 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. Basic knowledge of cryptography is assumed. Mathematical maturity and a strong theoretical CS background will be highly desirable. The course is designed to provide a fast-paced overview of modern cryptography and a brief introduction of fundamentals of post-quantum security. The pre-requisites are CS 435 or graduate standing.

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 appropriately. The textbook – "Foundations of Cryptography" (Vol. 1 and 2) by Oded Goldreich – is also recommended as an additional resource.

Grading and Evaluation

For evaluation, the course will contain 1 *in-class* mid-term, and a research project.

The following will serve as a good estimate of "points" distribution.

35	65
Midterm	Research Project

Other Information

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.

Lecture 1: History, Encryption, Perfect Secrecy, and IND-CPA Security.

Lecture 2: Pseudorandom Functions, Encryption, Hybrid Proofs and Reductions.

Lecture 3: Pseudorandom Generators and GGM construction.

Lecture 4: Hash Functions, Collision Resistance, and MACs.

Lecture 5: Computational Hardness, Modular Arithmetic, Fields, LWE, and One-Way Functions.

Lecture 6: (Dual) Regev Encryption, Leftover Hash Lemma, and Lattices.

Lecture 7: SIS, Hash Functions, Signatures, Random Oracles, and Lattice Trapdoors.

Lecture 8: Mid-term.

Lecture 9: Attribute-Based Encryption.

Lecture 10: Homomorphic Encryption.

Lecture 11: Lockable Obfuscation.

Lecture 12: Traitor Tracing.

Lecture 13: Project Presentations.