CS-282A and MATH-209A, FALL 2025 Prof. Rafail Ostrovsky

FOUNDATIONS OF CRYPTOGRAPHY

First lecture: Monday, September 29th, 2025 **CRYPTO**

When: M,W 4pm-5:50 pm
Where: Young Hall 2200
Email: rafail@cs.ucla.edu
Office: 475 Engineering VI;
Office hours: Immediately after each lecture, 5:50-6:30 pm in the lecture hall or by appointment.

IMPORTANT NOTE: There will be no lectures on October 20 and 23, as I will be at Oxford giving a Strachey lecture.

Description: This is a graduate course that introduces students to the theory of cryptography, stressing rigorous definitions and proofs of security. Topics include: notions of hardness, one-way functions, hard-core bits, pseudo-random generators, pseudo-random functions and permutations, public-key and private-key encryption, verifiable random functions, secret-sharing and function secret-sharing, message authentication, digital signatures, interactive proofs, zero-knowledge (ZK) proofs and its variants, collision-resistant hash functions, commitment protocols, key-agreement, Oblivious Transfer, Private Information Retrieval, Oblivious RAMs and multiparty secure computation (Yao, GMW, BGW, Garbled RAM). We will also cover succinct ZK and its applications.

Objectives: This course is intended to introduce students to current research in cryptography, including modern cryptographic definitions and proofs of security.

Prerequisites: Mathematical maturity and knowledge of undergraduate algorithms.

Textbooks: None. The course material will consist of online materials for recent topics, and my 2010 lecture notes; see:

https://web.cs.ucla.edu/~rafail/PUBLIC/OstrovskyDraftLecNotes2010.pdf

Grading Policy: Grading: Midterm 45%; Final 55%; All exams will be closed-book/notes/electronics.