CS 282A/MATH 209A: Foundations of Cryptography Prof. Rafail Ostrovsky

FOUNDATIONS OF CRYPTOGRAPHY

First lecture: Monday, September 26th, 2022 **CRYPTO**

When: M,W 2pm-3:50pm
Where: Engineering VI 134
Email: rafail@cs.ucla.edu
Office: 475 Engineering VI;
Office hours: Monday 4:15-5pm or by appointment (starting on 10/3/2022)

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

Objectives: This course is meant to introduce students to up-to-date 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 consists of on-line materials, and my 2010 lecture notes, see: http://web.cs.ucla.edu/~rafail/PUBLIC/OstrovskyDraftLecNotes2010.pdf

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