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

FOUNDATIONS OF CRYPTOGRAPHY

First lecture: Monday, September 27th, 2021 **CRYPTO**

When/where: FALL 2019, M,W 2pm-3:50pm on Zoom:

`https://ucla.zoom.us/j/94845546253`

Email: rafail@cs.ucla.edu **Office:** 475 Engineering VI;
Office hours: Wednesday 4:00-4:45pm on Zoom:

`https://ucla.zoom.us/j/93482657363`

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 pseudo-random permutations, semantic security, public-key and private-key encryption, secret-sharing, message authentication, digital signatures, interactive proofs, zero-knowledge proofs, private information retrieval, collision-resistant hash functions, commitment protocols, key-agreement, Oblivious Transfer, Oblivious RAMs and multi-party secure computation (Yao, GMW, BGW).

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 take-home.