CS 183 Prof. Rafail Ostrovsky

Introduction to CRYPTOGRAPHY

First lecture: Monday, March 30th, 2pm-3:50PM **CRYPTO**

When/where: SPRING 2020, M,W 2pm-3:50pm on Zoom;
Prof: Rafail Ostrovsky;
Office hours: Monday 4-4:50 pm or by appointment (starting from April 6^{th}.)
TA's:

- Eli Jaffe; Email: jaffe.eli96@gmail.com
- Ashutosh Kumar; Email: ashumac@gmail.com

Description: This is an undergraduate course introducing students to the theory of cryptography, stressing definitions, proofs of security and applications. 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, digital signatures, message authentication, digital signatures, interactive proofs, zero-knowledge proofs, private information retrieval, collision-resistant hash functions, commitment protocols, key-agreement, two-party and multi-party secure computation and Oblivious RAM.
Objectives: This course is meant to introduce students to cryptography, including modern cryptographic definitions and proofs of security as well as applications.
Prerequisites: CS180.
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: Take-home Midterm 45% ; Take-home Final 55% .