CS 183, SPRING 2022 Prof. Rafail Ostrovsky

Introduction to CRYPTOGRAPHY

First lecture: Monday, March 28th 2022, 12pm-1:50PM

Where: Royce Hall 190
When: M,W 12pm-1:50pm
Prof: Rafail (Rafi) Ostrovsky;
Office: 475 Engineering VI;
Office hours: Monday 2:15-3:00pm or by appointment, starting on April 11^{th}
TA's:

- Eli Jaffe; Email: jaffe.eli96@gmail.com
- Kevin Garbe; Email: kevin@garbe.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, blockchains, 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 or permission of instructor.

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.