

FOUNDATIONS OF CRYPTOGRAPHY

First lecture: Monday, January 8th, 2024

CRYPTO

When: M,W 4pm-5:50 pm**Where:** Boelter Hall 2444**Email:** rafail@cs.ucla.edu**Office:** 475 Engineering VI;**Office hours:** Monday 6:15-7 pm or by appointment (starting on 1/22/2024)

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 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).

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 consist of on-line materials for recent topics, and my 2010 lecture notes, see:

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

Grading Policy: Each student who is registered for class will scribe notes for a single lecture. Please use my 2010 lecture notes as a starting point for your scribes. The scribes for a given lecture will jointly prepare a \LaTeX document understandable for students who did not attend the class. Scribes are due 4 days after the lecture at 9 pm (either Friday or Sunday). \LaTeX templates for scribe notes will be posted on my homepage. Grading: Midterm 40%; Final 50%; Scribe 10%. All exams will be closed book/notes/electronics.