

FOUNDATIONS OF CRYPTOGRAPHY

First lecture: Monday, September 26th, 11AM-12:50PM

CRYPTO

When/where: FALL 2011, M,W 11am-12:50pm MS 5203;**Prof:** Rafi Ostrovsky;**Office:** 3732D Boelter Hall;**Office hours:** Tuesday 4-5pm or after class.**Course WEB PAGE:** <http://www.cs.ucla.edu/~rafail/CRYPTO.html>

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, contract signing and two-party secure computation with static security.

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.

Textbooks: None. The course material will consist of on-line materials, lecture notes scribed by students and research papers in cryptography which will be available either as class handouts or web-pointers.

Grading Policy: Class participation 15%; two in-class quizzes 30% each; Scribe notes 25%. All exams will be closed book.

Scribe notes: You must revise (previous) scribe notes for at least one topic. Each topic will span several lectures, and I expect the same team to cover each topic completely. The total number of topics each team will cover will be determined by the number of students in the class. The scribed lecture must update current lecture notes (written in \TeX format). We will provide a template and you should email me asking for \TeX source code for whatever parts you are updating. It is important that you should not only check for correctness of previous notes, fix all issues and improve readability, but also add whatever additional material I presented on each topic. You should not delete previous material from lecture notes, even if I did not manage to cover it in class, though if it is repetitive I expect you to consolidate it. You should also make sure that all notations are consistent when covering the same or related topic. Revised scribe notes will provide text for the class.