FOUNDATIONS OF CRYPTOGRAPHY

First lecture: Monday, September 29th, 2008 2-3:50PM Where: WGYOUNG 4216

Instructor: Rafail Ostrovsky, **Office:** 3732D Boelter Hall. **When/where:** FALL 2008, M,W 2-3:50pm WGYOUNG 4216. **Course WEB PAGE:** `http://www.cs.ucla.edu/~rafail/TEACHING/282A.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 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 consists 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 5%; 2 half-hour quizzes 15% each; Scribe notes 35%; Final project 30%.
Scribe notes: You must scribe multiple lectures, the total number to be determined by the number of students in the class. The scribed lecture must be given in TEX format (we will provide a template). It is important that you not only write what was said in lecture, but also clarify things and include all relevant material from my 2006 lecture notes. These scribe notes will provide the text for the class.
Scribe instructions: Each topic will be covered by several students, who must jointly write a preliminary version You should use my 2006 lecture notes as a starting point. Ask me for the latex source of the relevant lectures. After 2 days, the joint preliminary scribe notes are submitted to me. All scribes must than make an appointment within one week of the lecture to jointly discuss your notes with me. After I make one or more edits of the scribe notes, the final version will be available on-line.
Final project: Final project requires students to form small teams of 2-3 people each. Every team will be required to read a paper outside of class, write (in TEX) a summary explaining main ideas and proofs and give a verbal presentation of the paper and its analysis to the whole class.