CS 282A/MATH 209A: Foundations of Cryptography © Rafail Ostrovsky

FOUNDATIONS OF CRYPTOGRAPHY

First lecture: April 3, 2006 4-5:50PM *Where: WGYOUNG 4216*

Instructor: Rafail Ostrovsky, **Office:** 3732D Boelter Hall. **When/where:** Spring 2006, M,W 4-5:50pm WGYOUNG 4216. **Course WEB PAGE: (to go up this week)** `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, collision-resistant hash functions, commitment protocols, key-agreement, contract signing and two-party secure computation with static security. **Objectives:** This is the first part of a two-part course meant to introduce students to up-to-date research in cryptography, including modern cryptographic definitions and proofs of security.
Prerequisites: Mathematical maturity, CS180 or equivalent, knowledge of randomized algorithms, basic probability theory, NP-completeness. Knowledge of computational number theory will be helpful, though not required.
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 also include all relevant material from my 2005 and 1994 lecture notes as these scribe notes will provide the text for the class. For scribe instructions, see the footnote[1].
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.

[1]Each topic will be covered by several students, who must jointly write a preliminary version (you may use my previous year lecture notes as a starting point, as well as my 1994 lecture notes.) After 2 days, the joint preliminary scribe notes are submitted to me for grading. 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.