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

FOUNDATIONS OF CRYPTOGRAPHY

First lecture: January 10, 2005, 4-5:50PM — *Where: Geology 3656*

Instructor: Rafail Ostrovsky, **Office:** 3732D Boelter Hall. **When/where:** Winter 2005, M,W 4-5:50pm. Class held in Geology 3656. **No Class on February 7th and February 9th.** We will have make-up sessions in the end of the quarter. **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, 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: 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, as these scribe notes provide the text for the class. For scribe grading, 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 write a preliminary version independently of each other (though you may consult any on-line source before writing it). After 2 days, the preliminary scribe notes are submitted (as a printout) for grading. All scribes must than join their scribe notes into a joint single document and show to me by appointment within one week of the lecture. For each scribe effort, the individual effort is counted as 20% and then joint effort of the group as 15%. After I make one or more edits of the joint scribe notes, the final version will be available on-line.