

CSci 381 Advanced Cryptography - 3 credits - Vora

Elliptic Curve Cryptography. Computational theory of secrecy. Zero-knowledge proofs. Special topics chosen according to student and instructor interests.

Fall 2009 schedule: Thurs., 7:10 - 9:40 pm, Tompkins 205

Instructor: Poorvi Vora, Philips 706

Office Hours: 1-4 pm Thurs., and by appointment

Course Website: <http://www.seas.gwu.edu/~poorvi/Classes/CS381/>

Prerequisite: CSci 212 and CSci 284

Goal: To teach some of the more advanced topics in cryptology and to teach students to read, evaluate and write papers.

Grading class participation: 20%; Paper presentation + reports on other student papers: 40 %; Project: 40%

Class participation: You are expected to attend and participate in class. You may lose marks for disrupting the class.

Paper presentation: You will present several papers, from the reading lists provided. The presentation will involve explaining the paper to the class, commenting on its merits, identifying its flaws, and commenting on future research ideas that may come from the paper, for a total of twenty minutes. You may assume that all students have read the paper, and possess knowledge of the basics to understand the paper. Your job is to critically evaluate it. For each paper presented, including your own, you will submit a three-quarter-page report that briefly describes the main result of the paper, its contribution in light of the literature existing at the time, its strengths and weaknesses, and future research directions it suggests.

Project: The project will be a written paper surveying the literature in a field determined by the student in consultation with, and with the approval of, the instructor.

Any student who feels s/he may need an accommodation based on the impact of a disability should contact me privately to discuss specific needs. Please contact the Disability Support Services office at 202.994.8250 in the Marvin Center, Suite 242, to establish eligibility and to coordinate reasonable accommodations. For additional information please refer to: <http://gwired.gwu.edu/dss/>.

CSci 381 Advanced Cryptography, Fall 2007, Course Outline

Lecture 1, Sept. 3

Cryptography over Groups: Diffie-Hellman, El Gamal, efficient exponentiation.

Lecture 2, Sept. 10

Elliptic Curve Cryptography: elliptic curve algebra

Lecture 3, Sept. 17

Information theory of secrecy: review. Computational theory of secrecy: definitions.

Lecture 4, Sept. 24

Hard-core predicates, existence of PRNGs.

Lecture 5, Oct. 1

Next-bit prediction and security against statistical attacks. Student Presentation: Computational Secret Sharing.

Lecture 6, Oct. 8

Zero-knowledge Proofs. Bit commitment.

Lectures 7-13

Student Presentations