

**CSci 381 Advanced Cryptography - 3 credits - Vora**

Elliptic Curve Cryptography. Computational theory of secrecy. Zero-knowledge proofs. Cryptanalysis. Voting.

**Fall 2007 schedule:** Thurs., 7:10 - 9:40 pm, Rome 201

**Instructor:** Poorvi Vora, Philips 706

**Office Hours:** 1-4 pm Wed., 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** 3HWs: 10% each; class participation: 10%; Paper presentation + reports on other student papers: 30 %; Project: 30%

*HW:* Due at the beginning of class. No exceptions. You may collaborate in figuring out the HW solutions, but you must write out the solution on your own and may not copy any part of another person's work. You must acknowledge *every* source, including the ideas of a classmate. **Any violation of this policy will be considered a violation of academic integrity.**

*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 20 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. 6 (HW 1 assigned)*

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

*Lecture 2, Sept. 13 (HW 1 due)*

Elliptic Curve Cryptography: elliptic curve algebra

*Lecture 3, Sept. 20 (HW 2 assigned)*

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

*Lecture 4, Sept. 27*

Hard-core predicates, existence of PRNGs. Student Presentation: Shamir secret sharing.

*Lecture 5, Oct. 4 (HW 2 due)*

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

*Lecture 6, Oct. 11 (HW 3 assigned)*

Zero-knowledge Proofs. Bit commitment. Student Presentation: Visual Cryptography.

*Lecture 7, Oct. 18*

Student Presentations on Anonymity Primitives, Measurement and Audit.

*Lecture 8, Oct. 25 (HW 3 due)*

Student Presentations on homomorphic encryption and voting.

*Lecture 9, Nov. 1*

Student Presentations on electronic cash.

*Lecture 10, Nov. 8*

Student Presentations on statistical cryptanalysis.

*Lecture 11, Nov. 15*

Instructor Lecture: Coding theory. Related-key attacks. Concatenated Codes.

*Lecture 12, Nov. 29*

Student Presentations: SHA-1 Attacks.

*Lecture 13, Dec. 6 TBD*