

CSci 381 Advanced Cryptography - 3 credits - Vora

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

Fall 2005 schedule: Wed., 7:10 - 9:40 pm, Philips 108

Instructor: Poorvi Vora, Philips 706

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

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

Non-negotiable prerequisite: CS 212 or equivalent: graduate algorithms, and CS 284 or equivalent: introductory graduate cryptography. One of the two prerequisites may be excused for an A (but not an A-) in the other. The pre-reqs may be replaced by familiarity with proofs and modern algebra such as obtained through an undergraduate degree in mathematics.

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: 30 %

Project: 30%

CSci 381 Advanced Cryptography, Fall 2004, Grading Details

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 during the second half of the semester, from the reading lists of papers for each class. 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 15 minutes. You may assume that all students have read the paper and possess knowledge of the basics to understand the paper (these will be taught in the first half of the semester). Your job is to critically evaluate it.

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.

CSci 381 Advanced Cryptography, Fall 2004, Course Outline

Lecture 1, Aug. 31 (HW 1 assigned)

Elliptic Curve Algebra

Lecture 2, Sept. 7 (HW 1 due)

Cryptography using elliptic curves.

Lecture 3, Sept. 14 (HW 2 assigned)

Information Theory of Secrecy.

Lecture 4, Sept. 21

Computational Theory of Secrecy: Computational secrecy. Pseudo-random number generators (PRNG's), LFSRs, Blum-Blum-Shub, self-shrinking generator. Next bit prediction. One-way functions and PRNG's. Next-bit prediction and statistical attacks.

Lecture 5, Sept. 28 (HW 2 due)

Complete Computational Theory of Secrecy.

Secret Sharing: Shamir Threshold Scheme, access structures and general secret sharing, Brickell vector Space construction. Visual Cryptography.

Lecture 6, Oct. 5

Protocols: Oblivious Transfer, Bit Commitment, Simultaneous Contract Signing, Simultaneous Secret Exchange. Oblivious Transfer equivalence to deletion channel (Crepeau).

Lecture 7, Oct. 12 (HW 3 assigned)

Zero-knowledge Protocols contd. Multi-Party Protocols: Secret Sharing, Verifiable Secret Sharing. Catch up.

Lecture 8, Oct. 19

Student Presentations begin

Anonymity Primitives, Measurement and Audit. Chaum MIX, Juels-Rivest Randomized Partial Checking of MIXes, Crowds. Dining Cryptographers, Anonymity Set. Serjantov-Diaz Info-theoretic Anonymity. Chaum Blind Signature. Measures.

Lecture 9, Oct. 26 (HW 3 due)

Homomorphic Encryption and Voting. Benaloh. Schoenmaker. Chaum Receipt Voting

Lecture 10, Nov. 2

Cash.

Lecture 11, Nov. 9

Statistical Cryptanalysis. Piling-Up Lemma. Wagner Block Cipher Model. Smeets Stream Cipher Cryptanalysis Model. Filiol. Massey et al ??

Lecture 12, Nov. 16

Coding theory. Related-key attacks. Concatenated Codes.

Lecture 13, Nov. 30

Number-Theoretic Cryptanalysis. Factoring. Discrete Log. Exponential factoring algorithms. Sub-exponential factoring. Probabilistic polynomial factoring.