

CSci 283/CSci 172 Computer Security - 3 credits - Vora

Fall 2006 schedule: Tues., 7:10 - 9:40 pm, Rome 204

Instructor: Poorvi Vora, Philips 706

Office Hours: Tues: 1:30-4:30, Thurs: 10:30am-noon, 1-2:30 pm unless canceled in class.

TA: Yu-An Sun. Email: ysun@gwu.edu Office: 720 G, Philips Hall.

Office Hours: Wed 4-7:30pm and Tuesday 4:30pm to 7pm.

Course Website: <http://www.seas.gwu.edu/~poorvi/Classes/CS283/>

Purpose of course: To provide a broad overview of computer security at the advanced undergraduate/introductory graduate level.

Course content: Introductory cryptology and cryptographic protocols; program, database and network security; trusted operating systems; vulnerabilities/threats, attacks, defenses; administration of security; security policy.

Prerequisites: Undergrad level discrete math, programming, computer organization.

Text: *Computer Security: Art and Science* by Matt Bishop.

Grading: 25% for homework, 25% each for two in-semester tests, 25% for best 8 of 10 quizzes. *There will be no make-up quizzes.* Grading will be absolute and not on a curve. All HWs will be submitted in Blackboard. **You will not be allowed the use of laptops, PDAs or calculators and similar devices during quizzes and in-semester tests.**

Undergraduate and graduate students will be graded separately. Graduate students will have extra assignments. *If you are an undergraduate and wish graduate credit for this class, contact your adviser. Graduate credit is NOT automatically obtained by undergraduates through registration for the graduate course.*

Policy on collaboration: All examinations, papers, and other graded work products and assignments are to be completed in conformance with The George Washington University Code of Academic Integrity. You may discuss HWs among yourselves, and work on them in groups. However, each student is expected to write his or her own HW out independently; you may not copy one another's assignments, even in part. You may not collaborate with others on the tests and quizzes. You are expected to cite all your sources in any written work that is not closed book: papers, books, web sites, discussions with others - faculty, friends, students. For example, if, in a group, one student has a major idea that leads to a solution to a HW problem, all other students in the group should cite this student.

Any violations will be treated as violations of the Code of Academic Integrity.

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/>.

Syllabus: This is a tentative syllabus. There will be quizzes during each class except Weeks I, VII and XIV.

Week I 5 September: Introduction. Classical and Stream Ciphers.

Chapters 1, 9.1, 9.2.1, 9.2.2, and 11.2, Text.

Week II 12 September: Block Ciphers and Public Key Cryptography.

Chapters 9.2.3, 9.3.1, 9.3, 9.4, Text.

Week III 19 September: Public Key Infrastructure and Authentication.

Chapters 10.1, 10.2.3, 10.4 Text.

Week IV 26 September: Access Control.

Chapters 2 and 15 (part of), Text.

Week V 3 October: Security Policies.

Chapter 4 (except 4.5 and 4.6), Text.

Week VI 10 October: Confidentiality, Integrity and Hybrid Models.

Chapters 5.1, 5.2.1, 6.1, 6.2, 7.1, 7.2 from text

Week VII 17 October: Test.

Material Covered in Lectures I-V.

Week VIII 24 October: Return Test. Discuss. Identity.

Chapter 14, Text.

Week IX 31 October: Malicious Logic.

Chapter 22 (upto and including 22.5), Text.

Week X 7 November: Authentication, Confinement. Design Principles.

Chapters 14, 13, 16. Text.

Week XI 14 November: Information Flow. Risk analysis and ethical issues.

Week XII 21 November: Trusted OS.

Week XIII 28 November: Database Security.

Week XIV 5 December: Test. Material Covered in Lectures VI-XII.