

CSCI 284 and CSCI 162- Graduate and Undergraduate Cryptography - Spring 2008
George Washington University
2020 K St., No. 7, Mon: 3:30 - 6:00 pm

Course Outline

Instructor: Poorvi Vora, Room 706, Phillips Hall, poorvi@gwu.edu

Teaching Assistant: Yu-An Sun, Room 720G, Philips Hall, ysun@gwu.edu

Website: <http://www.seas.gwu.edu/~poorvi/Classes/CS284/>

Purpose of course: To provide a rigorous introduction to cryptography at the graduate/upper-class level. This course will be intensive. Do not take it if you are allergic to the prerequisites or to working hard.

Course content: Classical ciphers and cryptanalysis, Shannons perfect secrecy, Feistel ciphers and AES, public-key crypto (RSA, Discrete Log), one-way functions and hashes, digital signatures.

Prerequisites: Discrete mathematics, some complexity theory.

Text: Douglas Stinson, "Cryptography: Theory and Practice", Third Edition, 2005.

Grading: HWs, (30%), weekly quizzes (15%), two tests (15% each), a final (25%). You may lose marks for disruptive behaviour in class.

Policy on collaboration: All examinations, quizzes, 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 anothers assignments, even in part. You may not collaborate with anyone other than any official project-mates on the project. 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. **You may never copy code, under any circumstances, from any source.**

You are expected not to collaborate on the quizzes, mid-term and final, all of which are closed-book.

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 the instructor 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/>.

Planned Syllabus (subject to change): This is a tentative syllabus. There will be quizzes during each class except Lectures 1, 6 and 12.

14 January 2008, Lecture 1: *Classical Ciphers*.

21 January 2008, Holiday: Martin Luther King Jr. Day

28 January 2008, Lecture 2: *Number-theoretic algorithms*. HW 1 assigned. Due 4 February.

4 February 2008, Lecture 3: *SPNs*. HW 2 assigned. Due 15 February.

11 February 2008, Lecture 4: *Block and Stream Ciphers*.

18 February 2008, Holiday: Presidents' Day

25 February 2008, Lecture 5: *Probability Theory*.

3 March 2008, Lecture 6: Test 1.

10 March 2008, Lecture 7: *Shannon Secrecy*. HW 3 assigned: Due March 28

17 March 2008, Spring Break

24 March 2008, Lecture 8: *Linear and Differential Cryptanalysis*. HW 4 assigned. Due April 11

31 March 2008, Lecture 9: *Number Theory for RSA*.

7 April 2008, Lecture 10: *RSA*.

14 April 2008, Lecture 11: *Discrete Log and Applications*.

21 April 2008, Lecture 12: Test 2. Lectures 7-11. HW 5 assigned. Due April 30.

28 April 2008, Lecture 13: *Hashes*. HW 6 assigned. Due May 14.

30 April 2008, *Wednesday*, Lecture 14: *Authentication*.