

**CSCI 284 and CSCI 162- Graduate and Undergraduate Cryptography - Spring 2009**  
**George Washington University**  
**MPA 310, Mon: 3:30 - 6:00 pm**

**Course Outline**

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

**Teaching Assistant:** Prof. Mohammed Obiedat, obiedat@gwmail.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.

**Prerequisites:** Discrete mathematics, some complexity theory.

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

**Grading:** HWs, (40%), weekly quizzes (35%), 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 *not* discuss HWs among yourselves. Each student is expected to work on his or her own HW independently. You may not refer to any sources other than your class notes, the textbook, and material available on the course website (such as slides, class notes, linked websites, suggested reading) for solutions.

*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 Lecture 1.

**12 January 2008**, Lecture 1: *Classical Ciphers*. HW 1 assigned. Due 26 January.

**19 January 2008**, Holiday: Martin Luther King Jr. Day

**26 January 2008**, Lecture 2: *Number-theoretic algorithms*. HW 2 assigned. Due 9 February.

**2 February 2008**, Lecture 3: *Block Ciphers*.

**9 February 2008**, Lecture 4: *Probability Theory*. HW 3 assigned. Due 23 February.

**16 February 2008**, Holiday: Presidents' Day.

**23 February 2008**, Lecture 5: *Shannon Secrecy*. HW 4 assigned. Due 9 March.

**2 March 2008**, Lecture 6: *Cryptanalysis*.

**9 March 2008**, Lecture 7: *Stream Ciphers and Entropy*. HW 5 assigned: Due March 23.

**16 March 2008**, Spring Break

**23 March 2008**, Lecture 8: *Complexity of Exponentiation*. HW 6 assigned. Due April 6

**30 March 2008**, Lecture 9: *RSA Correctness Proof*.

**6 April 2008**, Lecture 10: *Discrete Log Problem and El Gamal Encryption* HW 7 assigned. Due April 20

**13 April 2008**, Lecture 11: *Secure Hash*.

**20 April 2008**, Lecture 12: *Digital Signatures*.

**27 April 2008**, Lecture 13: *Elliptic Curves*.

**29 April 2008**, *Wednesday*, Lecture 14: *Catch Up*.