Math 4175: Cryptography I  
Sections 84583 and 84584

Instructor: Eric Ufferman  
Office: 445 McBryde  
Phone: 231-3982  
Email: ufferman@vt.edu

Office hours: MW 11:10-12, TR 2:30-3:30, and by appointment. If there is sufficient demand for office hour(s) at additional time(s), I’m willing to add more.


Prerequisites: At least one mathematics course at or above the 3000 level and facility with either a programming language or a computer algebra system. Interpret the latter requirement as an ability to write basic computer programs and automate large amounts of computation. Do not attempt to take this course if you have not satisfied the prerequisites.

Syllabus: The class will cover roughly the first three chapters of the text, and selections from chapter five, although some material may not appear in the textbook. Topics include classical cryptosystems and their cryptanalysis, elementary information and coding theory, block ciphers and an introduction to public key cryptography.

Grade Policy: Your grade will be based on three components:

- Homework 30%
- Project 10%
- Tests 60% (Three tests, each worth 20%)

Scores of at least 90, 80, 70 and 60 percent guarantee letter grades of at least A-,B-,C- and D- respectively.

Homework: Homework will typically be assigned and collected on a weekly basis. Submitted work must adhere to the following guidelines. There will be no exceptions, but your lowest homework grade will be dropped:

- Homework is due at the beginning of class on the due date.
- It must be submitted in class. Do not try to submit your homework by email.
- It must be type-written and stapled.
- If you use a computer to solve any problem, hand in well-commented source code or computer algebra system code.
- Include and sign an honor pledge that states all work is your own.
Project: Students will work in teams. Each team will be assigned to research one of the five “AES Finalists”. Each team will be given half of a class period to present the findings of their research. Presentations will take place in late November or early December.

Exams: There will be two exams during regular class periods and one during the final exam period. The in-class exams are tentatively scheduled for Friday, September 25th and Friday, October 30th. Any changes to the exam schedule will be announced at least one week in advance.

The final exam will be during the exam period scheduled by the university. These periods are:

- Section 84583 (morning class): December 16, 7:45am
- Section 84584 (afternoon class): December 15, 3:25pm

The final exam is a required class meeting that will not be rescheduled for discretionary reasons, including conflicts with work schedules and with classes and exams at other colleges or travel plans.

Make-up Policy: In general, makeup exams will not be given. If a student misses an exam for reasons that are serious and beyond the student's control, the situation will be handled on an individual basis. Students should be prepared to submit documentation confirming the reason for absence.

Late homework is not accepted. In case of a serious and documented excuse, consideration will be given to a request to excuse a missing homework grade.

Disabilities: If you need adaptations or accommodations because of a documented disability, if you have emergency medical information to share with me, or if you need special arrangements in case the building must be evacuated, please make an appointment with me as soon as possible.

Academic Honesty: All students must abide by the Virginia Tech Honor Code while completing any graded work in this course. All submitted assignments and exams must represent the student's own work. No unauthorized assistance may be given or received on any exams or quizzes. Calculators may not be used on exams or quizzes.

Classroom Courtesy:

Please be courteous and respectful to your fellow students and the instructor. In particular, observe the following:

- Arrive to class on time and stay for the duration.
- Don't carry on conversations when class is ongoing.
- Silence all cell phones and other electronic devices while in class.
- Computers should be used for note-taking only.