

# Syllabus for Math 260, Mathematics of Cryptography

T,Th 9:30-10:50

Appleton 216, Spring 2008

Dr. Tamara Veenstra

## Contact Information:

<b>Office</b>	Appleton 221	<b>Office Hours</b>
<b>Phone</b>	x8634	T,Th: 11-12:30 and MW: 2:30-4; Others by appointment
<b>Email</b>	Tamara_Veenstra@redlands.edu	or luck.
<b>Web</b>	<a href="http://newton.uor.edu/facultyfolder/tamara_veenstra">http://newton.uor.edu/facultyfolder/tamara_veenstra</a>	

*Texts:* REQUIRED: Barr's 'Invitation to Cryptology'

RECOMMENDED: Singh's 'The Code Book' (focuses more on historical background and is a great read, but you won't officially be tested on this material.)

*Technology:* We will be using mathematical software, especially Maple, for some activities. You will be writing some small programs in Maple, though no previous programming experience is expected. Some assignments will be due over email. HW assignments are posted on my web site and in blackboard and, in general, will not be given out in class.

## Course Objectives:

- to **understand** the mathematics involved in encrypting and decrypting information;
- to improve your problem solving abilities;
- to increase your familiarity with using computer software to solve problems;
- to improve your ability to think logically, analytically, and abstractly; and
- to improve your ability to communicate mathematics, both orally and in writing.

## Course Content:

In this course, we will study the mathematics behind encrypting and decrypting secret messages. We will primarily follow a historical approach, beginning with the simplest methods of encoding messages, and work up to some of the more complicated present day cryptographic systems, which are used in web and electronic security. We will also discuss methods of breaking these codes and which ones are secure. Mathematics has played an important role in developing and breaking codes. We will study a variety of mathematical topics (matrices, modular arithmetic and a bit of other number theory, and some probability and statistics) as necessary to understand these codes.

*Grading:* Your grade will be based on the following categories: attendance/participation (10%), daily homework (15%) quizzes (15%), exams (60%).

*Attendance and Participation:* You must actively participate in class to receive full credit in this category. Required participation includes putting problems on the board, working on in-class activities, and generally behaving in a way that maintains and supports a good learning environment.

*Daily Homework:* There will be daily assignments. Some of these will be collected and graded and some of these will be discussed and put on the board at the beginning of class. I will call on people at random to present these problems. Homework presented on the board will be graded on effort, while collected homework will be graded on correctness. Since the HW is discussed at the beginning of class, late HW will not be accepted.

*Quizzes:* There will be quizzes approximately once a week. There may also be some pop quizzes. No makeup quizzes will be given.

*Exams:* There will be a 2 or 3 midterm exams and a cumulative final exam. **The Office of the Registrar has scheduled the final examination for Wednesday, April 16, 3-6.** No make-up exams will be given unless arranged prior to the exam.

### *Topics and Approximate Schedule*

We will spend 2-4 weeks on each of the four units:

- Unit 1: Monoalphabetic ciphers, implementing monoalphabetic ciphers with modular arithmetic, and using statistics to break these codes
- Unit 2: Polyalphabetic ciphers, Vigenere cipher, and Cryptanalysis of these ciphers especially Friedman and Kasiski test
- Unit 3: Block Ciphers and Computer based cryptography - the Hill cipher, Playfair and DES, number representation, stream ciphers, hash functions, etc.
- Unit 4: Public Key Cryptography -- RSA, Diffie-Hellman, Digital Signatures, El Gamal. Some RSA attacks - primarily factorization tricks.
- If possible, we will spend some time on coding theory as a 5<sup>th</sup> unit.

### **First homework assignment due Thursday January 10.**

1) Email me your answers to the following questions:

- What are you majoring in and why?
- What math courses have you taken so far at Redlands?
- Why are you taking this course? What do you hope to learn in it?
- Construct a metaphor for mathematics (as you see it). For example, if math were an animal what would it be? Explain why you chose your metaphor.
- Please tell me anything you think I should know about you, and/or anything you'd like to tell me about yourself.
- Is there anything you'd like to know about me?

2) Read Section 2.1 of Barr and do 2.1(1-6, 11-15).

3) BONUS Problem: Solve an online cryptogram at <http://teppo.tv/cryptogram/> or <http://www.cryptograms.org/>