MATH 1350: The Art of Secret Writing
Summer 2010

Instructor Information:
Corinne Sheridan
Email: csheridan@math.cornell.edu
Office: Malott 210
Office Hours: Monday 1:30 – 2:30 pm, Wednesday 9:30 – 10:30 am, and by appointment

TA Information:
Andrew Marshall
Email: alm255@cornell.edu
Office Hours: Malott 256, Tuesday 10-11 am, Thursday 1-2 pm, and by appointment

Course Information:
Class: MTWThF 11:30 – 12:45, Malott 206
Course Website: www.math.cornell.edu/~csheridan/Math1350.html
Extra Help: Math tutors available Sun - Thurs. in the Carol Tatkon Center Room 3343 from 7 - 9:30 pm.

Purpose of the Course:

In the "Art of Secret Writing", students will delve into the field of cryptology, the study of writing and breaking codes. Many students do not have the opportunity to see mathematics as something beyond algebra and calculus. This course allows them not only to learn mathematical principles but also to understand the concepts behind a topic that may have seemed mysterious before. As this course is independent of calculus and other college math courses, it is accessible to both non-majors and majors alike. In the first part of the course, we will examine some ciphers (code systems) used in the past, to begin to see the logic and reasoning behind a cipher. We will pair a cipher to the introduction of a mathematical principle that it uses to encode and decode messages. These principles will help us to understand the more current code systems being used today.

Course Description:

Math 1350 will investigate classical and current methods of message encryption and decryption, as well as analyze the strength of various cryptosystems. In examining the different methods, mathematical concepts such as modular arithmetic, matrix arithmetic, probability and number theory will be developed. The history and key figures in the field will also be discussed.

This course will require several years of high school mathematics, in particular algebra, and is an alternative to calculus to fulfill the math requirement for many majors. The course will meet for 75 minutes every day for six weeks.

Textbook:
Invitation to Cryptology, by Thomas H. Barr, Prentice Hall, 2002.

Supplementary texts (not required):
Cryptological mathematics, by R.E. Lewand, Mathematical Association of America, 2000.
(on reserve in the Math Library)
Introduction to cryptography, by J.A. Buchmann, Springer-Verlag, 2001.
(limited preview on Google Books)

Goals:

1. Build confidence in mathematical reasoning abilities.
2. Strengthen analytical thinking skills.
3. Improve mathematical communication skills.
4. Learn to work in pairs and groups to encourage and assist fellow students.

Learning Objectives

Upon completion of the course, students should be able to:

1. Discuss several types of classical cryptosystems and their different features.
2. Recognize and compute modular arithmetic.
3. Decode a shift cipher, a substitution cipher, and a Hill cipher.
4. Identify probabilistic principles and apply them to the cryptographic processes.
5. Explain the foundations of public-key cryptography.
6. Create a new cipher and encode a message.
7. Evaluate the strengths and weaknesses of fellow students' ciphers.

Format of Class and Expectations

Classes will be a combination of discussion, lecture, group activities, and class-wide activities. There will be weekly quizzes in class and weekly homework assignments. **Students are strongly encouraged to work on the homework assignments throughout the week, as this course is condensed from a semester-long course meeting two to three times a week, to a 6-week course meeting every day.** The material will be more difficult if you do not spend time every day on the homework assignment and reading.

I expect students to complete the reading and problem set assignments, participate in class, and show respect to their classmates and myself. The classroom will be treated as a learning environment, where questions and student contributions are encouraged and appreciated.

Grading and Assignments

Homework: Homework will be assigned almost every day but will be due every week on Tuesdays, except the first week. See this as a chance to get your hands dirty, to apply concepts to specific situations, and starting to apply principles on your own. Each homework assignment will be worth 50 points. You will be able to drop your lowest homework grade. Some problems will be graded for correctness, and you will also receive points for attempting all problems. NO LATE HOMEWORK WILL BE ACCEPTED. If you must miss class on a Friday, then you are responsible for getting your homework to me beforehand.

Quizzes: Quizzes will be given at the beginning of class every Wednesday, except for the first week, each worth 25 points. They will take about 15 minutes. Quizzes are a chance for you to attempt problems on your own in a timed setting. Quizzes will cover the material of the week that is on your homework problem sets. They will focus on the concepts, rather than computationally difficult problems. Some quizzes will be graded for correctness, some will be graded for effort (i.e. 25 points if you're there and try, 0 if you are absent) – I will not announce ahead of time which it will be. Again, you may drop your lowest quiz grade. Quizzes are a good opportunity for feedback between you and me. See them as a learning opportunity, rather than a stressful experience. NO MAKE UP QUIZZES WILL BE GIVEN.

Graded Activities: There will be a series of activities during the semester, two of which will be graded (see the weekly schedule). I will give out a rubric and specific instructions for each activity ahead of time.

Activity #1: Presenting Historical Ciphers
Activity #2: Create a new or Implement an existing cipher

Participation: Class will be highly participatory – I want you to be involved by asking questions, answering questions, working in pairs or groups as we have activities. Please ask questions! If you do not feel comfortable asking questions in class, email me ahead of time with your questions.

Midterm Exam: The midterm will cover the first half of the course, involving some concept-based questions and some computational questions. It will be given during class. You will not be allowed a calculator, computer, or any other aid.

Final Exam: The final exam WILL BE CUMULATIVE. It will be in the same style as the midterm exam with a balance of concept-based questions and computational questions.

Your grade will be determined out of 600 total points as follows:

Homework (6 at 30 points each, lowest dropped)	150 pts
Quizzes (5 at 25 points each, lowest dropped)	100 pts
Graded Activities (2 at 30 points each)	60 pts
Participation	60 pts
Midterm Exam	100 pts
Final Exam	130 pts

REMEMBER: No late homework will be accepted, and no make-up quizzes will be given. To allow for various circumstances, you will be able to drop your lowest homework grade and your lowest quiz grade.

Academic Integrity

You are allowed to collaborate on the homework, provided that it is done in a way that maximizes the benefit of the homework to all people involved. (One person simply telling another how to do a problem totally defeats the purpose of the problem.) You get maximum benefit from a homework problem if you work hard on it alone before combining your ideas with someone else's. In any case, the paper that you turn in with your name on it should represent your own solutions, written in your own words, regardless of whether you arrived at some of those solutions in collaboration with others.

In particular, you may not copy someone else's homework and turn it in as your own. This will be treated as a violation of Cornell's Academic Integrity Code (http://cuinfo.cornell.edu/Academic/AIC.html). Similarly, copying solutions that you might find on the internet or in some other source is illegal. Academic Integrity is expected also on all your exams.

Note to students with disabilities: It is Cornell policy to provide reasonable accommodations to students who have a documented disability (e.g., physical, learning, psychiatric, vision, hearing, or systemic) that may affect their ability to participate in course activities or to meet course requirements. Students with disabilities are encouraged to contact Student Disability Services and their instructors a confidential discussion of their individual need for academic accommodations. Student Disability Services is located in 420 CCC. Staff can be reached by calling 607.254.4545.

Course Schedule and Activities

Class	Topic	Read Before	In Class	HW – **YOU FILL IN**
6/28	Caesar Alphabet Wheels	N/A	Diagnostic Test	Problem Set 1
6/29	Functions, Definitions	1.2, 1.3		1.2 # 1, 2
6/30	Modular Arithmetic	2.1		
7/1	Shift Ciphers and Mod. Arith.		HW DUE	
7/2	Affine Ciphers	2.2		
7/5	NO CLASS			
7/6	(continued)		HW DUE	
7/7	Subsitution Ciphers	2.3	QUIZ	
7/8	(continued)			
7/9	Transposition Ciphers	2.4		
7/12	Polyalphabetic Subsitutions	2.5		
7/13	Probability and Expectation	2.6	HW DUE	
7/14	Discover Keyword Length	2.7	QUIZ, Activity	
7/15	Catch-up/review			
7/16	--		MIDTERM EXAM	
7/19	Analysis of Vigenere Cipher	2.8		
7/20	Hill Cipher and Matrices	2.9	HW DUE	
7/21	(continued)		QUIZ	
7/22	Shift and Block Ciphers	3.5		
7/23	Graded Activity	1.1	PRESENTATIONS	
7/26	Graded Activity		PRESENTATIONS	
7/27	Intro to Public-key Crypto	4.1	HW DUE	
7/28	Primes and Factorization	4.2	QUIZ	
7/29	Fermat's Little Theorem	4.3		
7/30	Special Topic	TBD		
8/2	Developing a Cryptosystem	5.1		
8/3	RSA Public-key Crypto	4.4	HW DUE	
8/4	(continued)		QUIZ	
8/5	Evaluate Each Other's Ciphers		CIPHERS DUE	
8/6	Special Topic 2	TBD		