Cornell University
Mathematics 135-The Art of Secret Writing

Section: 01
Lecture: MTWRF 10:00–11:15 a.m. in Malott Hall, room 206

Professor:	Michael Kozdron
Office:	543 Malott Hall
Phone:	255-3685
Email (Cornell):	kozdron@math.cornell.edu
Home Page (Cornell):	`http://www.math.cornell.edu/~kozdron/`
Email (Regina):	kozdron@math.uregina.ca
Home Page (Regina):	`http://stat.math.uregina.ca/~kozdron/`
Office Hours:	After class, or by appointment

Required Text:

- Thomas Barr, *Invitation to Cryptology*, Prentice Hall, 2002.

Optional Text:

- Simon Singh, *The Code Book*, Anchor Books, 1999.

Course Description:
3 credits. The course examines classical and modern methods of message encryption, decryption, and cryptoanalysis. We develop mathematical tools to describe these methods (modular arithmetic, probability, matrix arithmetic, number theory) and become acquainted with some of the fascinating history of the methods and people involved.

Prerequisites:
3 years of high school mathematics.

General Policies:
The policies on this page supplement those of the Cornell Summer Session. Students should note that "every summer registrant is considered a student and is subject to the general regulations governing student conduct that apply to all other students of the university." Students are expected to be familiar with the contents of the Campus Code of Conduct; for further information about student conduct, consult the Cornell Summer Session web page. Although this is a summer class, it is expected that the material covered in Math 135 remains consistent from semester to semester. For that reason, we will cover the same material as during the fall and spring sessions, and have a comparable final exam.

Grading Information:
Your final grade will be determined by your performance in the course, including class participation, homework, prelims, and the final exam.

Evaluation Type	Number	Percentage of Final Grade
Class Participation	-	5%
Homework	6	15%
Prelim Exams	2	40%
Final Exam	1	40%

Class Participation:
This catch-all category is intended to help encourage student participation in this class. There are three basic forms of "participation" which include: asking and answering questions in class, attending office hours, and contributing to classroom discussions. I will be available for extra help after most classes, and I strongly encourage you to stay around and ask questions if something is difficult. Periodically, there may also be short quizzes which will consist of one or two routine questions. The purpose of the quizzes is to ensure that the students are mastering the absolute basics of the course, and are attempting to keep up with the material. Quizzes will always be announced in advance.

Homework:
As is the norm in a university course, it is not possible to cover all of the required material in lecture. As a result, each student must take an active role in his or her own education. Mathematics (and especially cryptography) is not a spectator sport. It cannot be learned passively only by watching the instructor lecture. Instead it must be learned by doing. Consequently, most of what you learn in this course will be the result of working exercises that are designed to reinforce key concepts, develop skills, and test your understanding of the material. Before you try working the exercises, however, do the reading assignment. Reading the text will help you review the important concepts before you start on the exercises. Some of the exercises are straightforward, others are very complex. After each class meeting, you should work all problems assigned from the section discussed that class. It is expected that students are spending 2–4 hours per day reviewing material and doing homework. You are encouraged to talk with your classmates about the homework; you might even want to form a study group to work together on the most difficult homework problems. However, all problems you submit must be your own work. ***It is dishonest, and a violation of Cornell's Code of Academic Integrity, to submit someone else's work as your own.***

Prelim Exams:
There will be two major term tests, known at Cornell as Prelim Exams, that will be given during the semester. All prelims will be closed-book, and no aids will be allowed. Each prelim will be a comprehensive test of all of the material covered on the syllabus before that prelim, including lectures, assigned readings, and homework assignments.

Final Exam:
As with the prelims, the final exam will be closed-book and no aids will be allowed. The final exam will be comprehensive and cover all of the material listed on the syllabus.

Exam Dates:
The prelims will take place during the regular class time on the dates listed below. The final exam will take place in our usual classroom at a time scheduled by the Summer Session registrar.

- Prelim 1: **Monday, July 10, 2006, 10:00–11:15 a.m.**
- Prelim 2: **Monday, July 24, 2006, 10:00–11:15 a.m.**
- Final Exam: **Tuesday, August 8, 2006, 8:00–10:30 a.m.**

It is possible that these dates may include Religious Holidays for some students. NYS Education Law section 224-A mandates that faculty make available an opportunity to make up any examination missed because of religious beliefs. In order to facilitate preparation of makeup exams, I request that students intending to be absent in order to observe a religious holiday notify me by June 30, 2006.

Policy for Missed Classes, Missed Prelims, and Missed Final Exam:
Students should familiarize themselves with the section on Class Attendance, Meeting Times, and Examinations on pages 14–15 of *2005–2006 Courses of Study*.

Web Site:
I have written a web site for this section. The URL is

`http://www.math.cornell.edu/~kozdron/Teaching/Cornell/135Summer06/` (Cornell)
`http://stat.math.uregina.ca/~kozdron/Teaching/Cornell/135Summer06/` (Regina).

I will be updating this site throughout the term and you will be able to download any handouts that you don't get in class. I've included information about the course, the textbooks, and calculus in general.

Email:
Email will be a significant form of course related communication between both students and the instructor. Therefore, please check your email regularly for course updates and homework/prelim information. Feel free to email your questions to me. I will endeavour to respond within 24 hours. Should you not receive a reply within 24 hours, try sending the message again, or ask me in person if I received your mail.

Academic Integrity:
For a university community of scholars, academic integrity is the heart of intellectual life—both in learning and in research, to paraphrase the section on Academic Integrity in Arts and Sciences on page 431 of *2005–2006 Courses of Study*. Students should read carefully Cornell's Code of Academic Integrity and not assume they understand what integrity and cheating are and are not. Academic integrity most certainly implies more at the university than it did in high school. The standards of integrity are those that prevail in professional life. Students must acknowledge and cite ideas they adopt from others (not just direct quotations), and understand the general standards and policies of academic integrity, as well as specific expectations in individual courses. When in doubt, ask!

Therefore, students are expected to abide by Cornell University policies, including the campus Code of Conduct and the Code of Academic Integrity, as described in the *Policy Notebook*, and should pay particular attention to §I.C of the Code of Academic Integrity.