University of Regina
Mathematics 124–The Art and Science of Secret Writing

Section: 001
Lecture: TuTh 1300–1415 in Campion College Building, Auditorium (CM AUD).

Professor: Michael Kozdron
Office: College West 307.31
Phone (Office): 585-4885
Email: kozdron@stat.math.uregina.ca
Home Page: `http://stat.math.uregina.ca/∼kozdron/Teaching/Regina/124Winter09/`
Office Hours: TBA.

Required Texts:

- Thomas Barr, *Invitation to Cryptology*, Prentice Hall, 2002.
- Simon Singh, *The Code Book*, Anchor Books, 1999.

Course Description:

3 credits. The course examines methods of message encryption and cryptoanalysis. Attention will be given to the history of cryptology and the public-policy questions raised by its use in conjunction with the Internet. However, the focus will be on the mathematical tools needed to develop and analyze encryption algorithms. ***Prerequisite: Mathematics B30.

Student Responsibilities:

Students should familiarize themselves with both the *Responsibilities of Students* in Section 5.1 and the *Responsibilities of Instructors* in Section 5.2 of the *Undergraduate Calendar*. Especially note item 7 which states that: Instructors are expected to conduct their courses in such a way as to obtain evidence of student writing skills, in term papers, essays, reports, or other written work, and to demand competence in writing for a passing grade

Keeping Up-to-Date:

This is an introductory course on the mathematical techniques of both current and historical cryptography. The purpose of the class is to introduce students to some rather advanced mathematics in a meaningful, relevant, and contemporary way. Consequently, it is vital that students read the appropriate textbook sections before and after each lecture, and attempt the relevant homework problems. A glance at the syllabus will reveal that there will be a lively pace kept. Keeping up-to-date with the material is essential!

Grading Information:

Your final grade will be determined by your performance in the course, including assignments, the midterm, and the final exam. Students should consult *Grading Descriptions* in Section 5.9.1 of the *Undergraduate Calendar* for an outline of the expectations associated with various percentage grades.

Evaluation Type	**Number**	**Percentage of Final Grade**
Assignments	6	18%
Midterm Exam	1	32%
Final Exam	1	50%

Policy for Missed Classes, Missed Midterm, and Missed Final Exam:
Students are expected to attend every class. Multiple unexplained absences will not be tolerated. Students should familiarize themselves with the section *Deferrals* (Section 5.7) of the *Undergraduate Calendar.*

Assignments:
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 5–10 hours per week 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 serious University of Regina violation, to submit someone else's work as your own.***

Assignment Due Dates:
Assignments will be due at the beginning of class on the dates specified. No late assignments will be accepted. All assignments must be stapled, and your must not be crowded nor written in multiple columns.

- Assignment #1 due on Thursday, January 15, 2009
- Assignment #2 due on Thursday, January 29, 2009
- Assignment #3 due on Thursday, February 12, 2009
- Assignment #4 due on Thursday, March 5, 2009
- Assignment #5 due on Thursday, March 12, 2009
- Assignment #6 due on Tuesday, April 7, 2009

Midterm Exam:
There will be one major midterm exam that will be given during the semester. The midterm will be closed-book. The exam will be comprehensive, and cover all the material listed on the syllabus before that midterm, including lectures, assigned readings, and assignments.

Final Exam:
As with the midterm exam, the final exam will be closed-book. The final exam will be comprehensive and cover all of the material listed on the syllabus, including both lecture work and assigned readings.

Exam Dates:
The midterm will be held in class during the usual class time, and the location of the final exam will be determined by the Registrar near the end of the term.

- Midterm Exam: **Thursday, March 19, 2009, 1300–1415**
- Final Exam: **Tuesday, April 21, 2009, 1400–1700**

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

`http://stat.math.uregina.ca/~kozdron/Teaching/Regina/124Winter09/`

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.

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/midterm 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.

Students should read carefully the University of Regina guidelines on *Student Behaviour* in Section 5.13 of the *Undergraduate Calendar*, 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!

Students should also consult the pamphlet *Academic Integrity* published by the University Secretary, or contact that office for more information.