Math 4440/5440: The Mathematics of Coding and Cryptography Fall 2006

General Info

Instructor: Professor David Grant, grant@boulder.colorado.edu

Office Hours: M 1-1:50, W 2-2:50, F 10-10:50 (or by appointment), in Math 303 (x2–7208).

Class Meetings: MWF 11–11:50 PM in ECCR 131.

Text: W. Trappe and L. Washington, *An Introduction to Cryptography with Coding Theory, Second Edition.* (Prentice-Hall)

Prerequisites. Linear Algebra.

About the course.

Two of the major problems in computer science or electrical engineering involve data transmission. They are: I) Making sure that someone can understand the message you send; and II) Making sure that they can not.

Problem (I) is the problem of coding. When transmitting a stream of zeros and ones, some errors may occur, reversing a zero to a one and visa versa. This can happen due to human error in transmission, or noise over a channel through which the message is sent. These errors occur with a certain probability, so our goal will be to build enough redundancy into our message that the receiver can detect or correct a certain percentage of errors. On the other hand, we do not want to build in too much redundancy, for then we would be wasting valuable bandwidth.

Problem (II) is the problem of cryptography. People can intercept messages, so the sender wants to make sure that only the intended receiver can understand the message. This could be done with both transmitter and receiver having a secret code book, but it's impractical for a bank to have a secret code set up with each of 20 million customers! So we will focus on so-called public key cryptography, whereby the method for encrypting a message is public knowledge, yet with high probability, it is only the receiver who knows how to decrypt the message.

Both the problems turn out to be very mathematical. Fortunately, the mathematics involved in elementary coding and cryptography — algebra and number theory — are old and well-developed branches of mathematics. Unfortunately, it is not easy for a student interested in coding and cryptography to learn this requisite mathematics!

So the goals of the course are to help computer science and electrical engineering students learn the necessary mathematics to study these fields in more depth (and continue on to courses like ECEN 5682 and CSCI 6268), while at the same time teaching math students some of the beautiful applications of algebra and number theory. Indeed, I believe that the theory not only helps people understand the applications, but the applications help people understand the theory.

Course requirements and grading.

This course will meet three days a week. Homework will be assigned weekly, and will due the following Monday. (Graduate) Students enrolled in the 5440 version of the course will be given additional exercises, usually of a more abstract mathematical nature. There

will be two hour exams during our regular class time and in our usual room. The first will be on September 29 (so you can get feedback before the drop deadline) and the second will be on Nov. 3. There will be a take-home final, due at the end of our regularly scheduled final exam time, 1 p.m. on Dec. 19. Your final grade in this course will be determined by your total score out of 600 possible points. These points are broken down as follows: Homeworks count for a total of 200 points, the two hour exams will each be worth 100 points, and the final exam will make up the remaining 200 points. The final will, unlike the hour exams, be cumulative, with an emphasis on the material covered after the second exam.

Et Cetera:

The last day to drop a course without fee or a "W" on your transcript is Sept. 13. Also note that the last day to drop a course without petitioning the dean is Oct. 11.

Please inform me as soon as possible should you need, due to your observance of a religious holiday, to miss an exam, homework, or class. Provided you notify me well in advance, every effort will be made to reach a reasonable accommodation.

If you qualify for accommodations because of a disability, please submit to me a letter from Disability Services in a timely manner so that your needs may be addressed. Disability Services determines accommodations based on documented disabilities. (303-492-8671, Willard 322, www.Colorado.EDU/ disabilityservices)

The University has an honor code (http://www.colorado.edu/academics/honorcode/). I will expect each student to affix the pledge of the honor code to each exam.

The University of Colorado at Boulder policy on Discrimination and Harassment can be found at http://www.colorado.edu/policies/discrimination.html.

Topical outline of the course:

We will cover the introductory Chapter 1, and spend some time on the Classical Cryptosystems of Chapter 2. We will cover Chapter 3, on number theory and finite fields in detail (this is the mathematics we need for the course). We will do all of Chapter 6 and 7 on the RSA and discrete log cryptosystems, and discuss part of Chapter 9 on digital signatures. We will then cover the long Chapter 18 on coding theory in detail.

Further reading and resources

Cryptography (non-mathematical): The Code Book, S. Singh; The Codebreakers, D. Kahn.

Cryptography (mathematical): Cryptography, Theory and Practice, D. Stinson; Introduction to Cryptography, J. Buchmann; A Course in Number Theory and Cryptography, N. Koblitz; Algebraic Aspects of Cryptography, N. Koblitz.

Coding: A First Course in Coding Theory, R. Hill; Elements of Algebraic Coding Theory, L. Vermani; Introduction to Coding Theory, J. H. van Lint;

Number Theory: A Friendly Introduction to Number Theory, J. Silverman; The Theory of Numbers, G. H. Hardy and E. M. Wright; A Classical Introduction to Modern Number Theory, K. Ireland and M. Rosen.

Algebra: A First Course in Abstract Algebra, J. Fraleigh; Topics in Algebra, I. Herstein; Basic Algebra, I. II., N. Jacobson.