MATH/CS/ECE 435 SYLLABUS, Spring Semester, 2004-05 Academic Year
Lec. 1, TR 9:30 – 10:45 PM, B105 Van Vleck Hall

Prof. Richard A. Brualdi
Office: 725 Van Vleck Hall

Text is:
Intro. to Cryptography
2th ed., by J.A. Buchmann

Tel: 262-3298; E-mail: brualdi@math.wisc.edu
Office Hours: Mon (1:15–2:15), Tues. (3:30–4:30 PM), Thur. (2:30–3:30 PM)
WWW: http://www.math.wisc.edu/~brualdi

I have an email distribution list by which I can communicate to the class.

Please read carefully

Course Content: As the course title *Introduction to Cryptography* suggests, Math/CS/ECE 435 is a first course on the fundamentals of, and the mathematics behind, secure communication. *Cryptography* generally refers to methods to encrypt messages for secure communication, while *cryptanalysis* refers to the science of attacking, and finding weaknesses in, methods used to encrypt messages. While we shall be concerned with both aspects, that is, with

$$\{\text{cryptology}\} = \{\text{cryptography}\} \cup \{\text{cryptanalysis,}\}$$

we will be more concerned with methods of encryption.

We will cover both classical and modern cryptography and cryptanalysis. The classical systems, including substitution ciphers, affine ciphers, the Vigenère cipher, and Feistel ciphers, use elementary mathematics for their construction; analyses to attack and decrypt also use elementary mathematics including some aspects of probability and statistics. DES (Data Encryption Standard), adopted by NBS/NIST in 1977, is based on classical methods and has now been replaced by AES (Advanced Encryption Standard), as a result of an international competition organized by NIST. The winner of this competition was Rijndael ("Rhine Dahl"), now called AES, devised by two Belgian cryptographers. We shall develop the necessary background to understand both DES and AES. Modern cryptographic systems (public-key systems), such as RSA and El-Gamal, are heavily mathematical, employing such mathematical tools as modular arithmetic, prime number theory, factorization theory, group theory, field theory, ...). As a result we will have to spend considerable time on the underlying mathematics. We will also discuss various cryptographic protocols, pseudo-random numbers, digital signatures, identification, etc.

Class and Exercises I will try to cover as much of the book as time permits.:

First half of the semester: Chapters 1, 2, 3, 4/5

IN-CLASS EXAM

Second half of the semester: Chapters 5/6, 7, 8, a little of Chapters 9 and 10, 11, 12, 13, 14, 15.

Exercises Assigned exercises will be emailed to you after each chapter is covered. There will be two kinds of exercises: (1) some to practice on and check your answers (after you've done them!) with those given in the back of the book and (2) some to be handed in (after we finish each chapter) for marking. It is essential that you do both kinds of exercises with the not-to-be-handed-in exercises completed **before** you do the to-be-handed-in exercises. The assignments to be handed-in will have a **due date in class**; no late assignments will be accepted. Your work on these exercises should be well-presented in good English, and not written carelessly. While you can discuss the exercises with classmates, **the work you hand in should be your own write-up and not copied from someone else.** The assigned homework will be scaled to 100 points.

Attendance: It is expected that each student will be present at all of the classes. Office hours are for students who need additional help beyond that given in the class; office hours are not substitutes for class. The class and the book will reinforce each other. We will be covering many pages in the book. In the class lectures, you will learn what emphasis I am placing on the various topics in the course, and this should inform you on how to study what is in the book. The assigned exercises also give an indication of the emphasis in the course.

Exams and Grades

In-class, mid-term Exam on Thursday, March 10 worth 100 points.

Final Exam on Wednesday, May 11, 2005 at 12:25 PM worth 150 points

There will be no make-up exams (so check your schedule now).

Grades will be based on the exercises, mid-term and final; maximum number of points is $100 + 100 + 150 = 350$.

Other references of possible interest:

1. *Crypto* by Steven Levy, Viking Press, 2001.

2. *Newsweek*, January 15, 2001 (excerpt from above book).

3. *Elementary Cryptanalysis*, by A. Sinkov, Math. Assoc. America, 1964.
4. *Cryptography, Theory and Practice*, by D. Stinson, CRC Press, 1995.
5. *Cipher Systems*, by H. Beker and F. Piper, Northwood Books, 1982.
6. *Invitation to Cryptology*, by T.H. Barr, Prentice Hall 2002.
7. *Introduction to Cryptography*, by H. Delfs and H. Knebl, Springer 2002.
8. *The Codebreakers*, by D. Kahn, Scribner, 2001 rev. ed.
9. Two articles in the *Notices of the Amer. Math. Society*, by S. Landau, vol. 47. no. 3, 341-9, and vol. 47, no. 4, 450-9, 2000.

Other Information

Note to McBurney Disability Resource Center students: Students of the Center who are recommended for some accommodation (e.g., extended time on exams) should contact the instructor about this no later than January 30.

The Department of Mathematics; Van Vleck Hall (VV):

Chair: D. Griffeath (219 VV)

Associate Chair: J. Robbin (313 VV)

Department Administrator: V. Whelan (223 VV)

Undergraduate Advisor: G. Mari-Beffa (309 VV)

TA Supervisor: P. Milewski (809 VV)

Undergraduate Secretary: J. Schwantz (207 VV)

Sexual Harrassment Contact Persons: G. Mari-Beffa (309 VV), D. Rivard (720 VV)

Access and Accomodation Coordinators: J. Robbin (313 VV)

Faculty Minority Liaison: D. Camacho (321 VV) [Information available concerning diversity and multicultural issues (e.g. support services, academic internships and grants/fellowships). Dr. Camacho is also available to discuss minority students' concerns about mathematics courses: 263-3603, camacho@math.wisc.edu)]