MATH/CS/ECE 435 SYLLABUS, Spring Semester, 2000-01 Academic Year
Lec. 1, MWF 11:00-11:50 a.m, B139 Van Vleck

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

Text is:
Making, Breaking Codes: An Introduction to Cryptography
by Paul Garrett

Tel: 262-3298; E-mail: brualdi@math.wisc.edu; www: http://www.math.wisc.edu/~brualdi

Office Hours: Tuesday (3:00-4:30 p.m.), Wednesday (2:25-3:15 p.m), Friday (9:55-10:45 a.m.)

Course Prerequisite: Math 340 (Linear algebra)

Through DoIT I have created an email list for this course through which I can communicate with you over the Internet.

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. We shall be concerned with both aspects, that is, with *cryptology*:

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

We will cover both classical and modern cryptography and cryptanalysis. The classical systems, including substitution ciphers, affine ciphers, the Vigenere 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 is soon to be replaced by AES (Advanced Encryption Standard), which has recently been chosen (the announced winner is Rijndael ("Rhine Dahl") devised by two Belgian cryptographers). We shall develop the necessary background to understand both DES and AES. Modern cryptographic systems (public-key systems) 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 sequences (feedback shift registers), ...

Class, Exercises, Exams and Grades This is the first time I have taught this course, and so the first time I have used the book by Garrett. As a result it is difficult at this time to give precise information about what parts of the book will be covered on a daily basis. But here is a rough outline:

Chapter 1 Simple Ciphers - 3 days
Chapter 2 Probability - 3 days
Chapter 3 Permutations - 3 days

Chapter 4 A Serious Cipher - 4 days
Chapter 5 More Probability - 1 day
Chapter 6 Modern Symmetric Ciphers - 4 days
Chapter 7 The Integers - 3 days
Chapter 8 The Hill Cipher - 1 day
Chapter 9 Complexity - 1 day
Chapter 10 Public-key Ciphers - 6 days
Chapter 16 Pseudoprimes - 2 days
Chapter 18 Sketches of Protocols - 3 days
Chapter 21 Random Number Generators - 4 days

I will also be referring to some sections of the other chapters in conjunction with the material in the chapters above. Also there may be an occasional handout.

There will be two kinds of **Exercises**:

(A) Those to do and check your answers (after you've done them!) with those given in the back of the book. I have given you a minimal list of exercises; there are many other similar exercises in the book that you can choose to do. These exercises are to help you learn the material, reinforce the new concepts, and develop technique in problem-solving. Here working with one or more fellow students can be helpful. If you don't do these exercises, then when it comes time for the in-class exams, you won't have the experience and facility to complete the exams in the alloted time.

(B) Five exercise sets, two before spring break and three after, to be handed in and graded. These exercise sets will have a due date **in class**; no late assignments will be accepted. Please leave them on the desk as you enter the classroom on the due date. Your work on these exercises should be well-presented in good English, and not written carelessly. **Write them as if they were part of your resume for a high-paying job you really want!** It is important that you do both kinds of exercises with the exercises (A) from a given chapter completed **before** you do exercises (B) from that same chapter. The five exercise sets (B) will be equivalent to one in-class examination and thus will be scaled to **100 points**.

The assigned exercises (A) and (B) will be emailed you using the email distribution list.

There will be **one mid-term, in-class Exam** (**worth 100 points**) and a **final exam** (**worth 150 points**):

Mid-term Exam, in class on Wednesday, March 7.

Final Exam on Sunday, May 13, 2:45-4:45 p.m., place to be scheduled by the university.

There will be no make-up exams. Thus the total number of points you can earn is 350, and your grade will be based on these points.

Attendance: It is expected that each student will be present at all of the classes. It is rude and disruptive to both me and your fellow students to leave a class before the bell has sounded or I have dismissed the class for the day. 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.

Other Information

Note to McBurney Disability Resource Center students: Students of the Center who are recommended for some accomodation (e.g., extended time on exams) should contact the instructor about this no later than January 29.

The Department of Mathematics:

Chair: A. Adem (219 Van Vleck)

Associate Chair: D. Uhlenbrock (421 Van Vleck)

Department Administrator: G. Novara (223 Van Vleck)

Undergraduate Advisor: D. Shea (316 Van Vleck)

TA Supervisor: R. Wilson (411 Van Vleck)

Undergraduate Secretary: P. Conklin (203 Van Vleck)

Sexual Harrassment Contact Persons: G. Benkart (817 Van Vleck), D. Uhlenbrock (421 Van Vleck)

Access and Accomodation Coordinators: C. Rider (321 Van Vleck), D. Uhlenbrock (421 Van Vleck)

Faculty Minority Liaison: D. Rider (821 Van Vleck) [Information available concerning diversity and multicultural issues (e.g. support services, academic internships and grants/fellowships). Prof. Rider is also available to discuss minority students' concerns about mathematics courses: 263-3603, drider@math.wisc.edu)]