SYLLABUS

Cryptography, Spring, 2002

Instructor: James A. Davis
206 Jepson Hall
289-8094
jdavis@richmond.edu
http://www.mathcs.urich.edu/ jad

Office hours: W 9–10, 2–3; TR 10-11
or by appointment

I. COURSE DESCRIPTION:

"The fundamental objective of cryptography is to enable two people, usually referred to as Alice and Bob, to communicate over an insecure channel in such a way that an opponent, Oscar, cannot understand what is being said." This quote is the first sentence in our text, *Cryptography Theory and Practice* by Douglas Stinson, and it encapsulates our objectives for this course. We want to study the mathematics used to construct communication systems, and we also want to study the mathematics used to break these systems. We will analyze cryptosystems that have been used in the past, and we will study systems that are being used today.

In addition to our text, there are numerous other references that you might want to use as we go through the course. We will refer to popular books such as *The Code Book* by Simon Singh and *The Emperor's Code* by Michael Smith. We will do at least one unit on Elliptic Curve Cryptography using an unpublished manuscript by Nigel Smart of the University of Bristol. Our library has a small collection of Cryptography books. The explosion of electronic commerce over the past decade has generated enormous interest in how to keep transactions secure from criminals, and this has led to a vast literature on this subject.

One of the major tasks for you to accomplish this semester is a research project on a topic of your choosing. This project will include a written report as well as an in-class presentation. Details will be provided in early February.

II. GRADING:

Two hour exams (100 pts each)	200 pts
Exam dates: 2/7 3/14	
Homework grade	200 pts
You will turn in weekly homework assignments	
Project	200 pts
You will work on a project, culminating in a paper and a 20 minute presentation to class	
Final Exam (Thurs April 25, 9–12)	200 pts
TOTAL	800 pts

(NOTE: You can get 10 bonus points for attending a lecture sponsored by the math and computer science department, up to two lectures)

III. ATTENDANCE:

Attendance is expected. You are responsible for making up any work you miss if you are not in class. I reserve the right to punish serious abuse of privileges (I will warn you before I do so).

IV. ACADEMIC HONESTY:

All work on tests must be your own. The following 2 statements explain the position of the University on computer plagiarism, and they should be used as a guide to your computer work.

a. Any original work stored on a floppy disk or other data storage device is the property of the author; anyone else who presents all or part of such work as his or her own, with or without the permission of the author, shall be deemed guilty of plagiarism.

b. Anyone who gains unauthorized access to computer files stored by someone else shall be guilty of vandalism, whether or not the files are altered.