Syllabus

Instructor
Alan T. Sherman (login name: sherman@cs.umbc.edu)
Computer Science Department
ECS Building, Room 225J
Tele. (410) 455–2666 [direct], 455–3000 [department secretary]

Office hours: Monday–Thursday, immediately after class, and by appointment. On Tuesday and Thursday, my class ends at 3:45pm in CP210.

Teaching Assistant
None at this time.

Meeting Time and Place
Monday and Wednesday 4:00pm–5:15pm
MP (Math/Psychology) 101

Prerequisites
The formal prerequisites are CMSC-203: Discrete Structures, and Math-221: Introduction to Linear Algebra. CMSC-203 and Math-221 are required because the study of cryptography involves a substantial amount of mathematics, especially discrete mathematics. In addition, students are expected to be able to program in some high-level programming language (please note that the prerequisites for CMSC-203 include a programming course.)

Brief Course Description
Introduction to cryptology, the science of making and breaking codes and ciphers. Topics will include the following. Conventional and public-key cryptosystems, including DES, RSA, shift register systems, the Enigma, and selected classical systems. Examples of cryptanalytic techniques. Digital signatures, pseudo-random number generation, randomized encryption, cryptographic protocols, and their applications. Theories of cryptographic strength based on information theory and complexity theory.

This course has three major goals: 1) To understand and to be able to apply fundamental concepts of communications security. 2) To become familiar with and to understand the properties of selected cryptographic systems. 3) Given any cryptosystem, to be able to analyze its cryptographic strength. In addition, this course aims to sharpen your problem-solving skills and to improve your ability to express your ideas clearly and precisely in mathematical prose.

Texts

The following two texts are required; these books are available at the UMBC bookstore.

- Denning, Dorothy E. R., *Cryptography and Data Security*, Addison-Wesley (Reading, MA, 1983). [We will cover Chapters 1–3.]
- Sinkov, Abraham, *Elementary Cryptanalysis: A Mathematical Approach*, The Mathematical Association of America, New Mathematical Library no. 22 (1966). [We will cover the entire book, which deals exclusively with classical ciphers.]

Additional books on cryptology and related topics are on reserve at the UMBC Library (see the handout "Supplemental reading"). Assigned readings will be drawn from the required texts and from handouts to be distributed in class. We will also use a few selected draft chapters from a forthcoming book by Douglas Stinson.

Required Work and Expectations

Required work consists of weekly homework, weekly 10-minute quizzes, two 75-minute in-class exams, and a 2-hour in-class final exam. In addition, each student is expected to participate actively in class. The accompanying schedule lists the due dates for each of these activities.

Each homework assignment consists of required readings and problems to be solved in writing; some assignments will require computer programming. Solving problems is the best way to learn the course material; consequently, the homework is the most important activity of the course. Homework is due at the beginning of class on Wednesday, and no homework is assigned during the week of any exam.

Students are encouraged to work together on homework, but each solution and computer program must be written up individually. Plagiarism will be dealt with severely. For guidelines and advice on how to do the homework, see the handouts "Homework policy" and "How to solve and write up homework." You are expected to be familiar with the University policies on academic misconduct. If you are not familiar with these policies, please contact the Advisement Center or the Dean for Student Academic Affairs to obtain a copy of these policies.

Each quiz and exam is a written, closed-book in-class test. These tests are learning experiences which enable you to demonstrate what you can do. As indicated on the schedule, on most Mondays there will be a quiz, which will take place at the beginning of class. Immediately following each quiz, the instructor will go over the solution to the quiz. Through practice and through providing immediate feedback, each quiz is intended to enhance your understanding and to sharpen your problem-solving skills. Each quiz will emphasize material covered during the previous week.

Each student is expected to spend a total of approximately 10 hours per week on this course, roughly allocated as follows: attending lectures–3 hours, reviewing lecture notes–30 minutes, doing assigned reading–2:25 hours, doing written homework (or studying for exams)–4 hours, and seeking individual help from the instructor or TA–5 minutes.

Grading Policy

At the end of the semester, each student will receive a term grade as a measure of his or her performance on the course activities. These grades will be determined as follows. For each course activity, the student will receive an activity score. A term score will be computed as the weighted sum of the activity scores, using the relative weights given in Table 1. The instructor will convert term scores into letter grades by partitioning the sorted list of term scores for the entire class. This partition will be drawn primarily on the basis of absolute performance, without any predetermined cutoff points. The instructor reserves the right to make minor adjustments to the partition based on individual circumstances.

Late homework will not be accepted.[1] Quizzes cannot be made up and students will receive a 0 on each missed quiz. The lowest quiz score will be dropped.

Incomplete grades will be issued only under those extreme situations described by University policy for granting incompletes. Failure to complete assignments on time is not a sufficient reason for an incomplete.

In addition, the following grading rules will be applied. To pass the course, the student must make a serious attempt to complete each of the following activities: written homework, exams I–II, and final exam. In particular, each student is expected to make a serious attempt to solve every homework problem; any student who does not make a serious attempt to solve at least 60% of the homework assignments will not pass. To earn an 'A' it is necessary to make a serious attempt to solve all homework problems.

	Activity	Weight
1.	Class participation	2%
2.	Written homework*	33%
3.	Quizzes	10%
4.	Exam I*	15%
5.	Exam II*	15%
6.	Final exam*	25%
	Total:	100%

*To pass the course, it is necessary to make a serious attempt to complete this activity.

Table 1: Course activities and their relative weights.

Computational Facilities

All computer work will be done on the UMBC8 computer, which is a Silicon Graphics Crimson running the Ultrix operating system. For programming assignments, students must use the C or C++ prgramming languages. Students are encouraged to use the Gnu Emacs text editor, and to become familiar with Maple and xmosic.

[1] The main reasons for this policy are to enable the instructor to comment on the homework in class on the day it is due and to enable the instructor or TA to grade all solutions for each assignment in one sitting.