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 Monday and Wednesday, my class ends at 5:15pm in MP101.

Teaching Assistant

None to date.

Meeting Time and Place

Tuesday and Thursday 2:30–3:45pm
CP (Chemistry/Physics) 210.

Prerequisites

The formal prerequisites are Math–221 (Linear Algebra) and CMSC–441 (Algorithms) and CMSC–603 (Discrete Mathematics), or permission of instructor. Please note that this course requires a significant amount of discrete mathematics. Students are expected to be able to acquire the mathematics they need along the way.

Brief Course Description

Graduate introduction to cryptology, the science of making and breaking codes and ciphers. Topics will be drawn from the following. Conventional and public-key cryptography. Modern cryptosystems: DES, RSA, knapsack systems, shift registers. Examples of cryptanalytic techniques, including differential cryptanalysis. Digital signatures, including NIST's new DSA. Pseudo-random number generation. Randomized encryption. Cryptographic protocols, including the Diffie-Helman key exchange. Information-theoretic and computational complexity-based definitions of cryptographic strength. Zero-knowledge complexity. Quantum cryptography. Historical cryptosystems: Enigma, Hagelin, and selected hand ciphers. Electronic money and applications of cryptography to computer transactions.

This semester, CMSC-652 will be run primarily as a seminar course in which students will present seminal research papers from journals and conferences.

Texts
Required readings will be drawn from papers to be distributed in class and from the following text.

1. Rhee, Man Young, *Cryptography and Secure Communications*, McGraw-Hill (Singapore, 1994). [Current CMSC-652 text]

Additional books on cryptology are on reserve at the UMBC Library (see handout "Supplemental Reading"). We will also use a few selected draft chapters from a forthcoming book by Douglas Stinson.

Required Work
Required work consists of presenting one or two research papers, written assignments associated with these readings, and active class participation. In addition, each student is encouraged to undertake an optional individual research project. Each student is expected to make a serious attempt to understand all presented papers thoroughly. Skimming a paper the night before class is not sufficient effort to pass the course. There will be no examinations.

For each paper presented, the presenter must prepare one written assignment that will help the other students understand the paper. The assignment should be quantitative, challenging, doable, original, thoughtful, and focused. For example, the assignment might be to solve a special case of a problem or to extend the paper in some way. The presenter must also correct the solutions to the problem and distribute a model solution. Students are encouraged to work together, but each solution must be written up individually.

Each student is expected to spend a total of approximately 12 hours per week on this course, roughly allocated as follows: 3 hours attending lectures, 30 minutes reviewing lecture notes, 2:25 hours doing assigned reading, 6 hours doing written assignments, and 5 minutes seeking individual help from instructor or TA.

Grading
Assigned as measures of performance, term grades will be weighted as shown in Figure 1. In addition, the following grading rules will be applied. To pass the course, the student must make a serious attempt to complete all major activities, including class participation, written assignments, and paper presentations. In particular, each student is expected to make a serious attempt to solve every required homework problem. Late work will not be accepted.

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.

Computing Facilities
Each student should obtain a named account on the UMBC8 computer, which runs the Irix operating system. Students are encouraged to use the C or C++ programming language, the Gnu Emacs text editor, and the LaTeX document preparation system. Academic Computing Services offers introductory courses on a variety of topics that may help you use the UMBC computers more effectively.

	Activity	Weight
1.	Class participation	10%
2.	Written assignments	40%
3.	Paper presentations	50%
	Total:	100%

Figure 1: Course activities and their weights.

Academic Misconduct

Each student is expected to be familiar with all University and Department policies on academic misconduct. An egregious type of academic misconduct is plagiarism, which in each of its many forms involves representing somebody else's work as your own. Violations of academic honesty will be dealt with severely.