**Course Information**
CMSC-652 Cryptology, Section 101, Alan T. Sherman, Spring 2009, UMBC

**Instructor**
Alan T. Sherman, Ph.D, Associate Professor, Computer Science
Department of Computer Science and Electrical Engineering (CSEE)
URL to home page: www.csee.umbc.edu/~sherman
Office Hours: Wednesday, 9–10am, ITE 224, and by appointment, while classes are in session
Tele: 410-455-2666
Physical Mail Box: in CSEE Suite, ITE Third Floor
Email: sherman@umbc.edu Send email only to this address, and include “652” in the subject header.

**Teaching Assistant - None**

**Meeting Time and Place**
Monday, Wednesday, and Friday 10–10:50am, ACIV 013

**Text (required)**

**Course Description**
Introduction to research in cryptology, the art and science of making and breaking codes and ciphers. Each student will read and present recent papers in cryptology and carry out his or her own original research project. Topics will include block ciphers, stream ciphers, public-key cryptography, modes of operation, key management, digital signatures, message authentication codes, cryptographic hash functions, secret sharing, steganography, electronic cash, electronic voting, quantum cryptography, cryptography on elliptic curves, protocols, differential cryptanalysis, physical security, cryptocomplexity, and applications of cryptography.

**Prerequisites**
CMSC-441 Algorithms and math 221, or consent of instructor. Students from related fields are welcome, including students from Information Systems and Mathematics.

**Objectives**
At the end of this course, each student should be able to: (1) Be familiar with a broad range of research topics in cryptology. (2) Select and apply cryptographic primitives appropriately for security applications. (3) Design and analyze secure usable information systems. (3) Read and present research papers on cryptology, and carry out new and significant research projects of his or her own.

**Required Work**
Each student will present recent research papers, carry out and present an original research project of their own (or in a small group), and participate actively in class. In addition, there will be some written assignments, including weekly questions to be answered about presented papers. All requirements will follow the standard expectations of professional researchers in computer science, including the grant proposal process, writing technical reports, making conference presentations, and reviewing research manuscripts. All papers to be presented and project proposals must be approved by the instructor. Each project must be focused attempt at making a new and significant contribution to the field; survey papers are not acceptable.

Each student will make at least four class presentations. The first two will be on fundamental papers assigned by the instructor. The third will be on a paper closely related to the student’s project. The fourth will be the project presentation.

**Grading Policy**
Grades will be assigned as measures of performance on required activities. Semester grades will be weighted as follows: original research project (60%), paper presentations (20%), written assignment (15%), class participation (5%). Each required activity will receive a numerical grade, to be interpreted as follows: 90–100 (A), 80–89 (B), 70–79 (C), 60–69 (D), 0–59 (F). There is no final examination. All requirements will follow the standard expectations of professional
researchers in computer science, including the grant proposal process, writing technical reports, and making conference presentations.

Academic Integrity
``By enrolling in this course, each student assumes the responsibilities of an active participant in UMBC's scholarly community in which everyone's academic work and behavior are held to the highest standards of honesty. Cheating, fabrication, plagiarism, and helping others to commit these acts are all forms of academic dishonesty, and they are wrong. Academic misconduct could result in disciplinary action that may include, but is not limited to, suspension or dismissal. To read the full Student Academic Conduct Policy, consult the UMBC Student Handbook, the Faculty Handbook, or the UMBC Policies section of the UMBC Directory (or for graduate courses, the Graduate School website)” [from www.umbc.edu/provost/integrity].

One serious type of misconduct is plagiarism, which in its many forms, involves representing someone else’s work as your own. For example, copying homework solutions found on the Internet is misconduct. Buying, selling, acquiring term papers, or facilitating such activities, is also misconduct.

In this course, students are allowed and encouraged to work together while solving problems. However, each student must write up his solution entirely independently, without looking at anyone else’s written solution and without showing anyone his or her written solution.

Students are expected to be familiar with UMBC’s computer usage polices.

UMBC Center for Information Security and Assurance (CISA)
The UMBC Center for Information Security and Assurance (CISA) has a three-fold mission to promote research, education, and best practices in Information Assurance (www.cisa.umbc.edu). Supported by DoD, CISA hosts distinguished lectures and maintains a Cyber Defense Lab (CDL) available for student projects.