Syllabus
CMSC-443 Cryptology, Alan T. Sherman, Spring 2011, UMBC

Instructor
Dr. Alan T. Sherman, Ph.D.
Associate Professor, Computer Science
Department of Computer Science and Electrical Engineering (CSEE)
www.csee.umbc.edu/~sherman
Email: sherman@umbc.edu  Send email only to this address, and include “443” in the subject.
Office Hours: Monday, Wednesday, Friday 9:30-10am in ITE 224 (or ITE 228 Cyber Defense Lab), and
by appointment, while classes are in session.
Tele: 410-455-2666, Physical Mail Box: in ITE 325

Grader
none

Meeting Time and Place
Monday, Wednesday, Friday 11-11:50am in ITE 233. Section 1, #1085.

Textbook
third edition.

Grading
Final Exam-31%, Exam I-22%, Exam II-22%, Homework-22%. Quality of class participation-3%. An
‘A’ grade means the student can solve challenging problems fluently without help.
There is an optional research project (see separate handout). Students who elect to carry out this
project select a project weight 0.1 ≤ w ≤ 0.4 Their final grade is determined from wP + (1-w)G, where
P is the project score and G is the regular term score defined above.

Exam Dates
Exam I (Chapters 1-6)-Monday March 14. Exam II (Chapters 7-10)-Monday April 25.
Comprehensive Final Exam-Monday May 20, 10:30am-12:30pm.

Course Description
An introduction to cryptology, the science of making and breaking codes and ciphers. Topics include:
conventional and public-key cryptosystems, including AES, RSA, shift register systems and selected
classical systems; examples of cryptanalytic techniques; digital signatures; message authentication codes,
pseudorandom number generation; cryptographic protocols and their applications; hash functions, secret
sharing systems, key distribution, key agreement, and an introduction to the theories of cryptographic
strength based on information theory and complexity theory. Prerequisite: CMSC 341, MATH 221 and
STAT 355.

Goals
By the end of the course, should have an understanding of cryptographic primitives and how to apply
them appropriately. Students should be able to design and analyze security systems using these
primitives to achieve the goals of confidentiality, authentication, and integrity. Students should be able to
reason about the mathematical properties of cryptographic functions, expressing their thoughts in clear
and well-defined mathematical prose
Student Responsibilities
Each student is expected to solve problems actively every day (many more than are required for homework), to bring thoughtful questions to class, and to participate actively in class.

Prerequisites
CMSC-341, Math 221, and STAT-355.

Academic Integrity
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```