Cryptography
Spring 2014
MATH 408.56A[1] (3 credits), Tuesday, 6:00P-9:00P, Ware Center

Prerequisites: There are no specific course prerequisites, but students should be comfortable with reading and understanding elementary proofs and have had some exposure to computer programming.

Instructor: Dr. Buchanan
Office: Wickersham 217-1, Phone: 872-3659, FAX: 871-2320
Office Hours: 2:00P-2:50P (M_W_F), 2:30P-3:30P (Tu_Th), or by appointment
Email: Robert.Buchanan@millersville.edu

Textbook: *Introduction to Cryptography with Coding Theory*, 2nd edition, Wade Trappe and Lawrence C. Washington, Pearson/Prentice Hall, Upper Saddle River, New Jersey, 2006, ISBN: 0–13–186239–1.

Objectives:

The objectives of this course include introducing students to the basic mathematical principles of cryptography. Upon successful completion of this course students should be able to

- understand modular arithmetic, congruences, and some topics from elementary number theory,[2]
- understand the design, structure, and operation of symmetric-key cryptosystems such as block ciphers and stream ciphers,
- understand the design, structure, and operation of public-key cryptosystems including RSA and authentication,
- compare and contrast symmetric-key and public-key cryptosystems,
- understand the role of prime numbers in cryptography and various algorithms for primality testing,
- understand the design, structure, and operation of cryptosystems based on elliptic curves,
- describe the state of research and development of quantum cryptosystems, quantum computers, and their implications for existing cryptosystems.

Course Contents:

A list of topics to be covered in this course includes:

- Origin and history of cryptography
- The Integers
  - Divisibility
  - Greatest Common Divisor

[1] Cross listed as graduate course, MATH 695.54A.

[2] Overlap with MATH 393 *Number Theory* will be kept to a minimum by covering only the topics of number theory necessary for the understanding of cryptosystems.

  - Euclidean Algorithm
  - Extended Euclidean Algorithm
  - Factoring
  - Primality testing
- Symmetric-Key Cryptosystems
  - Congruences
  - Block ciphers
  - Permutations
  - Multiple encryption
  - Data Encryption Standard (DES)
  - Stream ciphers
- Public-Key Cryptosystems
  - Exponentiation
  - Discrete Logarithms
  - RSA Cryptosystem
  - Authentication
  - Knapsack problem
- Digital signatures
- Primality Testing
- Elliptic curves
- Quantum cryptography

If time permits other topics may be covered as well.

Attendance: Students are expected to attend all class meetings. If you must be absent from class you are expected to complete class requirements (tests and/or homework assignments) prior to the absence. Students who miss the deadline for an assignment should provide a valid excuse, otherwise they will not be allowed to make up the assignment. Assignments should be made up within one week of their scheduled deadline.

Homework: Homework assignments will consist of a mixture of pencil and paper, calculator and/or computer assignments. Students are expected to do their homework and participate in class. Students should submit all homework by the date due. Late homework will not be accepted without valid excuse. Discussion and collaboration between students on homework assignments is encouraged, but homework submitted for grading should be written up separately. Submitted written homework and programming assignments should not be merely identical copies of other students' work.

Tests: There will be two tests and a comprehensive final examination.

1. Tuesday, February 25, 2014
2. Tuesday, April 1, 2014

The final exam is scheduled for Tuesday, May 6, 2014. I will not "curve" test, quiz, or exam grades.

Grades: Course grade will be calculated as follows.

Class Participation	25%
Homework	25%
Tests and Exam	50%

Tests and the final examination will be graded individually on a 100-point scale. Homework sets will vary in the number of problems assigned, but generally each homework problem will be worth ten points. For example on a homework assignment of five problems, the maximum numerical grade would be 50 points. To ensure that all homework assignments are weighted equally, each student's score will be normalized by the maximum score for that assignment. Again for example, on a five problem homework assignment grades will be among the set of scores $\{0/50, 1/50, \ldots, 49/50, 50/50\}$. I keep a record of students' test, homework, and exam scores. Students should also keep a record of graded assignments, tests, and other materials. As an example of the calculation of the numerical course grade, suppose a student's two test grades were 87 and 70 (out of a maximum of 100 points on each test), the student's final examination grade was 75 (again, out of a maximum of 100), the student earned 21 out of 25 class participation points, and the student's ten homework grades were $\{25/30, 20/40, 40/50, 37/40, 40/40, 20/30, 0/40, 15/20, 45/50, 30/30\}$. This student's homework average is 0.7375. The student's numerical course grade is then

$$\frac{87+70+75}{3}(0.50) + (0.7375)(25) + 21 \approx 78.1.$$

I keep a record of students' assignment scores. Students should also keep a record of graded assignments and other materials. The course letter grades will be calculated as follows. I will not "curve" course grades.

90-92	A−	93-100	A		
80-82	B−	83-86	B	87-89	B+
70-72	C−	73-76	C	77-79	C+
60-62	D−	63-66	D	67-69	D+
		0-59	F		

Course Repeat Policy An undergraduate student may not take an undergraduate course of record more than three times. A course of record is defined as a course in which a student receives a grade of A, B, C, D, (including + and −) F, U, Z or W. The academic department offering a course may drop a student from a course if the student attempts to take a course more than three times.[3]

The last day to withdraw from a course (and receive the W grade) is April 4, 2014.

[3] Memorandum to mathematics faculty from Dr. Charles G. Denlinger, Assistant Chair, Department of Mathematics, August 30, 2004.

Inclement Weather Policy: If we should miss a class day due to a school closing because of weather, any activities planned for that missed day will take place the next time the class meets. For example, if a test is scheduled for a day that class is canceled on account of snow, the test will be given the next time the class meets.

Cell Phones: Silence (or better yet, turn off) all cellular telephones upon entering the classroom. Leaving class to initiate or receive a telephone call will not be tolerated and students doing so will not be re-admitted to the classroom until the following class meeting. Texting or tweeting during class interferes with the learning process. Students distracted by their cell phones are not engaged in class and will find, over the course of the semester, that learning and course grade will suffer.

Final Word: Math is not a spectator sport. What you learn from this course and your final grade depend mainly on the amount of work you put forth. Daily contact with the material through homework assignments and review of notes taken during lectures is extremely important. Organizing and conducting regular study sessions with other students in this class will help you to understand the material better.

No one can guarantee you success in this course. Your responsibilities and the instructor's expectation are outlined above. There will be no second chances, "do-overs", or extra credit assignments.