Elementary Cryptography: MATH 293

PPHAC 235, MWF 1:10 PM - 2:20 PM
Fall 2014

Instructor: Dr. Shannon Talbott
Office: 217 PPHAC
Phone Number: 610.861.1573
Email: talbotts@moravian.edu

Office Hours:
Monday 2:30 - 3:30 PM; Wednesday 10:15 - 11:15 AM; Thursday 1:45 - 3:45 PM; and by appointment

Text: *Introduction to Cryptography with Coding Theory, Second Edition,* by Wade Trappe and Lawrence C. Washington.

Course Goals:
This course is an introduction to cryptography and thus will emphasize the relevant mathematics used in modern cryptography including basic linear algebra and elementary number theory. We will discuss material from chapters 1,2 ,3, 6, 7, along with 12, 13, and 16, time permitting.

Upon completion of the course, a student will be able to do the following:

- Understand the theory of and recognize
    * classical cryptosystems, from shift cyphers to block cyphers
    * public key cryptosystems, including RSA
- Understand the underlying mathematics including elementary number theory and elliptic curves, time permitting
- Be able to employ mathematics to
    * create a key for certain cryptosystems (i.e. create codes)
    * find the key for certain cryptosystems (i.e. break codes)

Where to get help:

- Come to my office
- Work with each other

Grading System:

Homework/Quizzes
There will be homework assigned at the end of each section. It is vital that you do all of the homework problems assigned; you should keep all of your work in a notebook or binder for reference. For every hour in class, you should expect to

spend 2 hours doing work outside of class. You cannot learn math without lots of practice! Certain homework problems will be collected and graded for both completeness and accuracy. Late homework will not be accepted. Extenuating circumstances will be taken into consideration. You are encouraged to discuss the material with fellow students, but any work turned in must be your own.

Exams

We will have three in class exams and a final exam. If you will miss an exam (with an approved excuse), you must notify me PRIOR TO the exam. You will then be given a suitable (corresponding to the time beyond the exam date) but more difficult exam. Extenuating circumstances will be taken into account.
Your final exam will be on Wednesday, December 10 at 8:30 AM.

Attendance

Regular class attendance is expected of all students. You are responsible for all material assigned or covered in class. If you do miss a class for any reason, it is your responsibility to keep up with the class. You should see a classmate for notes, homework assignments, and any announcements from class.

Your final grade is based on the following distribution:

Homework/Quizzes:	35%
Participation:	5%
Exam I:	15%
Exam II:	15%
Exam III:	15%
Final Exam:	15%

Course grades will be determined by the following scale:

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

The exam schedule will be as follows, although slight changes may be made:
Exam I: Friday, September 19
Exam II: Friday, October 17
Exam III: Friday, November 14
Final Exam: Wednesday, December 10 at 8:30 AM

Course Policies:

Final Exam: Your final exam is on Wednesday, December 10 at 8:30 AM. A make-up final exam will not be administered to accommodate any travel plans.

Participation in class discussions: Class participation enhances your learning experience. Students who attend class regularly, participate in discussions, and

are in between grades at the end of the semester may receive the higher of the two grades.

Other Expectations of Student Performance/Behavior:
Please turn off your cell phone at the beginning of class. Be considerate of your classmates and keep private discussions during class to a minimum. Please check your email for any announcements regarding this class. If you wish to email me, please use your Moravian email accounts only as I frequently delete spam.

This syllabus is subject to change. Any changes will be announced in class.

Mathematics Department Academic Honesty Policy: The Mathematics Department supports and is governed by the Academic Honesty Policy of Moravian College as stated in the Moravian College Student Handbook. The following statements will help clarify the policies of the Mathematics Department faculty.

Learning Disability Accommodations: Students who wish to request accommodations in this class for a disability should contact Ms. Elaine Mara, assistant director of academic support services for academic and disability support, at the lower level of Monocacy Hall, or by calling 610-861-1401. Accommodations cannot be provided until authorization is received from the Academic Support Center.
The Writing Center is located in a building that is not accessible to persons with mobility impairments. If you need the services of the Writing Center please call 610-861-1392.