HON 1290: Introduction to Cryptology, Spring 2012

Instructor:	Dr. Amanda Knecht	**Office:**	SAC 323
E-mail:	amanda.knecht@villanova.edu	**Phone:**	610.519.6659
Office Hours:	M 1-4 pm, W 11:30am-12:30pm and by appointment		

Text: Required: *Codebreaker: The History of Codes and Ciphers*, S. Pincock, ISBN: 978-0-8027-1547-0

Contents: This course gives a historical introduction to cryptology and introduces a number of mathematical ideas and results involved in the development and analysis of secret codes. While the mathematical subjects treated include enumeration, probability, and some statistics, the bulk of the course is devoted to elementary number theory, with the goal of understanding public key encryption.

Structure The course has two components, the worksheet component and the computer component. Instead of a standard text book, I will give you worksheets to do in class. I will introduce each worksheet with some background material (definitions, motivation), and then you will complete the worksheets in groups. Each worksheet will consist of a list of problems that you will attempt to solve together during class over the course of a few class periods. As you solve problems from the worksheet, you will be asked to explain your solutions to the rest of the class. In particular, you should share the strategies you used to solve the problem, rather than simply giving the final answer. During the first few weeks I will help with these explanations, but my hope is that you will soon explain your own methods and solutions. Effective communication is a skill everyone should develop. On many Fridays we will have a computer component for which you will need to bring your laptop. You will be given various discovery-based projects designed to allow you to explore the ideas we have developed.

Philosophy This is not a traditional lecture-style course. You don't learn how to play basketball by watching a Villanova game on TV, so why should you learn how to do mathematics by watching a professor do mathematics on the board? This semester I will help you learn how to solve problems and create your own mathematics through experimentation, critical thinking, and discussion with one another.

But why should you want to learn how to solve problems and create the mathematics when I could just tell you the answers and show you how to work the problems? Because good problem solving skills are essential to success in all walks of life. Throughout your time at the Villanova, you will be faced with all sorts of different and challenging problems. Being relaxed and confident when confronted with a different situation is the hallmark of a good problem solver, and having that skill will serve you well in your time in college and beyond.

Employers aren't looking to hire people who mindlessly plug numbers into formulas that are given. They want people who are comfortable when faced with new challenges and possess good analytic skills. Chances are you won't have much specific need for the mathematics of cryptology in your future career. Nevertheless, no matter what you go on to do, knowing how to use logical reasoning to solve problems will always be a useful skill.

Goals My biggest hope is that when you leave this course in December you will no longer fear difficult problems and you will celebrate the struggle of thinking. Along the way I hope that you all develop the following skills:

- an ability to communicate ideas effectively
- an ability to teach others
- an ability to teach yourself
- a willingness to make mistakes
- a passion and curiosity for learning
- an ability to create questions

Maple: We will use the computer algebra program Maple in this course. It is available for free for all students at:

`http://www3.villanova.edu/maple/securedownloads/mapledownloadfaq.htm`.

You need to download and install the program on your laptop before Friday, January 27.

Participation As you may have gathered from the structure and philosophy of the course, attendance and participation are very important. I will keep track of how much effort you've put into each day's work, and how often you volunteer your thoughts in the explanation portion of class. Your participation in class and in labs will account for 20% of your final grade. **Don't skip class!** Clearly, when you skip a class, you miss out on the participation component of the course. However, there may be even more serious consequences...

Serial Absenteeism Clause

You are allowed up to two (2) unexcused absences from class. (The instructor decides what constitutes an excused absence on a case-by-case basis.) Coming to class more than five minutes late or leaving early counts as an absence. For each absence beyond those two, your final grade for the class will drop by one letter grade. For example, if you would have otherwise earned a B+ for the course but you have 3 unexcused absences, your final grade will be a C+!!! Also, any freshman missing 7 classes automatically receives a Y letter grade.

Homework Since this is the honors version of a math class, you will have two types of homework, regular homework based on the worksheets and out of the box questions. Homework is due at the beginning of class on the given due date. Your cumulated homework scores will account for 30% of your final grade. You are encouraged to discuss the homework assignments with other students in the class; however, if you do, you should write on your homework submission the students with whom you discussed the assignment. You may not copy the written work of another student or allow another student to copy your written work. What you submit should be your own work: written by yourself and in your own words.

Late homework will not be accepted in the absence of divine intervention or matters of similar weight. Unexcused, late, or missing papers count as zeroes.

Exams There will be two (2) midterm exams and a final exam. All exams will be held in class according to the schedule below. Your two midterm scores will each account for 15% of your final grade; your final exam score will account for 20% of your final grade. All enrolled students must plan to take exams at the scheduled times. Travel plans will not be considered an excuse to take an examination on a different date.

Grade Distribution

Participation	–	20%	
Homework	–	30%	
Midterm 1	–	15%	(*Friday,February 24*)
Midterm 2	–	15%	(*Wednesday, April 4*)
Final Exam	–	20%	(*Wednesday, May 9, 11:30-2:00)*

Getting Help As the course goes along, you will quickly realize the benefit of regularly attending office hours. You are encouraged to make appointments when necessary, especially if the regular office hours don't fit well with your schedule. Always feel free to email with questions about the course in general or to set up an appointment. As a rule, homework related questions are best answered during office hours. But if the need arises I will try to respond to email questions within one business day. *Emailing questions the night before an assignment is due is definitely not a good idea.*

Break Notes We will have a lab in class on Friday, March 2. The lab will be due at the end of class, and no late labs will be accepted. Also, your second exam is the day before Easter break. Plan your travel accordingly.

Special Arrangements If you have a documented disability requiring special accommodations, please inform me at the beginning of the semester, or at least two weeks prior to needing the accommodation (e.g., prior to the exam).

"It is the policy of Villanova to make reasonable academic accommodations for qualified individuals with disabilities. If you are a person with a disability please make arrangements to register with the Learning Support Office (LSS) by contacting 610-519-5636 or at nancy.mott@villanova.edu as soon as possible. Registration is needed in order to receive accommodations. All members of the Villanova community are encouraged to contact LSS with any questions or concerns."