CMSC 455: Network Security and Cryptography (3 credits)
Spring 2016
http://marmorstein.org/~robert/Spring2016/455.html

Instructor: Robert Marmorstein (robert@narnia.homeunix.com) **Phone:** 395 - 2185
Lecture: 9:30am-10:45 am TR Ruffner 352
Office Hours: 1:30-3:00pm TWRF or by appointment **Office:** Ruffner 329

Course description: This course covers several modern cryptographic systems, including the DES and AES encryption standards. Their applications to network security are discussed, along with issues of authentication, privacy, intruders, malicious programs and firewalls. The approach is from the theoretical side, and the mathematics of these areas is studied.

Prerequisite: CMSC 160 **AND** either MATH 175 or MATH 270.

Required Textbook: Cryptography: Theory and Practice, Douglas Stinson, CRC Press, 2005, Third Edition, ISBN: 978-1-5-8488508-5

Course objectives:

The student will learn to:

1. Encode and decode messages using simple substitution and transposition ciphers
2. Use public-key and private-key cryptographic functions in C++ programs
3. Compare and analyze the security and performance characteristics of cryptosystems

Course Work: Your grade will be determined by your performance on the final exam (25%), midterm exam (25%), quizzes and homework (30%) and programming projects (20%).

Grading Policy: Late work will not be accepted unless you have a major medical emergency which prevents you from completing the work on time. Final letter grades will be based on the following scale:

		100-91%	A	90%	A-
89%	B+	88-81%	B	80%	B-
79%	C+	78-71%	C	70%	C-
69%	D+	64-65%	D	63-0%	F

There is no grade of D- in this class.

You are responsible for making sure that assignments are correctly submitted. There will be no second chances or partial credit for incomplete submissions, including empty or incorrectly formatted archives.

Slip Days: I will allow three "slip days" over the course of the semester. Slip days can be used ONLY on programming projects (not on the exams or homework) to extend a due date by 24 hours. The “slip day clock” runs over holidays and weekends, so if you use a slip day on a project due on Friday, it will be due at the same time on Saturday (not on Monday).

Attendance: Missing more than 10% of scheduled class time may, at my option, result in loss of one letter grade. Absences for school events or illness may be excused if you make arrangements with me within 12 hours of the missed class. Missing 25% of classes for ANY reason (excused or unexcused) may, at my discretion, result in a grade of **F** for the course.

Cell phones and laptops: You must bring your laptop to each laboratory session. However, I do not allow cell phones or laptops in class during lecture. Please put away all personal electronic devices during class. Any violation of this policy will be considered an unexcused absence. If you are unable to bring your laptop to the lab for any reason (such as hardware malfunction), please contact me at least 6 hours in advance so that I can make alternative arrangements.

Food and Drink: Please do not eat in class. It distracts me and the other students. You may bring non-alcoholic beverages to class. If you are not able to eat lunch at another time, I may be willing to negotiate an exception to this policy, but you must make arrangements with me in advance or I will count you absent.

Honor Code: I take the honor code very seriously. All work in this class is considered pledged work. Therefore, while I urge you to take advantage of the freedom the honor code gives you to collaborate with other students, I have also established some rules to ensure that you learn the assigned material.

Exams and quizzes must be completed entirely on your own. You may freely discuss the programming projects and homework with other students as long as:

1. All work you turn in is your own original work, which you have personally typed or written.
This includes both homework assignments and projects. All the code you turn in should be code YOU have typed. You MAY write code down on the marker board or a sheet of paper to make discussion easier as long as you erase or dispose of the information before you leave the room. You may NOT share code electronically. You may NOT share printouts of your code with anyone. **You may look things up online, but you may not copy/paste or download anything you find.**

2. You do not copy large blocks of code.
Helping someone catch a syntax error in their code is fine. Giving them, in general terms, the idea of an algorithm is okay. But sharing an entire program, or even a significant component of that program (a non-trivial function, or more than a few lines of code) is cheating. A good rule of thumb is the three-line rule: in general, sharing more than three lines of code is too much. Sharing less than three lines is usually okay. Similarly, when getting help on homework, you can discuss general principles, but should not copy answers from someone else. This rule also applies to using print and electronic resources. Do not copy or download large blocks of code from the Internet.

Infractions of this policy will be dealt with harshly under the Longwood Honor Code. A student convicted of an Honor Code offense involving this class **will receive a grade of F** for the course in addition to any penalties imposed by the Honor board. All work completed in this class is considered to be pledged whether or not the pledge appears on the assignment.

Mandatory Reporting of Crimes and Sexual Misconduct: In accord with its history and mission, Longwood University believes that each individual should be treated with respect and dignity and that any form of crime or violence is incompatible with Longwood's commitment to the dignity and worth of the individual. Longwood University is committed to providing a healthy living, learning and working environment which promotes personal integrity, civility and mutual respect. If you have been the victim of a crime or sexual misconduct we encourage you to report this. If you disclose this to a faculty member or employee (with the exception of our Limited Reporting and Confidential Reporting Resources; for example, the Counseling and Psychological Services (CAPS) staff), they are required by law to notify the appropriate University officials. The faculty member or employee cannot maintain complete confidentiality and is required to report the information that has been shared. Please know that all reported information is treated with discretion and respect and kept as private as possible. For more information about your options at Longwood:

http://www.longwood.edu/titleix
http://www.longwood.edu/police/crimereports.htm
http://www.longwood.edu/studentconduct/12050.htm

or contact Jen Fraley(fraleyjl@longwood.edu), Associate Dean of Conduct and Integrity.

Tentative Course Schedule:

Jan. 19-21		Introduction to Cryptography and Cryptanalysis (Read Chapter 1)
Jan. 26-28		Simple Substitution and Transposition Ciphers, Mathematical Background
	Jan. 26	**LAST DAY of ADD/DROP (Must add or drop by 5pm)**
Jan. Feb. 2-4		Hill and Vigenere Ciphers, Cryptanalysis of Simple Ciphers, Frequency Analysis
Feb. 9-11		Shannon's Theory and the One-time Pad (Read Chapter 2)
Feb. 16-18		**Catchup and Review**, **Midterm Exam**
Feb. 23-25		Block Ciphers and the DES Cipher (Read Chapter 3)
Mar. 1-3		Introduction to AES Cipher (Chapter 3)
	Mar. 7-11	**Spring Break (No Class)**
	Mar. 14	**Deadline to withdraw without failing (by 5pm)**

Mar. 15-17	Field Theory of AES (Chapter 3)
Mar. 22-24	Cryptographic Hashing (Read Chapter 4)
Mar. 29-31	The RSA Algorithm and Integer Factorization (Read Chapter 5)
Apr. 5-7	Digital Signatures (Read Chapter 7)
Apr. 12-14	Key distribution and agreement (Read Chapters 10 and 11)
Apr. 19-21	Pretty Good Privacy: PGP and GPG, Secure Sockets: TLS and SSL
Apr. 26-28	Catchup and Review
May 4 (Wednesday)	**FINAL EXAM** (11:30am-2:00pm)