CMSC 455: Network Security and Cryptography (3 credits)
Spring 2018
http://marmorstein.org/~robert/Spring2018/455.html

Instructor: Robert Marmorstein (robert@narnia.homeunix.com) **Phone:** 395 - 2185
Lecture: 2:00pm-3:15 pm TR Ruffner 354
Office Hours: 2:00pm-2:50pm MWF, 12:30pm-1:45pm TR, or by appointment **Office:** Ruffner 329

Course description: This course covers modern and historical cryptographic systems with an emphasis on the mathematical underpinnings of cryptographic and cryptanalytic algorithms. Topics include simple substitution and transposition ciphers, matrix operations over a finite field, cryptographic hashing, the Data Encryption Standard and Advanced Encryption Standard cryptanalytic systems, Diffie-Helman Key distribution, the Chinese Remainder Theorem, and RSA encryption.

Prerequisite: CMSC 160 **AND** either MATH 261.

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

Course objectives: By the end of the course, the student will be able to:

1. Encode and decode messages using simple substitution and transposition ciphers
2. Implement modern ciphers in a high-level language
3. Apply mathematical techniques to the security and performance characteristics of cryptosystems

Course Work: Your grade will be determined by your performance on the final exam (10%), midterm exam (10%), quizzes and homework (45%), programming projects (30%), and participation (5%).

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+	68-64%	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 and Collaboration:

I believe wholeheartedly in the honor code. As such, I encourage you to actively collaborate with other students and to discuss homework problems and lab projects. However, there is a point at which collaboration becomes cheating and I deal harshly with cheating in my courses.

To help you understand the line between acceptable discussion of a project and dishonorable behavior, I ask you to observe the following rules:

1. Exams and quizzes are to be completed entirely on your own. All exams and quizzes will be closed-book, closed-notes unless I specify otherwise (usually by providing you material I have selected as a reference for the exam such as an ASCII table or other information source).

2. On all other assignments, everything you turn in should be something YOU have personally typed or hand-written. You may NOT copy code electronically from other students or the Internet.

The work you submit should, in general, be your own original work or material which I have provided and you have suitably modified by yourself.

This DOESN'T mean you can't use the Internet to look up topics related to the class.

It DOES mean that you should re-type any code you find online and not just download it or copy/paste it.

It also means you may NOT transfer code using flash drives, cell phones, e-mail, web sites, floppies, CDs, or any other electronic storage or communication device unless I specifically direct you to do so.

You MAY NOT print out copies of your code to share with other students. You MAY print out personal copies of code or copies to bring to office hours.

3. Do not copy large blocks of code from other students or the Internet. Do not copy homework answers.

The purpose of the projects and homework exercises is for you to demonstrate mastery of the material. You should never turn in any code or answers that you don't understand well enough to explain to me without help.

You MAY assist other students with their projects and homework assignments as long as you discuss only the general problem or the process of obtaining a solution. Point them to the appropriate material from lecture or the textbook or walk them through a related example that illustrates the process they need to solve the problem.

You MAY also compare answers once you have both worked out a solution.

You MAY NOT copy homework answers or large blocks of code. A good guideline of what "large" means is that more than three complete programming statements is usually too much. When in doubt, ask (or refrain from copying).

You MAY provide or get assistance with simple problems like syntax errors.

4. You MUST give proper attribution.

Whenever you receive help or use an on-line resource, you must acknowledge your sources. In projects, should do this by placing comments in the code. A simple comment like:

/* based on http://codewarrior.com */

or

/* Jessica helped me with the curly braces here */

is fine. The comment should go directly above or on the same line as the code on which you received help, so that it is clear exactly which parts of your program are original and which are not. On homework assignments, indicate that you have received help on a problem by making a note in the margin near the problem on which you collaborated.

When in doubt, ALWAYS cite your source.

5. You are responsible for securing your code.

Helping other students to cheat is also cheating. Furthermore, it is your responsibility to make sure that other students do not use your work to cheat. Be careful with who you let access your computer and report any missing files, flash drives, etc., to me promptly.

Infractions of these policies will be dealt with harshly under the Longwood Honor Code. Any student convicted of an honor offense involving this class will automatically receive a final course grade of F in addition to any penalties imposed by the Honor Board. You should consider all work in this class to be pledged work, 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 (Please check the course web site for updates):

Jan. 18	Introduction to Cryptography and Cryptanalysis (Read Chapter 1)
Jan. 23-25	Simple Substitution and Transposition Ciphers
Jan. 24	**LAST DAY of ADD/DROP (Must add or drop by 5pm)**
Jan. 30-Feb. 1	General Substitution Ciphers, Brute Force and Frequency Analysis **Lab 1: Frequency Analysis of the Affine Cipher (Due Feb. 1)**
Feb. 6-8	Matrix Multiplication, Matrix Inversion Hill and Vigenere Ciphers
Feb. 13-15	Shannon's Theory and the One-time Pad (Read Chapter 2), Prime Factorization and Euler's Totient, Greatest Common Divisor Algorithms **Lab 2: Cryptanalysis using a Dictionary Attack (Due Feb. 15)**
Feb. 20-22	**Catchup and Review**, **Midterm Exam**
Feb. 27-Mar. 1	Block Ciphers and the DES Cipher (Read Chapter 3)
Mar. 5-9	**Spring Break (No Class)**
Mar. 13-15	Introduction to AES Cipher (Chapter 3) **Lab 3: Implementation of a Substitution-Permutation Network (Due. Mar. 15)**
Mar. 13	**Deadline to withdraw without an F (by 5pm)**
Mar. 20-22	Field Theory and Cryptanalysis of AES
Mar. 27-29	Cryptographic Hashing (Read Chapter 4) One-way functions, Counting Permutations and Combinations
Apr. 3-5	The RSA Algorithm and Integer Factorization (Read Chapter 5)
Apr. 10-12	Pretty Good Privacy: PGP and GPG, Secure Sockets: TLS and SSL (Read Chapter 12) **Lab 4: Public Key Encryption (Due. Apr. 12)**
Apr. 17-19	Diffie-Helman Key Distribution (Read Section 10.1 and Chapter 11)
Apr. 24-26	Catchup and Review
May 4 (Friday)	**FINAL EXAM** (11:30am-2:00pm)