CMSC 455: Network Security and Cryptography (3 credits)
Spring 2020
http://marmorstein.org/~robert/Spring2020/455.html

Lecture: 9:30am-10:45 am TR Stevens 118

Instructor: Robert Marmorstein (marmorsteinrm@longwood.edu) **Phone:** (434)395-2185
Office Hours: 2:00-4:00pm MWF, 1:00-2:00pm T *or by appointment* **Office:** Ruffner 329

I am also available by appointment. My schedule is posted near my office door. To make an appointment, please check the schedule to see which times I am free, then contact me by e-mail and list some possible times we could meet. In general, I need at least 24 hours of notice to schedule an appointment.

Communications Policy
The best ways to get in touch with me outside of office hours are either to use Slack or to send e-mail to marmorsteinrm@longwood.edu. Typically, I will reply within 24 hours (often sooner) on weekdays. I often reply much quicker – even on weekends.

If you are asking for help with a project or homework problem by e-mail, you should attach your code or your work to the e-mail or copy/paste the part you are working on into the body of the e-mail. **Do NOT attach screenshots or pictures taken on your phone.** They are hard to read and take up too much space in my inbox. In general, e-mails containing images will be deleted unread.

An even better way to get in touch with me is to use **Slack**. Slack is a chat utility with clients for mobile devices and desktop computers. It will allow you to easily send me code snippets. Also, since I get notifications when a slack message comes in, I am more likely to reply to your message quickly if you use Slack than if you send me e-mail.

Slack is also a good way to communicate with other members of the class. Feel free to ask for help on the course Slack – as long as you stick to general questions about topics and do not share large blocks of code.

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** MATH 175.

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%).

Course Structure and Student Expectations:
This course is very theoretical and homework makes up the largest part of your grade. However, it also has a significant programming component. In general, we will spend three hours a week in lecture and discussion sections and you will be expected to work on the projects outside of class. You should expect to spend at least nine additional hours each week reading the textbook, preparing for exams and working on assignments.

Grading Policy: Late work will not be accepted (and will receive a grade of 0%) unless you have serious circumstances (such as a medical emergency) which prevent you from completing the assignment on time. In such cases, you do not need a doctor's note, but you must send me **e-mail** within a reasonable amount of time (typically within twelve hours of the due date) to explain your circumstances and make arrangements for the work to be completed.

Slip Days: You will be allocated a fixed number of slip days at the start of the semester. You may use your slip days to extend the due date of one or more programming projects. You can use all of your slip days on one assignment or you may use them over multiple assignments. Slip days can be used only on projects – not on homework assignments.

Slip days are calculated from the minute the project is due until you turn it in and are rounded up to the nearest integer value. That means that if you turn an assignment in 24 hours and 1 minute after the due date, you will use up two slip days. The slip day clock runs over weekends and holidays. If a lab is due on Friday and you turn it in on Monday, you will have used three slip days, not one. Slip days cannot be shared, traded, bought, or sold, but can occasionally be earned by participation in relevant campus activities I select.

Grading 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		
64 or lower: F		(There is no grade of D- in this course. Anything below a 64 is failing.)			

Attendance: I expect you to attend class unless you are sick or engaged in a school-sponsored sport or extracurricular activity. Please do NOT come to class if you are sick. Instead, contact me within 12 hours of the absence to check whether you've missed any work and make arrangements to make up any missed quizzes. You should also arrange to get notes from another student in the class. It is **your** responsibility to check the course web site for announcements, new assignments, and other important updates.

I will rely primarily on your honor for enforcement of the attendance policy. However, to comply with Longwood policy, I will keep a record of your attendance. In accordance with that policy, missing more than 10% of scheduled class time (4 class sessions) to unexcused absences may, at my discretion, result in loss of one letter grade and missing 25% of class or more (roughly 10 sessions), whether excused or not, may result in an automatic failing grade.

Cell phones and laptops: 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. We will be meeting in the computer lab – if you are doing work on the computer systems during lecture, I will also count you absent.

Food and Drink: You may bring non-alcoholic beverages, including soft drinks, to class. However, please do not eat in class (it distracts me and the other students). Violations of this policy will be considered an unexcused absence. I occasionally grant exceptions to this rule for students who must otherwise forgo lunch or have medical needs that require them to eat in class. If you feel that you need such an exception, you must make arrangements with me in advance (i.e. before bringing food to class).

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. 14-16	Introduction to Cryptography and Cryptanalysis (**Read Chapter 1**)
Jan. 21-23	Simple Substitution and Transposition Ciphers, Prime Factorization and Euler's Totient
Jan. 22	**LAST DAY of ADD/DROP (Must add or drop by 5pm)**
Jan. 28-30	General Substitution Ciphers, Brute Force and Frequency Analysis, Monoalphabetic and Polyalphabetic Substitution Ciphers, The Vigenere Cipher **Lab 1: Frequency Analysis of the Affine Cipher (Due Feb. 1)**
Feb. 4-6	Matrix Multiplication, Determinants, Matrix Inversion Hill and Permutation Ciphers

Feb. 11-13	Shannon's Theory and the One-time Pad (**Read Chapter 2**), Greatest Common Divisor Algorithms **Lab 2: Cryptanalysis using a Dictionary Attack (Due Feb. 15)**
Feb. 18-20	**Catchup and Review**, **Midterm Exam**
Feb. 25-27	Block Ciphers and the DES Cipher (**Read Chapter 3**)
Mar. 2-6	**Spring Break (No Class)**
Mar. 10-12	Introduction to AES Cipher (Chapter 3) **Lab 3: Implementation of a Substitution-Permutation Network (Due. Mar. 15)**
Mar. 17-19	Field Theory and Cryptanalysis of AES
Mar. 24-26	Catchup and Review
Mar. 31	**Deadline to withdraw without an F (by 5pm)**
Mar. 31-Apr. 2	Cryptographic Hashing (**Read Chapter 4**) One-way functions, Counting Permutations and Combinations
Apr. 7-9	The RSA Algorithm and Integer Factorization (**Read Chapter 5**)
Apr. 14-16	Pretty Good Privacy: PGP and GPG, Secure Sockets: TLS and SSL (**Read Chapter 12**) **Lab 4: Public Key Encryption (Due. Apr. 12)**
Apr. 21	Diffie-Helman Key Distribution (**Read Section 10.1 and Chapter 11**)
Apr. 23	**Research Day: NO CLASS**
Apr. 28	Catchup and Review
May 6 (Wednesday)	**FINAL EXAM** (11:30am-2:00pm)

Major Assignments:

Your grade in this class will largely be determined by your performance on the homework and the two exams. However, you will also be expected to complete four or five programming projects.

Projects:

There will be four or five programming projects in this class. For tentative due dates, see the schedule above. Together they will comprise 30% of your grade.

Homework:

There will be several significant homework assignments (typically one every two weeks). Due dates will be posted on the course web site. Homework will largely be taken from the readings for each week, so it is important that you have each chapter read by the beginning of the week.

Exams:

The midterm exam will be held on Thursday, Feb. 20th and will comprise 10% of your grade.
The final exam will be held on Wednesday, May 6th and will be a comprehensive final exam that comprises an additional 10% of your grade.