CMSC 455: Network Security and Cryptography (3 credits)
Spring 2026

https://marmorstein.org/~robert/Spring2026/cs455.html

Lecture: 12:30pm – 1:45pm TR (Rotunda 354)
Instructor: Robert Marmorstein (marmorsteinrm@longwood.edu) **Phone:** (434)395-2185
Office Hours: 3:00pm – 4:00pm MF, 10:00am – 10:50am TR **Office:** Rotunda 331

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 Slack and suggest some possible times you can meet. In general, I need at least 24 hours of notice to schedule an appointment.

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 and Maura Paterson, CRC Press, 2017, Fourth Edition, ISBN: 9781032476049

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. Apply mathematical techniques to analyze the security and performance characteristics of cryptosystems
3. Implement modern ciphers and cryptological algorithms in a high-level language

Communications Policy:
The best way to reach 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 than if you send me an e-mail. Slack also allows me to easily set up a Zoom meeting (or Google Hangout) if we need to video chat.

When you send me a Slack message, I instantly get a notification on my computer, tablet, and phone. Typically, I reply to Slack messages within 24 hours (often sooner) on weekdays and sometimes even on weekends. I am much slower at replying to e-mail (since I do not get a notification and have to explicitly check it). Typically, you can expect a reply to an e-mail within 48 hours (longer on weekends).

Slack is also a good way to communicate with other members of the class. You will be invited to a public #cmsc-455 channel in which you can discuss the projects and other course topics with other students in the class. Feel free to ask for and give help on this channel, but please stick to general answers rather than posting code.

You can also reach out to me by e-mail to marmorsteinrm@longwood.edu. However, please do not send me large files by e-mail. They take up space toward my limited quota on the mail server and cause me all sorts of headaches. **E-mail messages containing large files will be deleted unread**.

Asking for help
If you are asking for help with a project or homework problem, you can send me a direct message through Slack. You should attach your code or your work to a Slack message so that I can see where you are at. You should do this by using the "paperclip" icon to attach the file directly to your message or by copy/pasting the particular snippet of code you are working on to the body of the message.

Please do NOT attach screenshots or pictures taken on your phone. They are hard to read and do not allow me to compile your code without retyping it. Instead, attach the .cpp or .h file directly to the Slack message. You will probably need to do this from a browser running inside your Linux virtual machine (or other Linux system).

One last suggestion: don't "ask to ask". I am delighted to answer questions about the projects and homework assignments and you should feel free to ask questions at any time. Asking permission to ask a question wastes my time and yours.

Course Structure and Student Expectations:
This course is very theoretical and **homework makes up the largest part of your grade.** However, the course 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 lectures. 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. Since we will be meeting in the lab, there will also be a computer on your desk. You should not log into or use this system during lecture.

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. **You may NOT use generative AI tools (such as Bard, Bing, or ChatGPT) to solve homework assignments or write projects.**

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.

You MAY NOT use generative AI in any way in this course.

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.

Course Requirements: 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%).

Intellectual property, Mental Health, and Reporting of Crimes and Sexual Misconduct:

This class complies with campus policies on wearing of face masks, intellectual property, disability accommodations, mental health, and reporting of crimes and sexual misconduct. For more information, see http://www.longwood.edu/academicaffairs/syllabus-statements/.

Disability Accommodations Policy: If have a disability and require accommodations for this course, I am happy to work with you, but you must (prior to receiving accommodations) do two things:

1. Register with with the Accessibility Resources Office in Brock Hall

2. Schedule a meeting with me early in the semester to discuss a plan for your accommodations.

Should you need temporary accommodations due to an injury or illness, you should reach out to both me and ARO and we can discuss how to meet your needs while you work with ARO to address your long-term needs.

Tentative Course Schedule (Please check the course web site for updates):

Jan. 15	Introduction to Cryptography and Cryptanalysis	**(Read Chapter 1)**
Jan. 20 – 22	Simple Substitution and Transposition Ciphers, Prime Factorization and Euler's Totient	
Jan. 21	**LAST DAY of ADD/DROP (Must add or drop by 5pm)**	
Jan. 27 – 29	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 Jan. 29)	
Feb. 3 – Feb. 5	Mathematics review: Matrix Multiplication, Determinants, and Matrix Inversion, Hill and Permutation Ciphers	
Feb. 10 – 12	Shannon's Theory and the One-time Pad **(Read Chapter 2)**	
	Lab 2: Cryptanalysis using a Dictionary Attack (Due Feb. 12)	
Feb. 17 – 19	Block Ciphers and the DES Cipher	**(Read Chapter 3)**
Feb. 24	Catchup and Review	
Feb. 24	**Symposium on the Common Good: NO CLASS for seniors in CTZN 410**	
Feb. 26	**Midterm Exam**	
Mar. 3 – 5	Introduction to AES Cipher	**(Cont. Chapter 3)**
Mar. 9 – 13	**Spring Break (No Class)**	
Mar. 17 – 19	Field Theory and Cryptanalysis of AES **Lab 3: Advanced Ciphers (Due Mar. 26)**	
Mar. 24 – 26	Cryptographic Hashing One-way functions, Counting Permutations and Combinations	**(Read Chapter 4)**
Mar. 31 – Apr. 2	The RSA Algorithm and Integer Factorization	**(Read Chapter 5)**
	Lab 4: Hashing (Due Apr. 2)	
Apr**. 1**	**Deadline to withdraw without an F (by 5pm)**	
Apr. 7 – 9	Pretty Good Privacy: PGP and GPG, Secure Sockets: TLS and SSL	**(Read Chapter 12)**

Apr. 14 – 16	Discrete Logarithm and Elliptic Curves	**(Read Chapter 6)**
	Lab 5: RSA And Public Key Encryption (Due Apr. 16)	
Apr. 21 – 23	Diffie-Helman Key Distribution	(**Read Section 10.1 and Chapter 11**)
Apr. 28 – 30	**Catchup and Review**	
May 7 (Thursday)	**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 roughly five programming projects.

Projects: There will be either 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. The Homework and Quizzes will be worth 45% of your grade.

Exams: The midterm exam will be held on Thursday, Feb. 26th and will comprise 10% of your grade. The final exam will be held on Thursday, May 7th and will be a comprehensive final exam that comprises an additional 10% of your grade.