

Syllabus -- Spring 2021

Course Info

Title. Introduction to Computer and Network Security (aka. Introduction to Cybersecurity)

Credits. 3.00 credits

Format. Online

Prerequisites. CSE2500

Meeting time. Tue/Thu 9:30 - 10:45 am.

Meeting location. Virtual at this Webex link

<https://uconn-cmr.webex.com/uconn-cmr/j.php?MTID=mc57390ad5508b591e782defc3960851d>

If for any reason Webex is not working well for the class, we will switch to another software.

Also, if for any reason we cannot synchronously meet at the class time on the above link (power outage, internet disconnection, etc.), a recording of the class will be posted on HuskyCT instead.

Course Description

This is the introductory course to the area of cybersecurity. The course focuses on applied cryptography, and some of its applications and related areas in cyber security, including network and web security, usable security, privacy/anonymity, and blockchains. Cryptography is among the most important tools when it comes to information, systems, and network security. The course does not require any prerequisite systems course, and has some overlap with more advanced courses such as cryptography and network security; we recommend to take it first.

The course will allow you to develop the security-thinking approach or mindset; define security goals, violations, attackers capabilities and their goals, design secure schemes and protocols, and then argue (somehow) formally about the security of these schemes and protocols.

We will discuss many practical vulnerabilities, attacks and defenses, which will allow you to build skills to identify and fix vulnerabilities in applied cryptographic schemes/protocols. However, especially in the beginning, we will also learn some theory - mainly, few definitions, and (fewer) proofs.

Instructor and Contact Info

Ghada Almashaqbeh

Email: ghada.almashaqbeh@uconn.edu

Office Hours. Every Tuesday 4 - 5 pm (any changes will be announced on HuskyCT) at <https://meet.google.com/jmq-scsn-jgv>, or by appointment (if you have questions and cannot make it please email me to arrange another time). Note that in the meeting room you might be waiting until the student ahead of you finishes (if needed). Please if you want to join the office hour email me first so I will be online. I will not open the above meeting link unless I know that a student wants to ask questions, discuss some course related issue, etc.

Also, feel free to start discussions on HuskyCT especially when you think that the question could be relevant to several students.

TAs

Eric Bueno

Email: eric.bueno@uconn.edu

Connor Lenz

Email: connor.lenz@uconn.edu

Office Hours. Eric will have a weekly office hour every Friday at 11:30 am - 12:30 pm using the following link: <https://meet.google.com/rdv-yuwr-neg> . Please let Eric know that you want to join the office hour to be online.

Communication

The lecture slides and covered material will be posted on the course website (usually the night before the class): <https://ghadaalmashaqbeh.github.io/teaching/> . Announcements, problem sets, solutions, homework submission, exams, discussions, and class recordings will be posted on HuskyCT. The use of HuskyCT discussion is highly encouraged (a forum for the class will be created). Please do not ask or answer the homework problem set on the discussion board.

I will be answering questions on HuskyCT on daily basis (will check it once or twice a day), the TAs will be following these questions as well at a higher frequency. For emails, I will answer in 24 - 48 hours once I receive your email, if for some reason you do not hear back from me within this timeframe, please feel free to send me a reminder. I will not answer emails over the weekend (Friday 6 pm until Monday 8 am).

Regarding points reviews/disputes; any requests to review graded homeworks/exams/etc. should be discussed with the instructor not the TAs.

Suggested Textbook

- *Foundations of Cybersecurity, volume I: An applied introduction to cryptography, Amir Herzberg.*
 - A draft is available at <https://sites.google.com/site/amirherzberg/applied-crypto-textbook>

Students are encouraged to read lecture notes/slides before and after lectures, and to solve exercises and examples (found in the textbook), preferably trying to do so without viewing the solutions and only then checking against the solutions (where available).

Note: the above URL contains the textbook slides. The slides used in this class will be an adapted version of the origin textbook slides (add extra information, remove uncovered material, etc.). So the course slides should be the ones posted at <https://ghadaalmashaqbeh.github.io/teaching/>

Grading and Course Work

Homeworks	40%
Quizzes	10%
Midterm exam	25%
Final exam	25%

Homeworks will consist of a small number of problems covering the material taken in class. There will be one assignment every one or two weeks. All submissions must be PDF format, the use of Latex is highly encouraged (you can use an online software for that like overleaf.com). You can use other word processors (like MS word) but the final submission has to be converted to a PDF.

Submission and late policy. The goal is to have 6-8 homeworks in total. The least homework grade will be omitted when computing the total at the end of the semester. This is a tentative plan that is subject to change based on the semester flow and our progress in the course material.

Each student will get 5 (free) late days. After using these days, a late submission will receive a 15% deduction of its score per day, with five days delay at maximum. After that, no late submissions will be accepted. Assignments will be graded no more than two weeks after they are due.

Collaboration. Homeworks are done and *submitted individually*. However, students are encouraged to discuss high level ideas with each other given that they write their solutions individually and list the names of the students with whom they discussed/collaborated in the submission. Copied solutions are considered cheating. You can collaborate with another two students at maximum (i.e., total is three students). I encourage you to solve the problems on your own first and then resort to group discussion for further understanding and brainstorming. Do not use other resources (outside of your textbooks and collaborators) to attempt to find the problem or the solution.

Exams. There will be a take-home midterm exam and a final exam. Exams are done individually, no collaboration between students, and questions about the exam are restricted to clarifying the problem set but not about the validity of the solution (or getting hints on how to solve a problem).

Midterm exam will be posted on the last day of the midterm exam period (Monday, 2/15/2021) and will be given 2 days to be submitted.

The final exam will be a 2-hour one done anytime during the exam day in one sitting, the exact date will be announced later based on the registrar policy for online exams.

Quizzes. There will be 5-10 quizzes (based on the material progress) spanning the last 5 or 10 minutes of a class (a quiz date will be announced). It will cover the material of the same lecture of the quiz date and the previous one.

Grading Scale.

Grade	Letter Grade	GPA
90-100	A	4.0
86-89	A-	3.7
82-85	B+	3.3
79-81	B	3.0
76-78	B-	2.7
73-75	C+	2.3
69-72	C	2.0
66-68	C-	1.7
65-67	D+	1.3
62-64	D	1.0
59-61	D-	0.7
0-58	F	0.0

As necessary the instructor reserves the right to decrease the minimum value for any assigned grade.

Course Schedule (Tentative, will be adjusted as needed)

Week of	Topic
1/19/2021	Introduction, encryption.
1/25/2021	Encryption and pseudo-randomness
2/1/2021	Encryption, Authentication
2/8/2021	Authentication, Hashing
2/15/2021	Hashing and Blockchains.
2/22/2021	Buffer / recitation
3/1/2021	Shared key protocols
3/8/2021	Key Exchange and Recovery
3/15/2021	Public Key Cryptosystems
3/22/2021	TLS
3/29/2021	PKI
4/5/2021	Buffer / recitation
4/12/2021	Spring Recess - no classes!
4/19/2021	Usable security
4/26/2021	Only Tuesday Class - Buffer / recitation Thursday is a reading day - no class
5/3/2021	Final exams period

Policies

Student Authentication and Verification. The University of Connecticut is required to verify the identity of students who participate in online courses and to establish that students who register in an online course are the same students who participate in and complete the course activities and assessments and receive academic credit. Verification and authentication of student identity in this course will include secure access to the learning management system (when accessing course material and tools on HuskyCT) using your unique UConn NetID and password.

Academic honesty. This course expects all students to act in accordance with the Guidelines for Academic Integrity at the University of Connecticut. Additionally, consult UConn's guidelines for academic integrity. The collaboration policy described above is designed to allow students the resources to succeed while ensuring they learn and master the material. If you are unsure if something is acceptable according to the collaboration policy, talk to me!

Violations of this policy will be considered violations of the academic integrity policy and will be reported to the Academic Integrity Hearing Board. Consequences may include (but are not limited to) failure of the class. Example violations include: not reporting collaborators, jointly writing solutions, copying or plagiarizing solutions and projects from other sources.

Student conduct code. Students are expected to conduct themselves in accordance with UConn's student conduct code (<https://community.uconn.edu/the-student-code/>).

Final exam policy. In accordance with UConn policy, students are required to be available for their final exam and complete any assignments during the time stated. If you have a conflict with this time you must obtain official permission to schedule a make-up exam with the Office of Student Support and Advocacy (OSSA). If permission is granted, OSSA will notify the instructor. Please note that vacations, previously purchased tickets or reservations, graduations, social events, misreading the assessment schedule, and oversleeping are not viable reasons for rescheduling an exam or for late delivery of assignments.

Copyright. My lectures, notes, handouts, and displays are protected by state common law and federal copyright law. They are my own original expression. Students may take notes. In addition, students will be consulted before using their solutions either with or without their name.

Students with Disabilities. The University of Connecticut is committed to protecting the rights of individuals with disabilities and assuring that the learning environment is accessible. If you are a student with approved academic accommodations through the Center for Students with Disabilities (CSD), please let me know immediately so we can discuss implementation. If you anticipate or experience any physical or academic barriers based on disability or pregnancy, you should contact the CSD to request accommodations at csd@uconn.edu or (860) 486-2020. Information about requesting accommodations is available on the CSD website at <http://csd.uconn.edu/>

Resources for Students Experiencing Distress. The University of Connecticut is committed to supporting students in their mental health, their psychological and social well-being, and their connection to their academic experience and overall wellness. The university believes that academic, personal, and professional development can flourish only when each member of our community is assured equitable access to mental health services. The university aims to make access to mental health attainable while fostering a community reflecting equity and diversity and understands that good mental health may lead to personal and professional growth, greater self-awareness, increased social engagement, enhanced academic success, and campus and community involvement.

Students who feel they may benefit from speaking with a mental health professional can find support and resources through the [Student Health and Wellness-Mental Health](#) (SHaW-MH) office. Through SHaW-MH, students can make an appointment with a mental health professional and engage in confidential conversations or seek recommendations or referrals for any mental health or psychological concern.

Mental health services are included as part of the university's student health insurance plan and also partially funded through university fees. If you do not have UConn's student health insurance plan, most major insurance plans are also accepted. Students can visit the Student Health and Wellness-Mental Health located in Storrs on the main campus in the Arjona Building, 4th Floor, or contact the office at (860) 486-4705, or <https://studenthealth.uconn.edu/> for services or questions.

Accommodations for Illness or Extended Absences. Please stay home if you are feeling ill and please go home if you are in class and start to feel ill. If illness prevents you from attending class, it is your responsibility to notify your instructor as soon as possible. You do not need to disclose the nature of your illness, however, you will need to work with your instructor to determine how you will complete coursework during your absence.

If life circumstances are affecting your ability to focus on courses and your UConn experience, students can email the Dean of Students at dos@uconn.edu to request support. Regional campus students should email the Student Services staff at their home campus to request support and faculty notification.

COVID-19 Specific Information: People with COVID-19 have had a wide range of symptoms reported – ranging from mild symptoms to severe illness. These symptoms may appear 2-14 days after exposure to the virus and can include:

- Fever,
- Cough,
- Shortness of breath or difficulty breathing
- Chills
- Repeated shaking with chills
- Muscle pain
- Headache
- Sore throat
- New loss of taste or smell

Additional information including what to do if you test positive or you are informed through contract tracing that you were in contact with someone who tested positive, and answers to other important questions can be found here: <https://studenthealth.uconn.edu/updates-events/coronavirus/>