UCONN
UNIVERSITY OF CONNECTICUT

CSE 3400/CSE 5850
Introduction to Computer and Network Security/
Introduction to Cybersecurity
Computer Science and Engineering Dept.

Syllabus -- Spring 2022

Course Info

Title. Introduction to Computer and Network Security (or Introduction to Cybersecurity)
Credits. 3.00 credits
Format. Online
Prerequisites. CSE 2500
Meeting time. Tue/Thu 3:30 - 4:45 pm.
Meeting location. Virtual at this Webex link
https://uconn-cmr.webex.com/uconn-cmr/j.php?MTID=m52b1694efd5fda49fd8b413486dabe4d

(usually no meeting password is required, if required it is `JhpkmJ3rD37`)

The course is mainly synchronous. Some classes, when needed, will be asynchronous where a video of the class will be posted on HuskyCT before the class starts.
Asynchronous classes will be announced in advance.

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 taking 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@uconn.edu

Office Hours. Every Tuesday 5 - 6 pm (any changes will be announced on HuskyCT) at https://uconn-cmr.webex.com/meet/gha20001 , or by appointment (if you 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).

TA

Anna Mendonca, anna.mendonca@uconn.edu
Office Hours. Every Wednesday at 11:45am – 1:15pm using the following link:
https://meet.google.com/xcs-jjbv-fkh

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.

We will also have a discord server for the course for questions/discussions. This will be set up and announced later by the TA. Please use it for general questions (problem sets, course material, logistics, etc.) but not to answer the homework problem set/exams or ask questions that expose the answers indirectly.

I will be answering questions on discord on a daily basis (usually once a day), the TA 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 TA.

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

Please note the book is being updated frequently. So make sure to fetch the latest version from the link above for each chapter.

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 are the ones posted at the course website under 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 (based on progress in the course material). 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 and the key solution will be posted.

Collaboration. Homeworks must be 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 two-hour online final exam. Exams are done individually, no collaboration between students is allowed, and questions about the exam are restricted to clarifying the problem set but not about the correctness of the solution (or getting hints on how to solve a problem).

Midterm exam will be a take home one, posted on Monday, 3/7/2022 at 8 pm, and will be given 2 days to be submitted (by Wednesday, 3/9/2022 at 8 pm the latest).

The final exam will be a 2-hour online 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 4 - 5 quizzes (based on the course progress) each spanning 5 minutes (a quiz date will be announced). The quiz will be open on HuskyCT immediately after class until midnight, you can take it anytime during that period but once you start the quiz you have to submit within 5 min. A quiz will cover the material of the same lecture of the quiz date and the previous one.

Letter grades. The following is a suggested grade scale to get an idea of the required total for a specific letter grade. The instructor reserves the right to curve based on the class average.

Grade	Letter Grade
(89, 100]	A
(84, 89]	A-
(81, 84]	B+

(78, 81]	B
(75, 78]	B-
(72, 75]	C+
(69, 72]	C
(66, 69]	C-
(63, 66]	D+
(59, 63]	D
(55, 59]	D-
[0, 55]	F

Course Schedule (Tentative, will be adjusted as needed)

Week of	Topic
1/17/2022	Introduction, encryption
1/24/2022	Encryption
1/31/2022	Encryption and pseudo-randomness
2/7/2022	Pseudo random functions and block ciphers
2/14/2022	Authentication
2/21/2022	Hashing
2/28/2022	Hashing and Blockchains
3/7/2022	***Midterm Exam (no class on 3/8/2022 for the exam)*** Shared key protocols (class topic for 3/10/2022)
3/14/2022	***Spring Recess - no classes!***
3/21/2022	Key Exchange and Recovery
3/28/2022	Public Key Cryptosystems
4/4/2022	Public Key Cryptosystems
4/11/2022	PKI
4/18/2022	TLS
4/25/2022	Buffer / recitation
5/2/2022	***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. 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: 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/