Syllabus for COMPSCI 466

Applied Cryptography

Term: Spring 2021	Instructor: ⟨PROF_FIRST_NAME⟩⟨PROF_LAST_NAME⟩
Time: TuTh 4PM - 5:15PM	Office: Zoom
Room: Zoom	Phone: N/A
Units: 3	E-mail: ⟨PROF_EMAIL⟩

Instructor Office Hour: TBD.

TAs: ⟨TA_FIRST_NAME⟩⟨TA_LAST_NAME⟩(⟨TA_EMAIL⟩),
⟨TA_FIRST_NAME⟩⟨TA_LAST_NAME⟩(⟨TA_EMAIL⟩).

TA Office Hours: TBD.

Please be respectful of our time and do not come for help outside office hours.

Text(s): We will follow slides by Mihir Bellare available at https://cseweb.ucsd.edu/ mihir/cse107/slides.html; however, I will modify them somewhat to suit our needs. These modified slides will be presented in class. You are responsible for the the material in the modified slides as presented in class. I will annotate my slides during class. An optional accompanying textbook is available at https://web.cs.ucdavis.edu/ rogaway/classes/227/spring05/book/main.pdf. I will point out the corresponding readings.

Description: This is an undergraduate-level introduction to cryptography. It is a theory course with a significant mathematical component. However, our viewpoint will be theory applied to practice in that we will aim to treat topics in a way of applied value. We will discuss cryptographic algorithms used in practice and how to reason about their security. More fundamentally, we will try to understand what security is in a rigorous way that allows us to follow sound principles and uncover design weaknesses. The primary topics are: blockciphers, pseudorandom functions, symmetric-key encryption schemes, hash functions, message authentication codes, public-key encryption schemes, digital signature schemes, and public-key infrastructures.

Prerequisites: COMPSCI 311. If you earned less than a B in COMPSCI 311, it is recommended you reconsider taking the class. Also note that the more fundamental prerequisite is *mathematical maturity*. If you have taken courses other than COMPSCI 311 that demonstrate this (*e.g.* complexity theory, number theory, abstract algebra, combinatorics), the instructor may waive the formal prerequisite. Please consult the instructor if you are not sure you have the right background.

Course Outline: We will essentially follow the topics of Mihir Bellare's slides in sequence, occasionally going on tangents to cover interesting techniques or applications (*e.g.* key revocation, TLS, cryptocurrencies). A tentative (subject to change) course calendar follows:

Feb. 2: Intro	Feb. 4: Intro
Feb. 9: Blockciphers, HW1 out	Feb. 11: Blockciphers
Feb. 16: Blockciphers, HW1 in	Feb. 18: PRFs
Feb. 23: PRFs, HW2 out	Feb. 25: PRFs
Mar. 2: Sym Enc, HW2 in	Mar. 4: Sym Enc
March. 9: Hash Fns, HW3 out	Mar. 11: Hash Fns
Mar. 16: MIDTERM, HW3 in	March. 18: MACs
Mar. 23: MACs, HW4 out	Mar. 25: MACs
Mar. 30: Comp. NT, HW4 in	April. 1: Comp. NT
April. 6: PK Enc, HW5 out	April. 8: PK Enc
April. 13: PK Enc, HW5 in	April. 15: PK Enc
April. 20: No class	April. 22: Dig. Sig.
April. 27: Dig. Sig., HW6 out	April. 29: Dig. Sig.
May. 4: Overflow, HW6 in	

This course syllabus provides a general plan for the course; deviations may be necessary.

Homework: There will be six homework assignments worth 100 points each. The assignments will be pencil-and-paper; there is no programming required. For the homeworks, you can work with one another as long as you explicitly list your collaborators for each problem. Additionally, *you must write your final solutions by yourself, as if you are taking your exam.* Failure to do so may result in a zero on the assignment. I will *not* take into account any material other than your written solution, such as program code, in your grade. It is highly recommended that you typeset your solutions in LaTeX. A template will be provided. Messy or illegible writing will not receive any points.

Make-Up Policy: There will be no makeups on homework. To allow for excused absences, I will drop your lowest homework score. Makeups on an exam will be given at the discretion of the instructor. A legitimate and verifiable excuse is required. If the excuse is approved, the makeup will be given within one week of the missed test.

Exams: There will be comprehensive (up to that point in the class) 100 points midterm as well as a comprehensive (across the entire course) 200 points final exam. The midterm and final will be conducted via Gradesource.

Grades: Your raw score in the class is computed as $.5 \cdot \mathsf{HW}/500 + .25 \cdot \mathsf{M}/100 + .25 \cdot \mathsf{F}/200$ where HW is your total number of homework points, M is your points on the midterm, and F is your points on the final exam. Your grade will be no lower than the following cutoffs on the raw score:

.8 to 1	A
.6 to .799	B
.4 to .599	C
$< .4$	F

Accommodation Statement: The University of Massachusetts Amherst is committed to providing an equal educational opportunity for all students. If you have a documented physical, psychological, or learning disability on file with Disability Services (DS), you may be eligible for reasonable academic accommodations to help you succeed in this course. If you have a documented disability that requires an accommodation, please notify me within the first two weeks of the semester so that we may make appropriate arrangements.

Academic Honesty Statement: Since the integrity of the academic enterprise of any institution of higher education requires honesty in scholarship and research, academic honesty is required of all students at the University of Massachusetts Amherst. Academic dishonesty is prohibited in all programs of the University. Academic dishonesty includes but is not limited to: cheating, fabrication, plagiarism, and facilitating dishonesty. Appropriate sanctions may be imposed on any student who has committed an act of academic dishonesty. Instructors should take reasonable steps to address academic misconduct. Any person who has reason to believe that a student has committed academic dishonesty should bring such information to the attention of the appropriate course instructor as soon as possible. Instances of academic dishonesty not related to a specific course should be brought to the attention of the appropriate department Head or Chair. Since students are expected to be familiar with this policy and the commonly accepted standards of academic integrity, ignorance of such standards is not normally sufficient evidence of lack of intent. See more information at http://www.umass.edu/dean_students/codeofconduct/acadhonesty.