Syllabus for COMPSCI 466

Applied Cryptography

Term: Spring 2020	Instructor: Adam O'Neill
Time: TuTh 11:30AM - 12:45PM	Office: LGRC (low rise) 329
Room: Engineering Laboratory 303	Phone: N/A
Units: 3	E-mail: adamo@cs.umass.edu

Instructor Office Hour: TBD.

TAs: Ojaswi Acharya (oacharya@umass.edu), Weiqi Feng (weiqifeng@umass.edu).

TA Office Hours: TBD.

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

Text(s): Slides by Mihir Bellare available at https://cseweb.ucsd.edu/ mihir/cse107/slides.html will function as our "textbook;" 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, not Mihir's, but reading both is recommended to reinforce the material. I will annotate my slides during class. I will post the unannotated slides about a week in advance and annotated slides following class.

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). The course calendar follows:

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

January					February				
Mon	Tue	Wed	Thu	Fri	Mon	Tue	Wed	Thu	Fri
		1	2	3					
6	7	8	9	10	3	4 PRFs	5	6 sym enc **HW2 out**	7
13	14	15	16	17	10	11 sym enc	12	13 hash fns **HW2 in**	14
20	21 intro	22	23 blockcipher **HW1 out**	24	17	18 **no class**	19	20 hash fns	21
27	28 blockcipher	29	30 PRFs **HW1 in**	31	24	25 msg auth	26	27 msg auth **HW3 out**	28
March					April				
Mon	Tue	Wed	Thu	Fri	Mon	Tue	Wed	Thu	Fri
2	3 auth enc	4	5 auth enc **HW3 in**	6			1	2 pub-key enc **HW4 in**	3
9	10 auth enc	11	12 **MIDTERM**	13	6	7 pub-key enc	8	9 digital sigs **HW5 out**	10
16	17 **spring break**	18	19 **spring break**	20	13	14 digital sigs	15	16 applications **HW5 in**	17
23	24 num theory	25	26 num theory **HW4 out**	27	20	21 applications	22	23 applications **HW6 out**	22
30	31 pub-key enc				27	28 overflow	29 .	30 review **HW6 in**	

In-class Policies: Please do *not* use electronics such as laptops and cell phones in class. If you feel you absolutely must use such an electronic device, please consult me first.

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 is in-class and the date is on the calendar. The date and time of the final exam will be announced later. All exams are closed book and other materials.

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

Note that you can compute your grade on each individual assignment or exam from this. Such grade cutoffs will be provided for convenience.

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.