Instructor: Adam O'Neill
adamo@cs.umass.edu

CS-690C: Foundations of Applied Cryptography

Course Description: This is a *three-credit* graduate-level introduction to cryptography, emphasizing formal definitions and proofs of security. Though the course is theoretical in nature, its viewpoint will be "theory for practice."

To appreciate this distinction, consider a notion like "one-way functions." This is one of the most fundamental notions in classical modern cryptography. But if you want a one-way function in practice, you use something like a hash function or blockcipher. And these objects (correctly designed) are conjectured to achieve much stronger security notions. So we do not treat one-way functions.

In particular, we will discuss cryptographic algorithms that are 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 cryptographic principles and uncover design weaknesses. Tentatively, we will cover: blockciphers, pseudorandom functions and permutations, symmetric encryption schemes and their security, hash functions, message authentication codes and their security, authenticated encryption schemes and protocols such as SSL/TLS, public-key encryption schemes and their security, digital signature schemes and their security, and public-key infrastructures.

The schedule and topics are subject to change according to the instructor or students' preferences.

NB: Cryptography is only one part of a much broader field of information security. In particular, we will not consider implementation issues in depth, nor will we cover topics such as viruses, worms, buffer overflow and denial of service attacks, access control, intrusion detection, etc. Students interested in these topics are advised to take computer and network security courses.

Time and Place. TuTh 2:30–3:45, via Zoom.

Requirements: (1) 3-5 homeworks (50%), take-home midterm (25%), take-home final (25%).

Grading: Approximate grading is as follows: 80-100: A, 65%-80%: B, 40%-65%: C, <40%: F. Plus (+) is awarded for the upper-third in each range, Minus (-) is awarded for the lower-third in each range.

Textbook: See "resources" on course website.

Prerequisites: Graduate standing or consent of instructor. Most importantly, students should have *mathematical maturity*, being comfortable reading and writing mathematical proofs.

Academic Honesty: 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`.

For problem sets, you are encouraged to discuss with others, **but you cannot discuss solutions in detail, have another student dictate to you their solution, copy something from their written solution, *etc.*** When you actually write your solutions you must do so by yourself as if you are taking an exam. You must also explicitly list all collaborators with whom you worked and any references or online material you used. The take-home exams are to be done entirely individually. You may use any resources from the course website.

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.