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

COSC 466: Applied Cryptography

Course Description: This is an undergraduate-level introduction to cryptography. It is "applied" in that the viewpoint will be "theory applied to practice," meaning we will aim to treat foundational topics in a way of applied value. 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. Thus, it is at its core a theory class, in the tradition of theoretical computer science. It is designed to be challenging, but also fun and informative.

Tentatively, we will cover: Blockciphers, pseudorandom functions and permutations, symmetric encryption schemes and their security, hash functions, message authentication codes and their security, public-key encryption schemes and their security, digital signature schemes and their security, and public-key infrastructures. Time permitting, we will also touch on more advanced applications and protocols.

Note that 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: TTh 4:00-5:15pm, CSB 142.

Requirements: (1) Bi-weekly problem sets (50%), (2) In-class midterm (25%), and (3) In-class final (25%). Late submissions or make-up exams will only be granted with documented extenuating circumstance (e.g. medical). The problem sets will be pencil-and-paper assignments; there is no programming required. For the problem sets, you are allowed to work with others, but you must list your collaborators separately for each problem and should write your final solution by yourself as if you are taking an exam.

Textbook: There is no required textbook. We will mainly follow slides by Mihir Bellare available at `http://cseweb.ucsd.edu/~mihir/cse107/classnotes.html`. Additional references with alternative viewpoints and more advanced material include Introduction to Modern Cryptography by Jonathan Katz and Yehuda Lindell (`http://www.cs.umd.edu/~jkatz/imc.html`) and A Graduate Course in Applied Cryptography by Boneh and Shoup (`https://crypto.stanford.edu/~dabo/cryptobook/`).

Prerequisites: CS 311 with a grade of 'C' or better. More fundamentally, the basic requirement is **mathematical maturity**. Here is a rough test for mathematical maturity: Go to the bookstore, pick up any undergraduate-level introductory textbook in higher mathematics (analysis, combinatorics, topology, or whatever), and start reading. With enough thought, are you able to follow what is going on? Are you interested and engaged? If so, that is a good indication.

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`.