CS 20594: Cryptography

Instructor: Mohammad Mahmoody

Credit Units: 3

Time and Location: Tues Thurs 3:30pm-4:45pm, Olsson Hall 011

Instructor: Mohammad Mahmoody (Rice 511) mohammad@cs.virginia.edu

TAs: Ameer Mohammed

Office Hours: Wed 11am-12pm 511 Rice Hall.

Goals: This is an advanced introduction to foundations of cryptography. We will go over basic tasks in cryptography (e.g., encryption, authentication) as well as more advanced and sophisticated tasks (e.g., zero-knowledge proofs, secure computation) and will end the course by going over some of the most recent developments (homomorphic encryption, obfuscation, etc.) The course will be proof based and will approach cryptography from a "constructive" perspective using rigorous mathematical proofs..

Objectives: The objectives of this course are two folded:

- Learning the basics of what is already developed: One goal of this course it to learn what theory of computation has contributed to the design of secure crypto systems. Basic and "traditional" objects (a.k.a. primitives) such as encryption and authentication (in their private-key and public-key setting) are among these tasks. Toward the end of this course, depending on the time, we would like to discuss more recent objects that are developed for the purpose of making advances systems (such as cloud computing) more secure.
- Analyzing new problems, defining security, and using the right assumptions: By the end of this course students should be able to analyze the security aspects of a system from theoretical perspective, come up with "right" security definitions, and use the primitives (or invent one!) to satisfy that notion of security. This would involve a "construction" and a "proof of security".

Textbook and Resources: The content of the course will largely be based on the book: Introduction to Modern Cryptography: Principles and Protocols, by Jonathan Katz and Yehuda Lindell.

We will also have a Piazza page in which you can find the videos of the class (shortly after the class) as well as my handwritten notes during the class. Piazza will also serve as a place for discussions after the class. There you can ask any questions you have about the material and other students as well as the instructor will provide their thoughts on that.

Prerequisites: The course requires CS 3102 (theory of computation) as prerequisite, which in turn requires the course CS 2102 (discrete mathematics). In addition, knowing the material of CS 4102 (Algorithms) extremely helps, but is not enforced. If you have taken the course Computational Complexity, it would suffice as well. The students who take this course should feel matured at mathematics and be comfortable with mathematical proofs.

Assignments There will be one take-home final exam. There will be 3 assignments that will (evenly) make the final grade. The assignments will be based on the material covered in class. Each assignment will also zero-credit (not graded) assignments that only serve as warm-up for the actual assignments and are to make sure that you do not miss the points that are not fully explored in class (but should be easy for you to fixture out).

In addition, students will have to do a research project. I will upload a set of possible topics for the project by the middle of the semester. Then you would have to choose your topic, or propose one after 2 weeks. The projects would involve writing short drafts and giving talks.

Grading: Each assignment (or final exam) will make about 25% of their grade. Each assignment will be due in 7-10 days (will be specified each time). Students can work on assignments in groups of one or two, but each person is supposed to write their own final version individually. Copying others' drafts is not allowed (see the honor code below). The collaboration should be limited to discussing concepts and perhaps sketching a solution, but then each person should write their own solutions individually.

Honor Policy: All assignments are subject to the UVa's honor policy. Placing your name on an assignment implicitly pledges that you abide by the terms of this policy.