COSC 530: Introduction to Cryptography

Course Description: This is a graduate-level introduction to cryptography, emphasizing formal definitions and proofs of security. Though the course is theoretical in nature, its 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 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, public-key encryption schemes and their security, digital signature schemes and their security, and public-key infrastructures.

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. MW 2:00-3:15pm, St. Mary’s 326.

Requirements: (1) Complete weekly or bi-weekly problem sets (70%), and (2) complete a course project (30%). Possibilities for the course project include implementing a scheme we discussed, summarizing a research paper, or doing your own research project.

Textbook: There is no required textbook. We will mainly follow slides by Mihir Bellare available at http://cseweb.ucsd.edu/users/mihir/cse207/classnotes.html. Note that the above link also has course notes, but these are somewhat out-dated. For students who also want an additional hardcopy reference, we recommend Introduction to Modern Cryptography by Jonathan Katz and Yehuda Lindell (http://www.cs.umd.edu/~jkatz/imc.html).

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

Academic Honesty: Academic honesty is taken very seriously. For problem sets, you are encouraged to work with others, but 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. Most importantly, never turn in something that you don’t understand! I reserve the right to ask you to explain to me something you turned in, and if you cannot do so in a way that demonstrates your understanding, you will not receive credit and may be reported to the University.