Computer Sciences, UW–Madison Spring 2011
CS 838: Applied Cryptography **Instructor:** Thomas Ristenpart
Course Information January 18, 2011

Course Information

Meets: Tu and Th, 9:30AM–10:45AM in ENGR Hall 2239

Instructor: Thomas Ristenpart

Office: 7395 Computer Sciences

E-mail: rist@cs.wisc.edu

Course Web Page: `http://pages.cs.wisc.edu/~rist/cs838-spring2011/`. Slides, course notes, and problem sets will be posted there. (Hardcopies of these items will not be provided.)

Office hours: See course web page.

Contents: This course is an introduction to applied cryptography. Today's cryptographic systems are increasingly designed and evaluated via the "provable-security" tradition of modern cryptography. Consequently, a major theme of the course will be understanding provable security in the context of applied cryptography. We will spend a lot of time understanding how to formally define security goals, choose appropriate adversarial models, and prove correct protocols relative to these goals and models. In parallel, we will be exposed to cryptographic standards and implementations used everyday by hundreds of millions of people.

Texts: We will use a relatively comprehensive set of lecture notes written by Bellare and Rogaway. They will be available via the web page. There will also be slides made available; the slides will form the the basis of most lectures.

Pre-requisites: Computer algorithms, probability theory, randomized algorithms, some basic complexity theory (eg. $\mathbf{P}, \mathbf{NP}$, $\mathbf{NP}$-completeness, reducibility between problems) and, most importantly, general "mathematical maturity." This last just means being comfortable with mathematical definitions and proofs.

Homeworks: I will assign some number of problem sets (also called homeworks) throughout the course. Each individual should turn in a writeup. If you discuss a problem with anyone (in the class or otherwise) or use sources beyond those I provide to solve the problem, then you should explicitly indicate so in the writeup. Looking up solutions outright on the Internet is not allowed. Solutions are encouraged to be typeset using LaTeX.

Problem sets might contain extra credit problems. Doing these is entirely optional, though I recommend students interested in pursuing research in the area should attempt them.

Projects: The course requires completing a term project. These can be done individually or in groups. The goal is to go in depth in some topic related to applied or theoretical cryptography. A target will be term projects that can eventually lead to publishable research, though this will certainly not be required to do well on in the class.

A project could be an extension to some existing research paper, an implementation of a not-before-implemented cryptographic protocol, (provable) security analysis of a protocol or implementation, a meaningful enhancement of a widely-used open source cryptographic library (e.g., OpenSSL or OpenSSH), or some combination of the above. Groups could team up to, for example, both develop an implementation and provide a theoretical analysis of the implemented protocols.

Timeline for projects:

- Feb 8, 2011: one page proposal due
- Feb 14–18, 2011: brief meeting with me to discuss proposal
- Apr 4–8, 2011: brief meeting with me to discuss project progress
- Apr 28, 2011: short write-up due in class
- Apr 28, May 3,5 2011: project presentations in class

Project selection should be done with my consultation, so feel free to grab me at any point to discuss your ideas or ask for suggestions.

Final discussion: In the last week of the term, each student will be expected to meet with me for a short discussion. Be prepared to briefly present your project (no slides necessary), particularly if you worked in a group. Discussion might also include other technical topics from the course. The goal will be for me to assess how much you learned.

Grading: Grades will be assigned based on class participation, quality of the final project, and quality of problem set solutions. This is an optional graduate level course, and so I expect that grades will tend to be high.