Computer Sciences, UW–Madison
CS 838: Applied Cryptography
Course Syllabus

Spring 2012
Instructor: Thomas Ristenpart
January 24, 2012

Course Information

Meets: Tuesday, 4:00PM–6:30PM in CS 1263

Instructor: Thomas Ristenpart

Office: 7387 Computer Sciences

E-mail: rist@cs.wisc.edu

Course Web Page: `http://pages.cs.wisc.edu/~rist/cs838-spring2012/`. Slides, course notes, and problem sets will be posted there. (Hardcopies of these items will not be provided.)

Contents: This course is an introduction to modern 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 in-use 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.

Texts: The Bellare-Rogaway lecture notes (on web page) are nearest close reference. The Katz and Lindell textbook "Introduction to Modern Cryptography" is the next best reference. 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. **P**, **NP**, **NP**-completeness, reducibility between problems) and, most importantly, general "mathematical maturity." This last just means being comfortable with mathematical definitions and proofs.

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

Homeworks: I will assign some number of problem sets (also called homeworks) throughout the course. These will only be spot checked by me. These are entirely for your benefit: learning the theory underlying modern cryptography is best done by getting one's hands dirty. 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.

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.

A project could be an extension or continuation of an ongoing research project, extension to a paper, an implementation of a not-before-implemented cryptographic protocol, 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.