CS/ECE407 Cryptography – Midterm Topics Guide

The midterm exam will take place on Thursday, March 12 at 3:30-4:50pm in ECEB 2013.

You may a single sheet of notes. Your notes may be typed or hand-written (or both), and you may use both sides of the paper.

The exam itself will be a combination of two types of questions:

- Multiple choice, true/false, matching type questions.
- Free response questions.

In preparing for the exam, I recommend (1) reviewing the homework problems, (2) reviewing lecture slides, and (3) reviewing entries in the textbook. If you are interested in another resource, you can look at the partially-complete (and free) textbook here for additional discussion and exercises.

This guide lists the topic areas that might appear on the exam. Topics that are listed in **bold might appear as a free response question** (and those that are not in bold can only appear as a multiple choice, true/false, etc.)

While this guide is intended to help you prepare, **this guide is not a binding document, and I reserve the right to ask exam questions outside what is described here.**

In general, the midterm will cover topics of **symmetric-key cryptography** and **the rudiments of provable security**.

The Theory of Cryptography

- The methodology of modern cryptography
- Kerckhoff's Principle
- **Perfect Secrecy**
- **One-time pads**
- The relationship among PRFs/PRGs/OWFs/PRPs

Rudiments of Cryptography from Computational Hardness

- **The notion of a poly-time adversary**
- **The definition of indistinguishability**
- **The notion of a distinguisher**
- **The notion of a security reduction**
- **The notion of a hybrid argument**
- Negligible Functions

Symmetric-Key Cryptography

- **PRGs**
- **PRFs**
- Block Ciphers/PRPs
- Block Cipher modes of operation
- **MACs**
- **CPA security**
- CCA security
- Authenticated encryption (with associated data)
- Collision-resistant hash functions
- **Random Oracles**