The University of North Carolina at Greensboro
CSC 580: Cryptography and Security in Computing
Prof. Stephen R. Tate

Handout 6
March 3, 2014

Midterm Information

The CSC 580 midterm will cover material from Chapters 1–6 in the textbook, and the two outside readings (available on the web page). Questions will deal with definitions/terminology, short answer questions testing concepts, and problems to work out.

To review, I would suggest first going through the "Key Terms" and "Review Questions" at the end of each chapter, as well as the chapter reading questions that I distributed for each chapter. I would strongly recommend working on solutions to the chapter reading questions in Piazza — I will check Piazza regularly, and when there is a good answer for any of these questions, I will mark it as a "Good Answer" I will also give suggestions for answers that need improvement.

Beyond those basic questions, review your homeworks and the feedback I gave on your answers. I won't give you problems as hard as the homework problems that you haven't seen yet, but I might give you a variant of a homework problem that had been assigned — so understand the correct answers!

Finally, I will add a few additional questions to Piazza, similar to the type and level of problems that you'll see on the midterm. These are good practice, so you are encouraged to work on them! What follows is a quick outline of what I think are the most important topics in each chapter. This is *not* a complete list of things you need to know!

Chapter 1 – Overview. The purpose of this chapter is to introduce basic concepts and terminology, and to give a good "big picture" of computer security. The most important parts of this chapter are terminology as it is used to classify security goals, types of attacks, etc.

Chapter 2 – Classical Encryption Techniques. The important aspect of this chapter is to get you thinking about cryptography in simple terms. The classical ciphers aren't really important in and of themselves, with a few exceptions: (1) you should understand the basic concept of a monoalphabetic substitution cipher, and the modular arithmetic properties that were revealed by considering affine ciphers with "mod 26" arithmetic; and (2) the one-time pad is important.

Chapter 3 – Block Ciphers and the Data Encryption Standard. While DES is not used a lot these days, there are some very important concepts introduced in this chapter, including operations on binary values (especially the XOR operator), the basic block cipher concept, and round-based block ciphers such as the Feistel network.

Chapter 4 – Basic Concepts in Number Theory and Finite Fields. There's lots of important mathematical basics in this chapter, with the three most important topics being modular arithmetic (and its properties), Euclid's GCD algorithm (and the use of the extended algorithm for finding multiplicative inverses), and finite field operations (interpretation with polynomials and the binary/hexadecimal notation).

Chapter 5 – Advanced Encryption Standard. This is the most widely used symmetric cipher, so it is important to understand. The most important parts are the basic parameters (block and key sizes), but you should know the basic structure (the 4 building blocks) and have a good feel for efficiency/speed.

Chapter 6 – Block Cipher Operation. The most important part of this chapter is understanding block cipher modes. The ones you absolutely must understand very well are ECB, CBC, and CTR modes, and understanding things like dependencies and error propagation is important. The importance of randomizing these modes with appropriate IV or counters is also important.