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

Handout 6
December 5, 2011

Review Sheet for Final Exam

The final exam in this class will be Wednesday, December 7, from 3:30 – 6:30 (it will be designed for 90 minutes, but you will have the entire three hours if you'd like it). The exam will focus primarily on material covered since the last exam, but will include questions from material covered on the first two exams, as well as questions which try to pull everything together. Make sure you review the terminology that was introduced in these chapters (terms are given at the end of each chapter).

Earlier exams provided pretty thorough coverage of Chapters 1 – 9. The following is a list of the main topics we have covered since the last exam:

- Sections 10.1–10.2 (Diffie-Hellman and ElGamal)
- Chapter 11 (Cryptographic Hash Functions)
- Sections 12.1–12.5 (MACs and HMAC)
- Chapter 13 (Digital Signatures)
- Chapter 14 (Key Management and Distribution)
- Basics of network/IP protocols and controls (firewall and intrusion detection concepts and terminology)

The final exam will be similar to earlier exams, except that there will be more problems to work out, including one "challenge" question that requires you to think more creatively about the topics we have covered. For this question you will have at least 2 alternative questions, and you only need to solve one of them. Here's a sample "challenge question":

- The country of Oceania has decided to outlaw encryption but to allow integrity-protecting technologies such as hash functions and digital signatures. Since the policy-makers know that hash functions are "one-way", they figure people can't use them for encryption. However, any secure hash function can be turned into a secure symmetric cipher. Devise a way to do this. Some answers are better than others, but I don't expect perfection here — you simply need to have a reasonable approach: describe why you think your particular technique is secure.

On the back of this page are samples of the more standard exam questions.

- What are the requirements of a cryptographic hash function (hint: the book listed 6 properties)? Give a brief (one sentence) description of each.
- Both MACs and digital signature schemes are designed with the goal of being resistant to "existential forgery." Describe what this means and why this is an important property.
- What is a certificate and what role does it play in the distribution of public keys? Describe what a certificate does, what it protects against, and how it does this.
- Give three different types of firewall, with a brief description of each. Make sure it's clear how the different types are actually different.