CPTR 427 Review for Final Exam

Review of the second half of the semester

This review covers the second half of the semester. The final exam will be comprehensive in nature, so make sure you see the midterm review in addition to this one.

Notice when I ask for detailed explanations for the questions on this review, I want *all* the details. Try to keep your answer orderly and concise. E.g. do not use terms and ideas you don’t describe or describe as an afterthought. Think about your answer and how you should write it and then start writing.

# Cryptography and Network Security

## Chapter 9

Know RSA! An RSA simple decrypt will be on the exam, so bring your calculator. (See example on p 271) Also you will be required to generate a public and private key pair from two primes that I will supply.

## Chapter 11

1. Name the attacks on authentication when communicating across a network. (p 319)
2. Differentiate between a MAC and a one-way hash function. (11-5/6)
3. Name three desirable properties of hash functions (p 341)
4. Is it necessary to recover the key to attack a MAC algorithm? (11.8)
5. Be able to describe in general what a birthday attack is and specific ally how it is used with hash codes (11.4).

## Chapter 12 Hash and MAC

1. How is a password used in an HMAC? (12.3)
2. Why has there been an interest in developing a message authentication code derived from a cryptographic hash function as opposed to one derived from a symmetric cipher? (12.5)

## Chapter 13 Digital Signatures

1. List two disputes that can arise in the context of message authentication. (13.1)
2. Describe a digital signature in terms of properties and requirements. (13.2/3)
3. List three general approaches to dealing with replay attacks in digital signatures. (13.8)

## Chapter 14 Kerberos and X.509 Certificates

1. Be able describe the entities and processes involved in acquiring access to a resource protected by Kerberos. (Figure 14.1 and 14.2)
2. Describe an SSL certificate. What cryptographic elements do you find there? (14.2)

## Chapter 16 IPSec

1. Describe IPSec. Make sure to include:
   1. SA
   2. AH
   3. ESP
   4. Modes (transport vs. tunnel)
2. Give two example applications that may use IPSec.

# Labs

See the questions on the Lab Handouts online.