**CSCI 6345 FINAL EXAM REVIEW**

Dear students: please study notes, ppt slides and lecture recordings. This review will serve only as a guide. Please check this site frequently for updates.

1. Several questions on IPV6 address. I covered essential material in class.
2. Questions on DHCP server and client such as configuration, lease, renewal, relay, scope, etc.
3. Several questions on cryptography, both symmetric and asymmetric, such as difference between them, which is appropriate for long messages, short messages, how are asymmetric keys used for encryption at the senders side, what is done at the receivers end, how is non-reputiation accomplished?
4. Routing in ASs, Inter domain and Intradomain, specific protocols used for each, and matrics used.
5. Specific questions about bridging and parts of a router.
6. Several questions on UDP and TCP. Difference between them, layers under which they function, how do they enhance IP? How do you create a socket? When do you use stream or datagram? Know SYN, ACK, SACK, attacks, sequence number, Rwnd, window size, ACK value, flow control, etc.
7. Given a CIDR, give beginning, ending, and total number of addresses. How is a class determined given and IP address.
8. Direct vs. indirect delivery, how routing tables and ARP used for these. Static and dynamic routing tables, their advantages and disadvantages, how many tables?
9. Several questions on each field in the header. You will need to calculate several values and explain packets received. Also several questions on fragments (why fragmentation is necessary) and necessary flags and fields. Explain TTL. What information is needed to put a fragment back together?
10. Questions on supporting protocols such as NAT,ICMP, ARP, RARP, BOOTP, DHCP; which is pre-boot?

**Study**

Security Question: If Alice wants to send Bob an encrypted message using asymmetric Key how it done? How would it differ from a symmetric key encryption? What is digital signature? Ho could Alice be sure that a message was sent by Bob?

A packet with 4000 bytes needs to be sent. Fragmentation is allowed. It first passes through a network with a MTU of 1400, later it travels through a network with a MTU of 800. Show the fragments formed in the first network, and show the second fragment from this one being fragmented as it travels through the second network. I am looking specifically for Header length, Total Length, fragmentation flags, and fragment offset fields. Also show the byte numbers in each fragment. Also, explain how reassembly takes place.

Compare and contrast physical vs. IP address schemes. Make sure to include: (a) How these addresses are assigned, (b) Under which layer in which each layer operate, (c) How an unknown destination address is discovered (what protocols or servers are used), (d) One of these addresses can be divided into two parts, what are they and how can these parts be isolated?

Several methods of gaining access to the media (MAC layer responsibility) were described in class. Explain the most common one. Explain static allocation models and collision free protocols.

Explain sliding windows as related to TCP how it is used to control flow rate. Discuss IGRP and EGRP, and differentiate between RIP and OSPF.

Alice sends a digitally signed document to Fred. Describe the process of digital signature and how Alice can’t repudiate. If she wants to send the signed document securely, how can that be done

**Problems**

A packet has arrived with M bit value of 1 and fragmentation offset is zero. Is this first, middle or last fragment? Explain. What if the offset was 100, what would be the first byte number (from the original whole packet) in this fragment? Explain.

An IP datagram arrived with the following in the header (HEX – I ADDED THE SPACE FOR CLARITY):

45 00 00 54 00 03 00 00 20 06 00 00 7C 4E 03 02 B4 0E 0F 02