CNT 4704: Network Analysis
Final Exam

Prof. Cliff Zou
Dec. 9, 2015

Instructions:

- The exam is open everything, including books, notes, and computers.
- The total number of points for each question is given in parenthesis. There are 100 points total.
- Show all your work. Partial credit is possible for an incorrect answer, but only if you show some correct intermediate steps in obtaining the answer.

Affidavit:

I certify that I have finished this exam solely by myself without any discussion or help from any other person.

Student Name:

PID:

Question 1: Knowledge questions (18 points)

Answer each of the following questions *briefly*.

a). What is the size of TCP header (without optional field)? UDP header? IP header?

b). What is the full names of CSMA/CA and CSMA/CD? Why wireless LAN uses CSMA/CA instead of CSMA/CD?

c). What are the basic differences between Ethernet switch and Ethernet hub?

d). What is the maximum transmission efficiency for pure ALOHA? for slotted ALOHA?

e). What is public key cryptography and symmetric key cryptography? The advantage and disadvantage of each?

f). How many different types of data link frames does WiFi protocol have? Their names?

Question 2: CRC Computing (15 points)

Suppose the divider G is 1101, the data D has value of 10010101, 10100010, and 01011101, respectively. What is the value of R (i.e., CRC code) for each data D? Show your calculation procedure.

Question 3: Public Key Crypto (11 points)

Based on the notations and symbols used in the textbook, a web server has a pair of public/private keys (K^{+}_{s}, K^{-}_{s}). Suppose the Certificate Authority has its own public and private keys of (K^{+}_{ca} , K^{-}_{ca}).
(1). Give the formula representation of the server's Digital Certificate signed by the above certificate authority.
(2). Suppose the webserver sends out a message *m*, provide the formula representation of the message's Message Digest, and Digital Signature?

Question 4: Subnet Addressing (20 points)

Suppose a company has been allocated with the IP space of “128.119.128.0/17”.

a). How many IP addresses does this subnet have? Show the last IP address of this address space.

b). If the network administrator wants to break this network into 3 subnets. The first subnet has half of the address space, the remaining 2 subnets each has 1/4 of the address space. The IP addresses of these 3 subnets have sequential order, i.e., the IP addresses in subnet k is smaller than the IP addresses of subnet k+1, (k=1,2). What are these subnets? (note: each subnet should be represented by prefix format)

Question 5: Classical Crypto (16 points)

(1). Suppose the cybertext “`vyfo iye`” was generated by using Caesar Cipher. Please find out its plaintext (two meaningful words) and the shifting key used in this encryption.
(2). Using Vigenere Cipher with this 4-digit shifting key “4, 8, 12, -1”, encode message "this is an easy problem."

Question 6: Network Probing (20 points)

Please use the knowledge and online resources taught in class to answer the following questions (you can use other online resources, too). You must explain the procedure (or online resources) you have used to obtain the answers:
(1). Find out what are the domain name(s) of the email server (or servers) responsible for this email address: savage@cs.ucsd.edu
(2). Find out in which US city and which ISP owns this IP address: 128.119.240.84
(3). Find out what IP subnet has been allocated to Apple Computer Inc.? How many IP addresses does Apple company own?