Washington State University
CptS 455 Fall 2013 Sample Final Exam
Final exam is December 9, 2013 at 8AM in the regular room

Your name: _____

There are 5 pages, 11 numbered questions on 3 sheets (front and back). Please check to make sure your exam is complete before starting. You may have one 8 1/2 x 11 sheet of notes (both sides, typewritten or handwritten). Otherwise, this is a **closed book, closed notes, closed neighbor** exam. Calculators are allowed.

1. (15) a. Suppose there are 3 wireless nodes A, B, and C.
   a. Describe a geometric configuration of the 3 nodes and their wireless communication ranges in which the "hidden terminal" problem could arise for node A when it tries to communicate with node B.

   b. Given the geometric configuration you describe in part (a) describe what happens when node A sends to node B while node C is also transmitting.

   c. Describe a collision-avoidance protocol that can help solve the hidden terminal problem.

2. (10) An 802.11 network in infrastructure mode uses 3 MAC addresses in its headers.
   a. When a mobile node sends a packet, which devices' MAC addresses are in the link-layer header (in any order)?

   b. How does the mobile node learn each of the three MAC addresses it uses in the headers that it sends? (Hint: the answer is different for each of them)

3. (15) In a public-key encryption system we use $K_B^+(m)$ to denote message *m* encrypted or decrypted using party B's *public* key and $K_B^-(m)$ to denote *m* decrypted or encrypted by B's *private* key. Further $K_B^+(K_B^-(m)) = K_B^-(K_B^+(m)) = m$.
   a. Using the notation above with K_B (with appropriate +/- superscripts) standing for Bob's keys and K_A standing for Alice's keys, if Alice wants to send a secret message *m* to Bob so that only he can read it what does she send?

   b. Similarly, using the notation above, if Bob wants to send a message *m* to Alice so that she can be sure that it came from him, what does he send?

   c. If Bob and Alice have a lot of messages to send to one another public key encryption may be rather costly in terms of the amount of computation required. How can Bob and Alice leverage the power of public key cryptography to achieve secret communication without incurring the cost of public key cryptography for every message?

4. (10) Suppose Alice wants to send message *m* to Bob. Alice and Bob share secret *s* and have agreed to use cryptographic hash function *H* to implement a message authentication code (MAC).
   a. What does Alice send to Bob?

   b. What does Bob do when he receives the message from Alice?

5. (20) Consider RSA with $p = 5$ and $q = 23$. (Show all work!)
   a. What are *n* and *z* ?

   b. Let *e* be 49. Show that this is an acceptable choice for *e*? (Show calculations to prove it, don't just state the rule)

   c. Show that the corresponding decryption key, *d*, is then 9. (Show calculations)

   d. If the cyphertext is 2 what is the plaintext? (Show calculations)

6. (15 pts) What are the layers of the IETF IP protocol model. Describe the service(s) provided by each layer.

7. (15 pts) Consider a communication link with round-trip latency of 50 msec., and bandwidth 125 kbyte/s.
   a. What is the bandwidth-delay product for this link?

   b. What is the required *window size* in order to achieve the maximum bandwidth?

   c. Suppose you observe (perhaps using a tool like Wireshark) that the *receiver's advertised window size* of a TCP connection traversing this link is almost always *much* smaller than what you answered for part b. What are some possible causes?

8. (10 pts) Suppose `int` variable `s` is a TCP socket, `char *` variable `buf` points to a character buffer, and `int` variable `msgLen` contains the length of the message held in `buf` that you want to send on `s`. What code do you have to write in C to do this?

9. (10 pts) Suppose `int` variable `s` is a TCP socket, `char *` variable `buf` points to a character buffer, and `int` variable `msgLen` contains the amount of data that you want to read from `s` into `buf`. What code do you have to write in C to do this?

10. (10 pts) Which socket system calls would typically be used in a **server** using the **UDP** (not TCP) protocol and in what order?

11. (10 pts) What is the difference between *flow control* and *congestion control* for TCP?