CMPT 371, Final Exam

1. (20 points: 2×10) Short questions.

(a) Encryption using a private (symmetric) key is more efficient than using a public key system. True or false:

(b) A DNS query, as well as asking the IP address corresponding to a domain name, can also be asking for a domain name for a given IP address. True or false: ______________

(c) To make sure that public keys are authentic, they are signed by ______________

(d) ______________ ALOHA is more efficient in terms of throughput than ______________ ALOHA.

(e) If Alice signs a message \( m \), obtaining \( m' \), can Trudy, if she intercepts \( m' \), obtain the original message \( m \)? Yes or no: ______________

(f) A switch operates on the _________ layer. A hub operates on the _________ layer.

(g) BGP can be configured to ignore shortest path routing. True or false: ______________

(h) TCP guarantees in-order delivery of segments. True or false: ______________

(i) ______________ is a protocol for moving mail between mail servers.

(j) On a graph with \( n \) nodes, \( m \) links, and \( t \) multicast nodes, the size of the minimum multicast tree (ie, the number of links that it contains) is at least ______________

2. (10 points) Consider a local area network with a bus topology where two of the nodes are A and B. The distance from A to B is \( x \). The bandwidth of the bus is \( b \) and the speed of data on the link is \( c \). If A and B are using CSMA/CD, what must be the length of a frame (please specify “at least” or “at most” such that A and B collide but do not detect it? If you need to make any assumption on any parameter of the system, please write them down.
3. (20 points: 10+10) Security.
   (a) Assume that Alice has a message to send to Bob. She first signs it, then encrypts, both using RSA. What is the function that Bob has to compute in order to obtain the original message? Write in the notation that I used in class; I will not accept answers of the form “Bob first checks the signature then decrypts” etc.
   (b) How would an encryption system such as PGP combine symmetric and public key cryptography? What is the purpose?

4. (20 points: 5 + 15) Network layer.
   (a) How many IP addresses are there in the space 123.64.0.0/10?
   (b) Is it possible for the cost of the minimum multicast tree to be more than the cost of the reverse path forwarding tree? Argue. How about more than the cost of the minimum spanning tree? Is it possible to run two http servers in a network behind a NAT server? Explain.

5. (15 points: 10 + 5) Earlier topics.
   (a) What is the mechanism for flow control in TCP?
   (b) What function does MIME serve?

6. (15 points) Consider Slotted Aloha where host A and B have just collided. Assume that $p = 1/2$. If we assume that no other node will want to transmit in the foreseeable future, what is the probability that after 3 time slots neither A nor B has been able to transmit successfully? For extra credit, can you generalize this to $k$ time slots and general $p$?