Student ID: ___________________

CS457: Computer Networking
Date: 5/8/2007
Name: ________________________

Instructions:

1. Be sure that you have 10 questions
2. Write your Student ID (email) at the top of every page
3. Be sure to complete the honor statement after you complete the exam
4. This is a closed book exam
5. The seats on both sides of you should be empty
6. State all assumptions and be sure your answers are legible
7. Show all work; the graders will give partial credit
8. Answer each question clearly and to the point; do not define or describe concepts unless asked to do so; assume that the graders are familiar with the concepts

Question	***Points***	***Score***
1	10	
2	10	
3	10	
4	10	
5	10	
6	10	
7	10	
8	10	
9	10	
10	10	
total	**100**	

Student ID: ____________________

1. Answer the following True/False questions by circling either **T** or **F.**

    1. 100% redundancy (ie. transmitting every bit in a packet twice) provides perfect bit error detection T [✓ F]

    2. Partitioning schemes (TDMA, FDMA) are better than random access schemes (Aloha, CSMA) when all nodes have packets to send [✓ T] F

    3. CDMA works with both wired and wireless networks T [✓ F]

    4. Wireless links provide a "broadcast" channel where every node hears every other node T [✓ F]

    5. Using "Ingress Filtering" on all routers would solve the IP spoofing problem [✓ T] F

    6. SSL uses both public key and symmetric key cryptography [✓ T] F

    7. FTP is a stateless protocol T [✓ F]

    8. UDP implements congestion control but not flow control or reliability T [✓ F]

    9. Some link layer implementations provide reliable delivery and flow control [✓ T] F

    10. All nodes on the Internet have a Physical Layer implementation [✓ T] F

Student ID: ____________________

2. **Random Access Protocols**

a. With the Slotted Aloha protocol, how long does a node wait once it gets a new frame to transmit? Can there be collisions and, if so, what does the node do when there is a collision?

The node waits until the next time slot and tries to transmit. If there is a collision, it will try to retransmit in each subsequent slot with probability *p*.

b. How is pure (unslotted) Aloha different from slotted Aloha? What effect does this have on efficiency (the long-run fraction of time with successful transmissions)?

In pure Aloha, the time slots of different nodes are not synchronized. This makes it twice as likely to have a collision.

c. How is CSMA different from unslotted Aloha?

In CSMA, the node senses the carrier signal and only sends when no other packets are being sent.

d. How is CSMA/CD different from pure CSMA?

In CSMA/CD, the node listens for other packets while it transmits. If another packet is detected, it sends a short jamming signal and then stops transmitting.

e. How is CSMA/CA different from CSMA/CD?

In CSMA/CA, the node waits a random amount of time before sending any packet (instead of only after a collision). It also uses ACK packets to detect collisions.

Student ID: ____________________

3. **Hubs, switches, and routers**

a. What is the difference between a hub and a switch? What effect does this have on the "collision domain"?

A hub is layer 1, a switch is layer 2. A hub immediately transmits every incoming bit from any link to all other links. Thus, all nodes are in the same collision domain. A switch buffers incoming packets and transmits them according to the MAC protocol of the outgoing link(s). Thus, nodes on different links are in different collision domains.

b. What is the difference between a switch and a router? What effect does this have on the number of times they must forward a message.

A switch is layer 2, a router is layer 3. A switch builds its switch table by eavesdropping on packets. Thus, the switch is plug and play but will need to forward a messages to all output links if it has not heard from the destination node. A router builds its routing table through routing algorithms (eg. distance vector or link state). Thus, a router can forward a message to almost any host by sending only a single message.

c. When MUST you use a switch instead of a hub?

When the links to be connected have different bit rates.

d. When MUST you use a router instead of a switch?

When the links between the switches contain a cycle.

Student ID: ___________________

4. **RTS/CTS**

With RTS/CTS on an 802.11 network:

a. What prevents two nodes from sending RTS packets at the same time? Is it still possible for two RTS packets to collide? If so, how?

RTS packets are sent using CSMA/CA, so carrier sensing and a random back-off prevent them from colliding. Collisions can still occur, for example, in the "hidden-terminal" scenario.

b. What prevents a node from sending a RTS packet while another node is sending a data packet? Is it still possible for an RTS packet to collide with a data packet? If so, how?

RTS packets are sent using CSMA/CA, which should prevent most collisions. While "hidden terminals" may not hear the data packet, they should hear the CTS message which should cause them to *defer* until they hear the ACK of the data packet. A collision is still possible, however, if a hidden terminal misses the CTS packet.

c. What prevents two nodes from sending data packets at the same time? Is it still possible for two data packets to collide? If so, how?

Only one node can reserve bandwidth with the receiver at a time. Thus, only one node should ever send a data packet at a time. Collisions are still possible, however, if there are multiple receivers that reserve bandwidth for different transmitters at the same time.

Student ID: ____________________

5. **Mobile Routing**

We want to route between a stationary node A and a mobile node B. Name the packet types and the entities involved when:

a. a mobile node registers in a visited network?

The foreign agent sends a ICMP agent advertisement message.
The mobile node sends a registration request to the foreign agent.
The foreign agent sends a registration request to the home agent.
The home agent sends a registration reply to the foreign agent.
The foreign agent sends a registration reply to the mobile node.

b. a correspondent uses indirect routing to send a message to a mobile node?

The correspondent sends an IP message addressed to the mobile node's permanent address.
The home agent intercepts the message and wraps it in another IP message addressed to the foreign agent.
The foreign agent unwraps the original message and forwards it to the mobile node.
The mobile node may respond with a message addressed to the correspondent, using its permanent address as the source address.

c. a correspondent uses direct routing to send a message to a mobile node?

The correspondent send a request to the home agent for the mobile node's foreign address.
The home agent responds with the foreign address.
The correspondent sends a message addressed to the node's foreign address.
The mobile node may respond with a message addressed to the correspondent, using its foreign address as the source address.

Student ID: ____________________

6. **Cryptography Fundamentals**

a. With symmetric key cryptography, the encryption of a message using a key is reversible using the same key. In public key cryptography: (make an analogous statement)

The encryption of a message using a public key is reversible using the private key, and vice versa.

b. What authentication problem does a nonce (challenge) solve? Does this work with public key cryptography, symmetric key cryptography, or both? Why?

The replay attack. This works with symmetric key cryptography because we can assume that only the person we want to authenticate has the shared key. It would work with public key cryptography only if we can verify the person's public key.

c. Name two guarantees of digital signatures.

1. A digital signature guarantees the identify of the person who created the signature
2. A digital signature guarantees the integrity of the message that was signed

d. All cryptographic techniques require us to identify a physical person or company based on the possession of a secret key. This is often achieved with the help of a Key Distribution Center (KDC) or Certificate Authority (CA). How does the CA or KDC first establish the identity?

1. You KDC could physically hand the person a shared key
2. The certificate authority could authenticate the person with a driver's license

Student ID: ____________________

7. **Public Key Cryptography**

a. Should you use the public key or private key to digitally sign a message?

A message should be signed with a private key, so that anybody that has the corresponding public key can verify the signature.

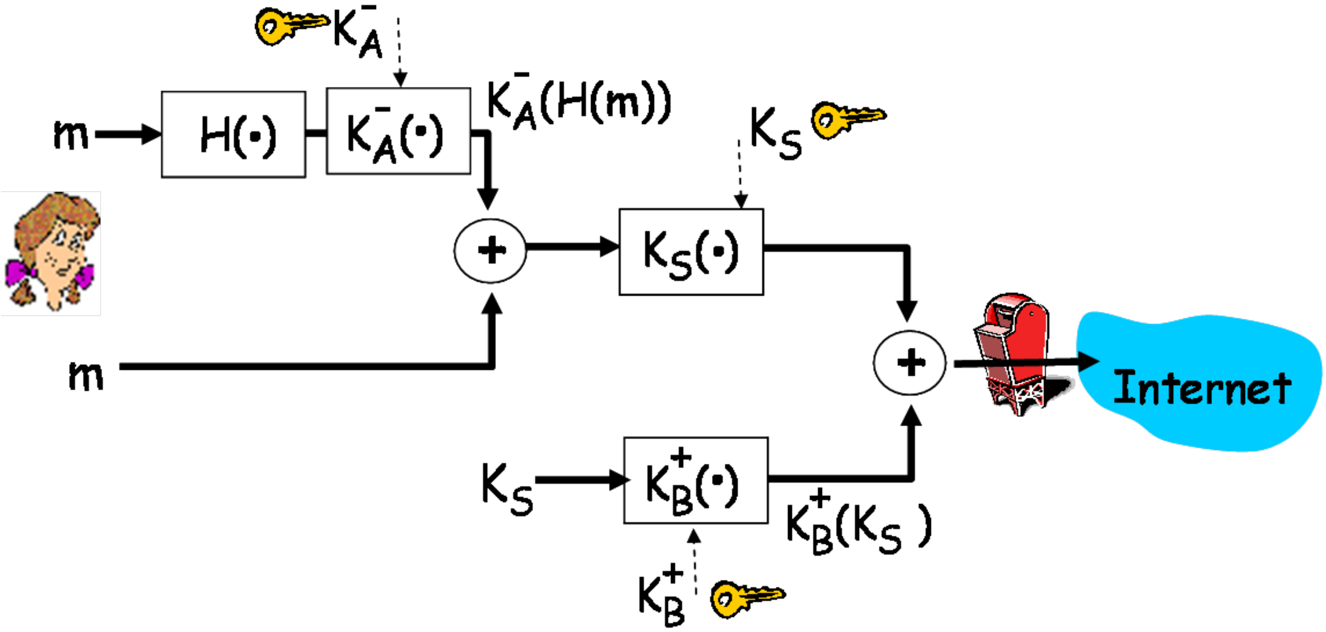
b. Why would you use a message digest when creating a digital signature? What property must a cryptographic hash function have to produce a message digest that provides message integrity?

A message digest reduces the size of the data that must be encrypted to produce a digital signature. It can be created using a cryptographic hash function which 1) is difficult to backward compute (find a message that produces a given hash value) and 2) for which it is difficult to find a "collision" (two messages with the same hash value).

c. How would you communicate with amazon.com if the certificate authority Verisign went down permanently?

You could still use Verisign's public key to decrypt amazon's certificate and get amazon's public key, as long as you knew Verisign's public key before Verisign went down.

d. Draw a diagram of an encryption scheme that provides email privacy, authentication, and integrity without encrypting the entire message using a public key



Student ID: ___________________

8. **The Application Layer**

a. Describe the difference between the client/server model and the peer-to-peer model of applications.

The client/server model requires one always-on server that offers services to the client. In the peer-to-peer model, all nodes provide and use services and not all nodes are always-on.

b. Name one application that uses a hybrid of the client/server and peer-to-peer models.

The Napster and Kazaa networks both use a hybrid model by using servers to coordinate between peers. In some sense, SMTP “servers” are both clients and servers.

c. When one host sends a UDP packet to another host, what values will the receiving host use from the packet headers to direct the segment to the appropriate socket?

The destination address and the destination port

d. When one host sends a TDP packet to another host, what values will the receiving host use from the packet headers to direct the segment to the appropriate socket?

The source address, the source port, the destination address, and the destination port

Student ID: ___________________

9. **Persistent Connections and Pipelining**

Assume that you want to to retrieve a web page that has 5 images.

a. How many messages must be sent when using non-persistent HTTP before this web page can be viewed, *including connection establishment, data retrieval, and connection close*? How many RTTs?

A total of 6 objects must be retrieved, each requiring a new TCP connection that must be opened and closed. Thus, 36 messages will be sent, requiring 18 RTTs.

b. How many messages must be sent when using persistent HTTP with no pipelining? How many RTTs?

Only one connection must be opened, so 16 messages will be sent requiring 8 RTTs.

c. How many messages must be sent when using persistent HTTP with pipelining? How many RTTs?

16 messages will be sent, just as without pipelining. However, the 5 images will be retrieved simultaneously, reducing the process from 8 to 4 RTTs.

d. How does the bit-rate of a network affect the amount that persistent connections and pipelining can improve transfer speeds?

In a low bit-rate network, the transfer times are dominated by the time it takes to transmit the data, so the benefit of removing the connection open/close messages or the data request delays becomes less significant.

e. How does the latency of a network affect the amount that persistent connections and pipelining can improve transfer speeds?

In a high latency network, the transfer times are dominated by the time it takes to send a round-trip message, so the benefit of removing the connection open/close messages or the data request delays becomes more significant.

Student ID: ____________________

10. **The Routing Layer**

a. A circuit switched network requires a connection to be established before two hosts can send messages to each other, and each packet is addressed by the circuit number. A packet switched network: (make an analogous statement)

sends packets on-demand, with no reservations, and each packet is addressed to a destination host.

b. In Link State routing, a router measures the cost of the link to all neighboring nodes and sends this information to all nodes in the network. In Distance Vector routing: (make an analogous statement)

a router measures the cost of the route to all nodes in the network and sends this information to all neighboring nodes.

c. Why do we have different routing algorithms for inter-AS and intra-AS routing?

Intra-AS routing is oriented towards efficiency while inter-AS routing is oriented towards scalability and providing autonomy of routing policies

Student ID: ____________________

Honor Code

____

____

____

Signature ______________________________