Final Exam

- 7:20pm, May 12th
- Location: **To be announced**
- Two pages of letter-size, double-sided cheating sheets, created by hand
- Calculator required
- No other equipments allowed
- Comprehensive; roughly 70% after midterm
- If you want special arrangements (IN, etc.), present your request *before* the final.

Course Grade

- Before I submit your grade, you will be informed via email
  - your final exam mark,
  - your entire record of the semester,
  - my equations of calculating course grades, and
  - your course grade.
Last Office Hours

- There will be an office hour session after the final but before I submit your grade to the Univ.
- This will be your last chance to set the record straight.
- It will be very difficult to change your grade after it has been submitted, and I will be very reluctant to do so.
- The time and date will be announced before the final; please watch the course web page periodically.

Circle the functions of the three-way hand shaking procedure to establish TCP connections..
  - To compute the path to reach the destination for use by the connection.
  - To compute the sizes of sliding windows.
  - To negotiate initial sequence numbers
  - To negotiate the use of the Nagle’s algorithm.
  - To determine the purpose of the connection, for example, control or data.
  - To distinguish obsolete connection requests from current ones
  - To discover the hardware/DLL addresses of endpoints
Practice Questions

What is the retransmission ambiguity problem? How does the Karn’s algorithm solve the problem?

Point out “True” or “False” for the following statements about Internet delivery.

– Datagrams may be lost in transit
– Datagrams may be fragmented in transit
– Datagram suffering transmission errors will be discarded by routers.
– Segements of one TCP connection always arrive at the destination machine in the right order.
– Data delivered through a TCP connection will arrive at the destination application in the right order.
– Segements of a TCP connection always use the same path to reach destination.
In an operating system X, the data link layer is part of the device driver, the network layer is in the OS kernel, and the transport layer is implemented as a user-space library. Point out where each of the algorithms is implemented.

- Nagle’s algorithm
- Exponential backoff
- Dijkstra’s algorithm
- Karn’s algorithm
- MD5

Circle the routing protocol(s) used for intra-AS routing in the Internet
- OSPF, BGP, HTTP, SMTP, RIP, ARP

Circle the routing protocol(s) that use(s) Dijkstra’s shortest path algorithm.
- OSPF, BGP, RIP, PNNI

Circle the routing protocol(s) that is capable of policy routing.
- OSPF, BGP, RIP, PNNI
Point out to which layer in the OSI reference model the following devices belong.
- Routers
- Ethernet switches
- Bridges
- Repeaters
- DNS servers
- FTP servers
- Address translation boxes
- Web servers

Show that the slow start mechanism increases cwnd exponentially relative to RTTs.

A TCP sender sees duplicates of identical acknowledgments. Give two explanations of how this could happen.
- What is Fast Retransmission?

- What is Fast Recovery?

- How does PGP maintain message secrecy?

- How does PGP authenticate a message?
A user logs into an FTP server, downloads 3 files, and logout. How many TCP connections are involved in the session?

Which of the following protocols(s) is/are mostly likely to trigger the Nagle’s algorithm.
- FTP
- TELNET
- SMTP
- HTTP

Circle the host ID parts of the following IP addresses.
200.100.10.1 20.20.20.20 130.13.13.13

A TCP segment is leaving a private network that uses a gateway PC to perform IP masquerading. Circle the field(s) in TCP/IP headers of the packet that will be updated by the gateway PC.
Source IP address, source port #,
Destination IP address, destination port #,
Acknowledgment #, IP header checksum
Consider a secure remote login procedure

– The client asks the user to enter the username and password
– The client computes $D = \text{MD5}(\text{password})$
– The client randomly chooses an IDEA key $K$
– The client computes $M' = \text{IDEA}(M, K)$, where $\text{username}|D$
– The client computes $K' = \text{RSA} \_\text{Enc}(K, \text{public} \_\text{key}(\text{Server}))$
– The client sends $(M', K')$ to the server

Give the computation the server uses to recover the plaintext $M$.

Give the computation to check the password. We assume that the server maintains a password table for all users and $\text{Passwd}(X)$ gives the password of user $X$. 
□ Show that our remote login procedure is vulnerable to the replay attack.