This homework is optional, and intended to help you study for the final exam. As incentive to turn it in, we will take the best 3 out of 4 of your homework scores when calculating your final grade.

Note that some of these questions come from previous year’s exams.

1. **Security**

For over ten years, the following protocol was thought to be secure. It is a protocol which allows two people, $X$ and $Y$, to authenticate themselves to each other. Let $K_X$, $K_X^{-1}$, and $K_Y$, $K_Y^{-1}$ be the public and private keys of $X$ and $Y$, respectively. Let $N_*$ be a nonce (i.e. a random number) generated by node *. Let the notation $\{M\}K_x$ mean that the message $M$ is encrypted using key $K_x$. The protocol is then:

\[
\begin{align*}
X & \rightarrow Y : \{N_X, X\}K_Y \\
Y & \rightarrow X : \{N_X, N_Y\}K_X \\
X & \rightarrow Y : \{N_Y\}K_Y
\end{align*}
\]

Alice wants to authenticate herself to Mallory using the above protocol in order to send Mallory a postcard. Mallory, however, being the unscrupulous person she is, can use Alice’s gesture of friendship to turn around and impersonate Alice to Bob-the-banker! Once Mallory has authenticated herself to Bob as Alice, she can then transfer money from Alice’s account to her own, or do other nefarious deeds.

a) Show how Mallory is able to impersonate Alice by writing above each line in the packet exchange diagram the message that would be sent.
b) Explain how the protocol can be made secure against this attack, and show a packet exchange diagram for your modified protocol.

c) If Alice, Mallory and Bob are all computers on an internet, explain where Mallory must be located with respect to Alice and Bob to carry out her attack, and how she might be able to accomplish it.

2. **QoS**

a) Assume that all the traffic through a network is UDP traffic. The average delay for the packets I send to reach their destinations is \( l \) milliseconds. If the average amount of traffic through the network doubles, what would I expect to happen to \( l \)? (a) it stays the same, (b) it halves, (c) it doubles, (d) it more than doubles. Why? If you need more information to answer the question, state what that information is and how it affects your answer?

b) Explain how diffserv on a router can be configured to create three Classes of Service. (1) A service with low probability of dropping packets. (2) A service with low latency. (3) A best-effort service.

c) In order to offer a bound on the worst case delay the low latency traffic will see, what information do you need and how would you compute the delay bound?

3. **Multimedia**

Video applications typically run over UDP rather than TCP because they cannot tolerate retransmission delays. However, this means video applications are not constrained by
TCP’s congestion control algorithms. What impact does this have on TCP traffic? Be specific about the consequences.

Fortunately, these video applications often use RTP, which results in RTCP “receiver reports” being sent from the sink back to the source. These reports are sent periodically (e.g. once a second) and include the percentage of packets successfully received in the last reporting period. Describe how the source might use this information to adjust its rate in a TCP compatible way.

4. TCP Congestion Control

Louis Reasoner has just finished his Internet Draft where he claims to have discovered three strategies that will eliminate congestion as a problem in the network. Each of these strategies would be very expensive to implement and create a logistical nightmare to coordinate. Ignoring those issues, however, each proposal has a fatal flaw. Either it does not relieve congestion under all traffic patterns, or it creates another problem in the process of relieving congestion.

For each of these myths, explain why it does not relieve congestion or describe the new problem it creates. Draw figures of network topology if needed to illustrate your example.

- Since the throughput of TCP decreases when a packet is lost, and packets are lost because buffers in the network routers fill up, we will fix congestion by increasing the size of the buffers in the network by several orders of magnitude
- Since buffers fill up because packets are waiting to go onto a link, we will increase the speed of all the links in the network by a factor of 10.
- To avoid congestion in the network, we will require access links to be slower than the links in the core of the network.