ECE671
Fall '10 – Exam II

Prof. Wolf

Name: _____

ID Number: _____

	Maximum	Achieved
Question 1	12	
Question 2	10	
Question 3	14	
Question 4	14	
Total	50	

This exam is closed book, closed notes. Two pages handwritten notes are allowed. No electronic devices (other than calculators) are allowed. Be concise, but show your work. Write legibly.

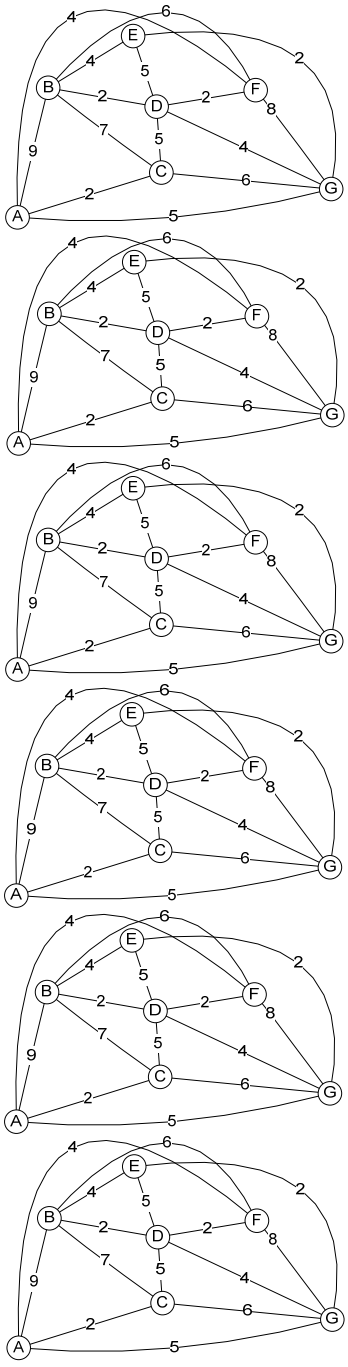
Time: 75 minutes.

Question 1 (12 points):

Answer the following questions regarding shortest path routing.

a) Show the iterations of Dijkstra's algorithm on node A in the following scenario. Show each pair of shortest known distance D(x) and predecessor p(x) for all steps. Circle the node that chosen next to be added. Mark in each topology figure the links that belong to the shortest path tree. (8 points)

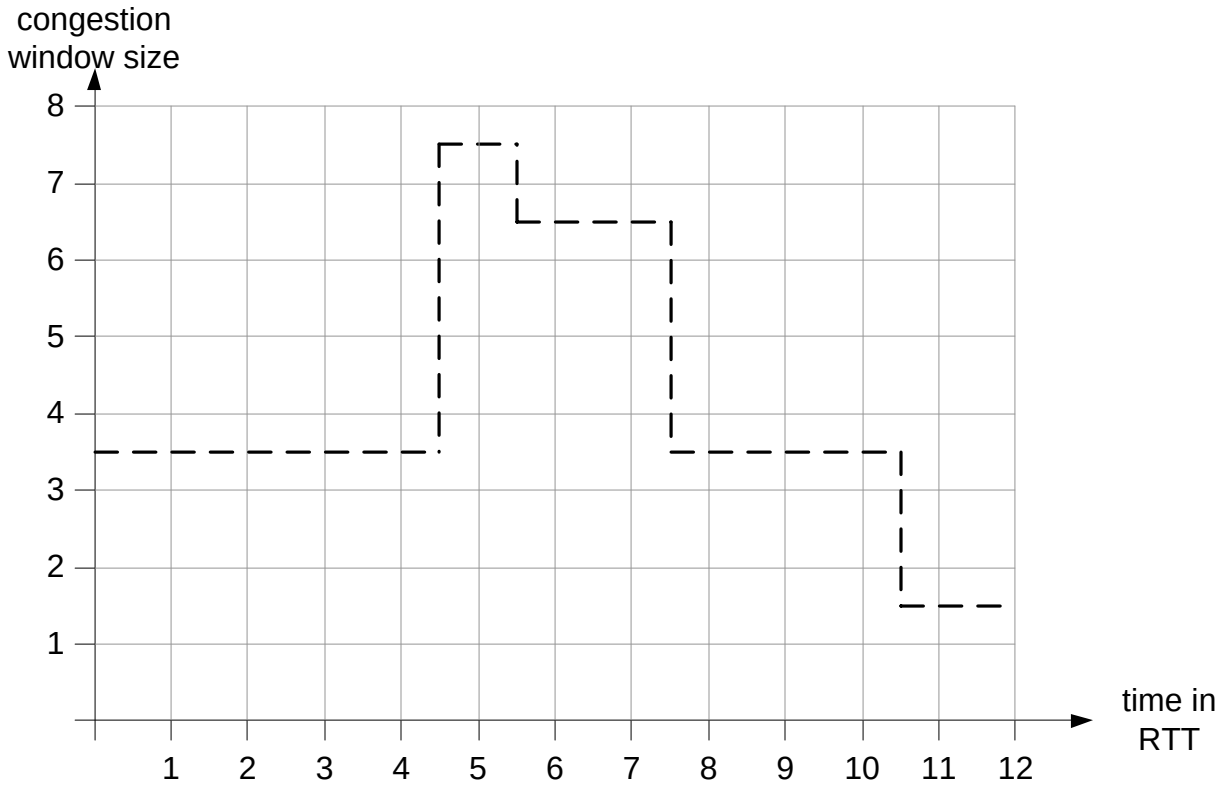
D(B),p(B)	D(C),p(C)	D(D),p(D)	D(E),p(E)	D(F),p(F)	D(G),p(G)



b) Dijkstra's algorithm gives you the lowest-cost path from a source to a destination. If you use "delay" as the cost metric, you get the path with the lowest delay. If you want to compute the path with the highest available bandwidth, what metric could you use? If Dijkstra's algorithm is unsuitable for such a calculation, explain why. (4 points)

Question 2 (10 points):
Answer the following questions regarding congestion control.

a) Assume a TCP Reno implementation. Show the congestion window size in the figure below (up to and including t=12). Assume the initial congestion window size at time t=1 is 1 and the threshold value is initially set to 8. The available bandwidth (same unit as congestion window per RTT) is shown as a dashed line. If TCP's congestion window exceeds this value, packet loss occurs. Assume that a triple duplicate ACK event occurs. (6 points)



b) Consider the maximum amount of data that an ideal transport layer protocol could transmit between t=1 and (including) t=12. When comparing how much data TCP actually (successfully) transmits to the receiver, what is TCP's efficiency in this example? (4 point)

Question 3 (14 points):
Answer the following questions regarding security and cryptography in computer networks.

a) Show a deterministic finite automaton (i.e., a state machine) that uses the alphabet {A,B} and can detect any sequence that contains "ABAB" and "BAAA". Mark detection states with double circles. (6 points)

b) Assume that user *A* wants to send message *M* securely to user *B*. Also assume that they use public key cryptography, and a secure public key distribution mechanism is in place. Describe (1) what operations *A* needs to do with *M*, (2) what *A* needs to transmit, and (3) what *B* needs to do to verify the security property in order to achieve the security properties listed below. Please describe the *minimal* set of operations to achieve the required properties. For notation, please use "K_A^+" as public key of *A* and "K_A^-" as private key of *A* (similarly for *B*). (4 points)

Integrity, authenticity, and non-repudiation with digital signature:

(1)

(2)

(3)

Confidentiality:

(1)

(2)

(3)

c) A colleague suggests a “secure ping” program to measure end-to-end delay. The source of the secure ping packet attaches a 1000 bytes nonce to the ping packet and signs it using its private key. The target of the secure ping verifies the source using the source’s public key. Then, the target creates a response packet that signs the sender’s nonce with the target’s private key and sends it back. The source then checks that the received packet matches the original nonce and checks the signature with the target’s public key. Assume that public keys are distributed securely. What is your opinion on the effectiveness of the proposed secure ping measurement tool for the purpose of measuring end-to-end networking delay? (4 points)

Question 4 (14 points):
Answer the following questions regarding discrete-time Markov chains. Consider a user that uses two applications to download content from the Internet: (1) a web browser to download web sites and (2) a video player application to download videos. The download of a web site requires exactly 12.5 kB (kilobytes) and the download of a video requires exactly 1.25 MB (megabytes). The user has the following behavior: every 10 seconds, she downloads either a web site or a video. If she downloaded a web site in the previous iteration, she will download another web site with 80% probability (else she downloads a video). If she downloaded a video in the previous iteration, she will download another video with 50% probability. (The time to download either type of data is assumed to be less than 10 seconds and does not affect the user's behavior.)

a) Show a discrete-time Markov chain with two states (state 0 for web site download, state 1 for video download) that represents the user's behavior. (4 points)

b) Determine the steady-state probabilities for the Markov chain in a). (6 points)

c) Determine the average amount of data that is transferred by the user (in bits per second). (4 points)