Instructions:

? Please use two exam blue books – answer questions 1, 2 and 3 in one book, and the remaining questions in the second blue book.
? Put your name and student number on the exam books NOW!
? The exam is closed book.
? You have 120 minutes to complete the exam. Be a smart exam taker - if you get stuck on one problem go on to another problem. Also, don't waste your time giving irrelevant (or not requested) details.
? The total number of points for each question is given in parenthesis. There are 100 points total. An approximate amount of time that would be reasonable to spend on each question is also given; if you follow the suggested time guidelines, you should finish with 10 minutes to spare.
? Show all your work. Partial credit is possible for an answer, but only if you show the intermediate steps in obtaining the answer.
? Good luck.

PLEASE WRITE NEATLY
I need to be able to read your answers!
(seemingly encrypted solutions can not be decrypted!)

PLEASE USE TWO BLUE BOOKS
as described in instructions above
Question 1: `Quickies` (21 points, 25 minutes) Answer each of the following questions briefly, i.e., in at most a few sentences.

a) Where can queueing occur in a router? Briefly explain the conditions that lead to such queueing.
b) What is meant by the term “tunneling”?
c) What is the purpose of using a nonce in an authentication protocol?
d) What is meant by IP spoofing? How can a router be used to prevent IP spoofing?
e) What is a MIB?
f) What is an important difference between an SNMP request/response and an SNMP trap message?
g) What is meant by TLV encoding?

Question 2: Secure and authenticated message transfer (18 points, 23 minutes)

Suppose that Alice has a single message, m, that she wants to encrypt and send to Bob. Alice is computationally limited wants to encrypt the message in as efficient a manner as possible. Alice also wants to authenticate herself to Bob, i.e., include enough information that Bob knows that only Alice could have sent the message. Initially, Bob and Alice share no common secrets (e.g., password or shared secret key). Also, the only server available in the environment is a public key distribution server (certification authority).

a) Describe the steps that Alice takes to send the message, given the requirements above. Be specific in describing the algorithms/approaches and steps that Alice takes. (e.g., don’t just say “Alice encrypts the message”. If she encrypts it, state the algorithm she uses. If she needs a key, indicate how/where she gets the key?).
b) Describe the steps that Bob takes to decrypt and authenticate the message. Again, be specific about the algorithms/approaches he takes.
c) What (if any) is the role of the certification authority in the transaction above?
Question 3: Multiple access protocols (21 points, 20 minutes)

We studied a number of multiple access protocols in this course, including (1) TDMA, (2) CSMA, (3) Slotted Aloha and (4) Token passing.

Suppose there are \( N \) stations on a LAN that has capacity (transmission rate) \( C \). All packets have a fixed length \( L \) and the end-to-end propagation delay of the channel is \( P \). For each of the protocols above, answer the following questions:

a) Suppose only one station ever has a message to send (i.e., the other \( N-1 \) stations generate no traffic). What is the maximum possible throughput seen by this single node under each of the protocols above?

b) Suppose now that all stations have the same average traffic arrival rate. We are now interested in the aggregate throughput of the LAN. For each of the above protocols, is it possible to achieve a throughput of 1 (i.e., have the channel always be fully utilized)? If not, indicate how/why the protocol limits the maximum throughput to less than 1.

c) In a heavily loaded network, what is the worst case amount of time a node has to wait under each of the protocols, before it can send a message?

Question 4: Steaming multimedia over a TCP/IP network (15 points, 17 minutes)

Consider an application in which a stored multimedia file is going to be streamed from a client to a server. Here, our goal is to focus not only on this application, but also to consider how certain functionality appears in multiple layers of the protocol stack.

a) Error handling. Briefly (a sentence or two at most for each layer) describe how errors or loss might be detected or corrected/mashed at the application layer, transport layer (assuming UDP transport), and the data link layer.

b) Flow control. Flow control is matching of the sending rate of the sender, with the receiving capabilities of the receiver. Briefly (a sentence or two at most for each layer) describe how flow control (capability matching) is used at the application, transport and data link layers when streaming a multimedia file (assuming UDP transport).
Question 5: Addressing, and following the data (25 points, 25 minutes)

Consider the simple network shown below:

```
 111.111.111.111

A       X       E
```

222.222.222.222

a) Write down an IP address for all interfaces at all hosts and routers in the network. The IP addresses for A and E are as given. You should assign IP addresses so that interfaces on the same network have the same network-part of their IP address. Indicate the number of bits in the network-part of this address.

b) Choose physical addresses (LAN addresses) for only those interfaces on the path from A to E. Can these addresses be the same as in part a)? Why?

c) Now focus on the actions taken at both the network and data link layers at sender A, the intervening router, and destination E in moving an IP datagram from A to E:
   1. How do A, E and the router determine the IP addresses needed for the IP datagram?
   2. What, specifically, are the addresses in the IP datagram that flows from A to the router. What, specifically, are the addresses in the IP datagram that flows from the router to E.
   3. What are three other fields found in an IP datagram?
   4. How do A, E and the router determine the physical (LAN) addresses needed for the data link layer frame?

d) Suppose that the router in the figure below is replaced by a bridge.
   1. How would the IP addresses change in this case?
   2. How would the physical (LAN) addresses change in this case?
   3. How would does a learning bridge learn the physical addresses of the attached hosts?