

**THE UNIVERSITY OF WESTERN ONTARIO  
LONDON CANADA**

**COMPUTER SCIENCE 457a  
MIDTERM EXAMINATION  
OCTOBER 25, 2003  
2 HOURS**

NAME: \_\_ Marking Scheme \_\_\_\_\_

STUDENT NUMBER: \_\_\_\_\_

Question

1-25. \_\_\_\_\_

26. \_\_\_\_\_

27. \_\_\_\_\_

28. \_\_\_\_\_

29. \_\_\_\_\_

30. \_\_\_\_\_

31. \_\_\_\_\_

32. \_\_\_\_\_

33. \_\_\_\_\_

Bonus. \_\_\_\_\_

TOTAL \_\_\_\_\_

(Out of 120 marks)

There are no cheat sheets, books, or other reference materials allowed for this exam. No calculators, cell phones, or other electronic devices are permitted either.

Part I – Multiple Choice, True/False – Choose the best answer from the choices given. Circle your answer on the paper, and fill in the answer on the Scantron form. [50 marks total, 2 marks each]

1. Multimedia data has which of the following fundamental characteristics:
  - a. It is loss intolerant and delay intolerant.
  - b. It is loss intolerant and delay tolerant.
  - c. It is loss tolerant and delay intolerant.
  - d. It is loss tolerant and delay tolerant.
  - e. None of the above.
  
2. A differentiated services router distinguishes between packet flows in implementing different Per-Hop Behaviours by using the packets'
  - a. Source IP address, destination IP address, and markings.
  - b. Source and destination IP addresses.
  - c. Source and/or destination port numbers.
  - d. Markings.
  - e. None of the above.
  
3. Which of the following redundancies can be found in a digital video stream but not in a single still image?
  - a. Spatial.
  - b. Temporal.
  - c. Chromatic.
  - d. All of the above.
  - e. None of the above.
  
4. The same amount of bandwidth tends to be given to the luminance and each of the two chrominance signals in video transmission.
  - a. True.
  - b. False.
  
5. Which approach to audio and video compression results in predictable resource requirements that make network resource management easier?
  - a. Constant bit rate compression.
  - b. Variable bit rate compression.
  - c. Both constant and variable bit rate compression.
  - d. Neither constant nor variable bit rate compression.
  
6. Which approach to audio and video compression can maintain consistent quality across a stream without wasting scarce resources?
  - a. Constant bit rate compression.
  - b. Variable bit rate compression.
  - c. Both constant and variable bit rate compression.
  - d. Neither constant nor variable bit rate compression.

7. Using TCP for multimedia transmission usually requires a larger playout delay than if UDP was used instead.
- a. True.  
b. False.
8. Which of the following does the RTSP standard do:
- a. Define the encodings, compression, and encapsulation of audio and video over the network.  
b. Restrict the transport protocol allowed to transport streamed media.  
c. Specify how media players must buffer audio and video data.  
d. All of the above.  
e. None of the above.
9. Suppose we choose a larger value for a fixed playout delay for a real-time interactive multimedia application. This will result in:
- a. Less loss, less interactivity.  
b. Less loss, higher interactivity.  
c. More loss, less interactivity.  
d. More loss, higher interactivity.  
e. None of the above.
10. The Real Time Protocol (RTP) is intended to provide a real-time service that can provide timely delivery of data to provide quality of service guarantees.
- a. True.  
b. False.
11. Which of the following are provided by a Real Time Protocol (RTP) packet?
- a. Payload type identification.  
b. Sequence numbering.  
c. Time stamping.  
d. All of the above.  
e. None of the above.
12. Multimedia calls set up using the Session Initiation Protocol (SIP) must use the same media encoding for all participants in the call.
- a. True.  
b. False.
13. Using a leaky token bucket for policing and a weighted fair queuing (WFQ) approach to scheduling, we can provide provable upper bounds on delays.
- a. True.  
b. False.
14. RSVP does not specify how a network actually provides a resource reservation.
- a. True.  
b. False.

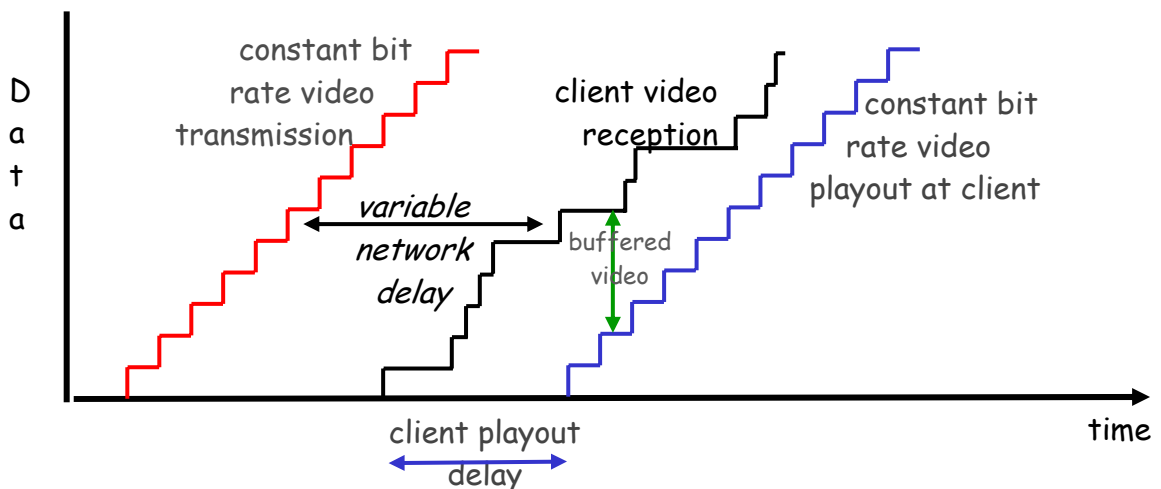
15. The ROT13 algorithm is the same as a Caesar cipher with the key  $k=13$ .
- a. True.  
b. False.
16. It is possible to construct a polyalphabetic cipher out of multiple monoalphabetic ciphers.
- a. True.  
b. False.
17. All monoalphabetic ciphers are vulnerable to a chosen-plaintext attack.
- a. True.  
b. False.
18. When a public key is signed by any Certificate Authority, you know that public key can always be trusted.
- a. True.  
b. False.
19. If a network adapter is in promiscuous mode, it means:
- a. The network adapter is malfunctioning.  
b. The network adapter can read all network traffic.  
c. The network adapter is constantly writing to the network.  
d. The network adapter is encrypting all transmissions.  
e. None of the above.
20. Which of the following poses a potential security risk in handling backup copies of data:
- a. Protecting backups from being overwritten.  
b. Hiding all backups in a locked location on-site to prevent theft.  
c. Encrypting backups to protect their contents.  
d. Verifying all backups to ensure they are properly working.  
e. None of the above.
21. The Wired Equivalent Privacy (WEP) protocol is a very secure protocol and should be considered safe for use in wireless networks.
- a. True.  
b. False.
22. The Secure Sockets Layer (SSL) can be used with either TCP or UDP data.
- a. True.  
b. False.
23. IPsec can be used with either TCP or UDP data.
- a. True.  
b. False.

24. The Authentication Header (AH) protocol, part of IPsec, provides which of the following security functions:
- a. Source authentication.
  - b. Data integrity.
  - c. Data confidentiality.
  - d. Source authentication and data integrity.
  - e. Source authentication, data integrity, and data confidentiality.
25. The Encapsulation Security Payload (ESP) protocol, part of IPsec, provides which of the following security functions:
- a. Source authentication.
  - b. Data integrity.
  - c. Data confidentiality.
  - d. Source authentication and data integrity.
  - e. Source authentication, data integrity, and data confidentiality.

Part II – Short/Long Answer – Complete the following questions in the space provided on the exam paper.

26. The following question parts deal with buffering and playout delays. [8 marks total]
- a. Describe how client-side buffering and playout delay can be used to compensate for network-added delay and delay jitter. Use a diagram depicting the rate of video transmission, reception, and playout in your answer. [6 marks]

With a client-side buffer, clients can receive data and store it without immediately playing it back, thus providing a playout delay. Instead of playing received data immediately, data is played from the buffer while received data fills the buffer back up. The more data accumulated in the buffer before playback, the larger the playout delay, and the larger the network delay and delay jitter that can be accommodated. When data is delayed more than usual, the amount of data in the buffer dips as more is played out than refilled; as long as the buffer does not drain completely, playout will be fine. Consequently, with buffering and playout delay, network added delay and delay jitter can be compensated for, simply by digging in to the buffered data while waiting for the delayed packet to arrive.



- b. Why is a packet that is received after its scheduled playout time considered lost? [2 marks]

If a packet misses its scheduled playout time, we would have two choices. One is to hold up the stream to wait for the packet, and the other is to drop the packet. The first approach is not acceptable; if the packet is dropped, the overall impact on quality is minimal. (Interpolation or repeating can be used instead.) So, it makes sense to intentionally discard the late packet, so it is effectively considered lost. It also makes little sense to keep a packet delayed and out of order, as this would likely corrupt playback of the media stream.

27. The following question parts deal with RTP and RTCP. [8 marks total]

- a. Why does RTCP reserve a steady amount of its bandwidth for handling sender reports, when receiver bandwidth is shared amongst all receivers (thereby giving each receiver less bandwidth for RTCP reports than the sender, when there are a lot of receivers)? [2 marks]

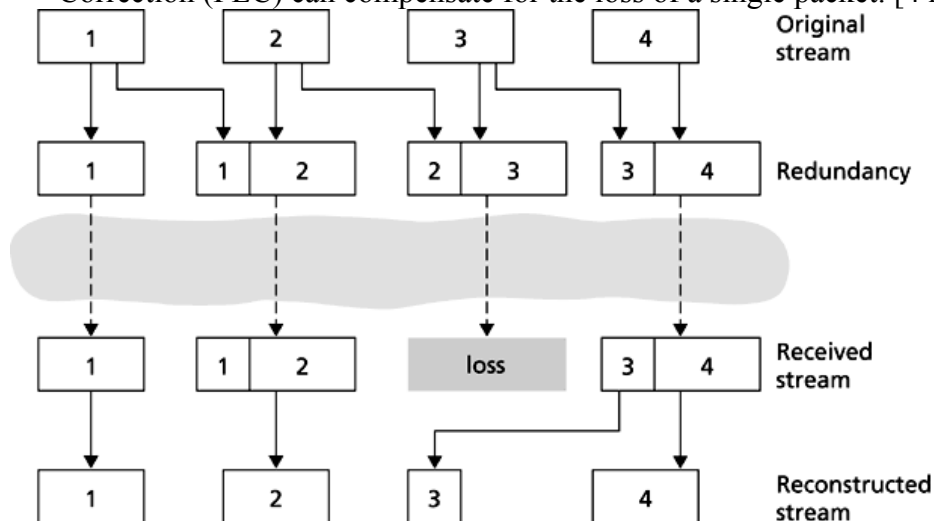
Sender reports are more important and can serve critical purposes in applications. For example, synchronization of audio and video streams can depend on sender reports. Fewer reports or missing reports means less synchronization, which can mean lower quality in the application as a whole.

- b. Suppose you have a multimedia application with one audio stream and one video stream, with each stream being transported with RTP. Explain how RTCP can be used to help synchronize the audio and video streams together. [6 marks]

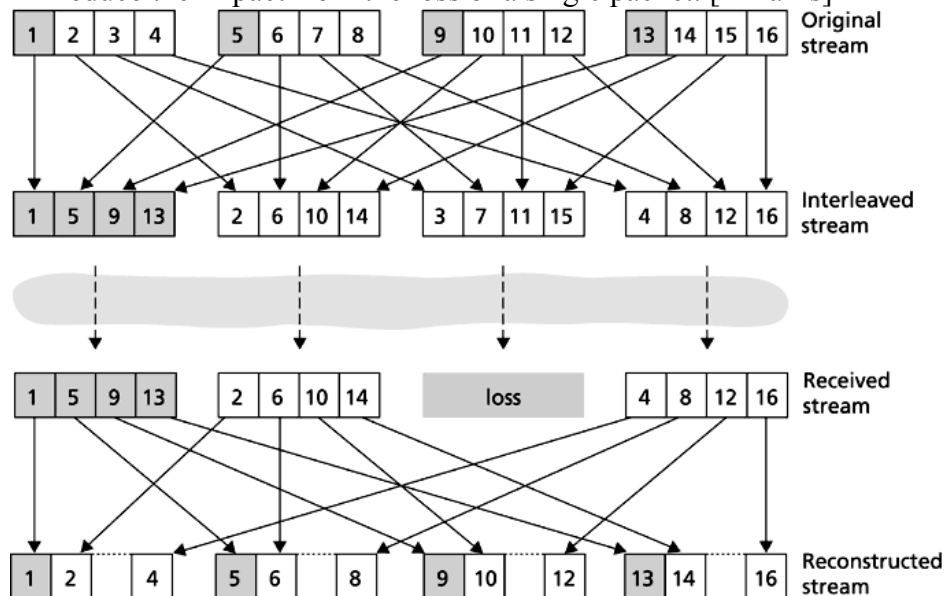
RTCP sender reports will contain for each stream both the current stream-specific timestamp within the stream and the current wall clock time. If we look for RTCP sender reports with the same wall clock time, the RTP packets from the audio and video streams with the corresponding timestamps from the same sender reports will have been generated at the same time, and should be played back at the same time. In doing this, we can synchronize the playback of the two streams.

28. The following questions deal with error recovery and concealment in networked multimedia applications. [12 marks total]

a. Using a diagram, illustrate how the “piggyback” approach to Forward Error Correction (FEC) can compensate for the loss of a single packet. [4 marks]



b. Using a diagram, illustrate how the interleaving approach to error recovery can reduce the impact from the loss of a single packet. [4 marks]



c. What are the two main approaches to receiver-based repair for error concealment in multimedia data? Describe each approach briefly. [4 marks]

Repetition and interpolation are the two approaches. In repetition, the data before the lost data is repeated. If the loss is small enough, this is not noticeable, and is cheap to do. Interpolation constructs new data from the preceding and following data around the loss by picking the half way point between the data and blending them together. This is more expensive, but has better results.

29. The following questions deal with scheduling network packets to improve quality of service in applications. [8 marks total]

- a. What purpose does a “discard policy” have in a FIFO scheduling discipline? Name two possible discard policies. [3 marks]

Discard policies determine which packets of data to discard when they arrive to a full queue. Possible discard policies include tail drop (drop the arriving packet), random drop (pick a random packet to drop), and priority drop (when a priority scheme is used, and the lowest priority data is dropped).

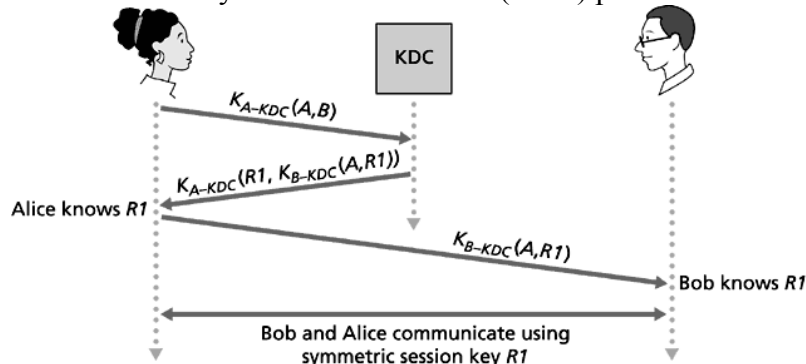
- b. In class, we discussed non-preemptive priority queuing for networks. What would be preemptive priority queuing in this context? Does preemptive priority queuing make sense for computer networks? Explain. [3 marks]

Preemptive scheduling occurs if, when a lower priority packet is being transmitted and a higher priority packet arrives, the transmission of the lower priority packet is interrupted, and the higher priority packet is transmitted in full instead. This does not make sense in networks because it wastes network bandwidth ... the partial packet resulting from the preemption is no good to anyone, so it makes no sense to do the preemption.

- c. How can a weighted fair queuing (WFQ) approach to scheduling network packets be made to act the same as a work conserving round robin approach? [2 marks]

If the weights for all queues are set to 1, weighted fair queuing will behave essentially the same as a work conserving round robin approach. If the weights are set to be the same, but not all to 1, you get the same proportion of time given out to each queue, but it will not function exactly the same as round robin.

30. The following questions deal with Key Distribution Centers (KDCs) and Certificate Authorities (CAs). [10 marks total]
- a. Consider the Key Distribution Center (KDC) protocol from class shown below.



Why doesn't Alice need to explicitly authenticate Bob before using the session key  $R1$ ? Why doesn't Bob need to explicitly authenticate Alice before using the session key  $R1$ ? [6 marks]

When Alice sends  $K_{B-KDC}(A,R1)$  to Bob, she knows that only Bob can use it as only he and the KDC know the key. Thus, only Bob can uncover the session key  $R1$ , and the exchange of messages using  $R1$  can only be done with Bob, and so Bob is authenticated. From Bob's perspective, Bob knows that  $R1$  and  $K_{B-KDC}(A,R1)$  were sent to Alice using  $K_{A-KDC}$ . Consequently, Alice was the only one that could decrypt that message to get  $R1$  out of it. Furthermore, the message to Bob from Alice was encrypted with the secret key shared only between Bob and the KDC, which means that message was produced by the KDC as a result of Alice's authentication. So, when Bob is involved in an exchange of messages encrypted with  $R1$ , he can be sure it is Alice, and Alice is also authenticated.

- b. Consider the KDC and CA servers. Suppose a KDC fails and goes down. What is the impact on the ability to parties to communicate securely; that is, who can and cannot communicate? Justify your answer. Suppose now that a CA fails and goes down. What is the impact of this failure instead? [4 marks]

When a KDC goes down, no one can get session keys to communicate with other people any more, so only those with session keys at that time can communicate. No new communications can commence as those would require the KDC to generate session keys and assist in authentication. When a CA fails, all existing certificates are still good, so everyone can still communicate using those certificates. Only the registration of public keys and generation of new certificates fail, so no new users can communicate, but all previously registered users can commence communications with other registered users.

31. The following questions deal with general principles of security. [9 marks total]
- a. What is meant by the following statement, as it pertains to network security: “Do unto yourself before someone does unto you.” Why is this important to network security? [3 marks].

This statement basically says that you should test your own security before an intruder does so. This is important to security because if your network is untested, there could be several potential security problems that an intruder could take advantage of if they find them first.

- b. What is meant by the following statement: “Security through obscurity doesn’t work.” Why is this the case? [3 marks]

The statement means that achieving security only by hiding the details of how the security works is not a good approach to security. This is the case because secrets and hidden things tend not to stay that way for long. It does not take much for an outsider to discover them, and if that is the sole source of your security, you are in big trouble.

- c. What is meant by the following statement, as it pertains to network security: “Technology alone won’t make you safe.” Why is this the case? [3 marks]

This statement basically says that a lot more goes into a secure environment than just technology, primarily because security is a people problem. All of the technology in the world will not work if people fail to use it properly.

32. The following questions deal with wireless network security. [9 marks total]
- a. Provide two reasons why the University of Western Ontario does not use the Wired Equivalent Privacy (WEP) protocol for securing its wireless network. [4 marks]

With 20-30,000 individuals authorized to use the network, each would have to know what the “secret” WEP key is. There is no way that distributing the key, and keeping it secret, would happen with this size of a user population. Another reason is that WEP is not that secure a protocol in the first place. (Putting it in place could give non-technical users a false sense of security.) Since the University is also investigating newer and better security protocols, there is no need to push WEP out immediately.

- b. Since the University of Western Ontario does not use the Wired Equivalent Privacy (WEP) protocol, what methods does it use for limiting access to the network and suggest for securing communications once access has been granted? [5 marks]

Users gain access to the network by authenticating themselves with a secure web server using their UWO login ID and their UWO password. After authentication, their system is unblocked, and general access is granted. Without authentication, the device cannot communicate in any meaningful way with the rest of the network. To secure communications once access has been granted, the University recommends the use of encryption at the transport and application layers through the use of SSL (for web pages and such) and SSH for remote logins. In many cases, insecure protocols will be blocked to prevent their use.

33. The following question parts deal with handling security threats. [6 marks total]
- a. What is meant by the term “port scanning”? If this causes no damage on its own, why is it a threat to network security? [3 marks]

Port scanning refers to attempting to access each possible port number on a system in sequence, through sending it a UDP packet, or attempting to open a TCP connection to that port number. This allows an intruder to see what services are running and who is listening for what. While this causes no damage on its own, this information can be used in a subsequent attack.

- b. What is “traffic padding”? Why would you want to use traffic padding in a network for security purposes? When is it a good idea not to use traffic padding? [3 marks]

Traffic padding is the process of adding fake data to real data in a network to mask what is real and what is not. This makes interception and traffic analysis attacks harder, as they do not know which data should be targeted, providing better security. If a network is congested, or is suffering from a lack of bandwidth, adding fake traffic to the network can cause serious performance problems, and should be avoided.

Bonus Question: What is the fifth word in the theme song from Gilligan’s Island? [2 marks, and my deepest sympathies!]

The fifth word in the theme song is “and”. (“Just sit right back and ...”)

This page has been left intentionally blank. Use it as additional workspace or extra space for answers if necessary.