# The University of Melbourne
# School of Computing and Information Systems
# COMP90007 Internet Technologies
# Final Exam
# Semester 1, 2023

**Reading Time:** 15 minutes

**Total Time:** 2 hours 15 minutes (including reading time)

**Instructions to Students:**

This paper has 6 pages, including two cover pages.

- The exam has 8 questions worth a total of 60 marks, making up 60% of the total assessment for the subject.
- The value beside the Question number displays the marks allocated to each question.
- Please answer all questions using English in the given order. Please type your answers and **save as one PDF file**. Handwritten assignments using tablet or scanned will not be accepted.
- Submission should only contain the question number and the answer (do not repeat the text of questions in your submission).
- Partial marks will be available. No question requires writing lengthy answers. Please be clear and brief as you may lose points for unclear or redundant descriptions.
- Make sure to **save your progress locally and regularly** during the exam and at the end. **Upload the PDF file before due time.** We recommend not leaving the uploading of your file to the last minute.
- If you submit after the due date and time, your submission will be marked as late. Your exam will be available for 30 minutes after the due date and time to allow late submission due to any technical issues during the exam. Once this additional 30 minutes has passed, you will no longer be able to access your exam in the LMS.

**Authorised Materials:** This exam is open-book. The work you submit *must be based on your own knowledge and skills, without assistance from any other person*.

While undertaking this exam you *are permitted to*:

- make use of textbooks, lecture slides (including electronic versions), lecture recordings and material provided as part of tutorials in this subject.
- make use of your own personal notes.
- use calculators or mathematical software to compute numeric answers.
- make use of other materials with proper references.

## IMPORTANT!! Collusion, Plagiarism, Copying and use of AI tools are not allowed under any circumstances.

- **Collusion** includes, but is not limited to, talking to, phoning, emailing, texting or using the internet to communicate with other students. Similarly, you cannot communicate with any other person via any means about the content of this exam during the examination time. If another student contacts you during the examination period, please inform the subject coordinator immediately.
- Your answers to the exam **must be in your own words** and not directly copied from lecture notes, tutorial materials, the Internet or joint study notes you have prepared with your friends. You may refer to sources, but answers should be written in your own words.
- Any similarity detected between your answers, the answers from other students and/or from the Internet or other sources will be investigated and may result in severe penalties.

**Technical support**

- **During the exam**, if you have questions about the exam content, please use the Exam Support Chat.
- **Technical support** for this exam can be accessed at: https://students.unimelb.edu.au/your-course/manage-your-course/exams-assessments-and-results/exams/technical-support
  Additional information about **Canvas Assignment**, including troubleshooting tips, can be found: https://students.unimelb.edu.au/your-course/manage-your-course/exams-assessments-and-results/exams/how-do-i-take-my-exam/formats/LMS-assignments

**Questions commence on the next page.**

**Question 1: [8 Marks]**

A company operates trains on an 800km stretch of track and wishes to enable digital communication between the train and the stations at each end of the track to communicate with the train drivers and to remotely operate the train, using video streamed from the train in the event of an emergency.

i)      Please list the key QoS requirements for this application and explain why. Please answer in brief bullet points.

ii)     Please list the physical layer technologies that would be suitable for this application and explain why. Please answer in brief bullet points.

**Question 2: [6 Marks]**

100 MB (Megabytes) of data is to be transmitted over 100m of twisted pair with a bandwidth of 10MHz (Megahertz) with data encoded using 4 voltage levels. The speed of the signal over the wire is 200,000 km/s.

   i)      What is the Propagation Delay for the transmission?
   ii)     What is the Transmission Delay for the transmission?
   iii)    If the data is encoded using a Hamming (7,4) code for forward error correction, how does this change your answers to i) and ii) above?

Please show all calculations and steps.

**Question 3: [6 Marks]**

A wireless network has 32 stations.  Stations 2, 4, 16 and 24 have packets to transmit.
   i)      List the sequence of events if the Bit Map Protocol is used in brief dot points.
   ii)     List the sequence of events if the Binary Countdown Protocol is used in brief dot points.
   iii)    Compare the two protocols for efficiency and fairness using brief dot points.

**Question 4: [12 Marks]**

The figure below shows 8 routers in a network. The delay on each line is shown along with the routing table for node A.
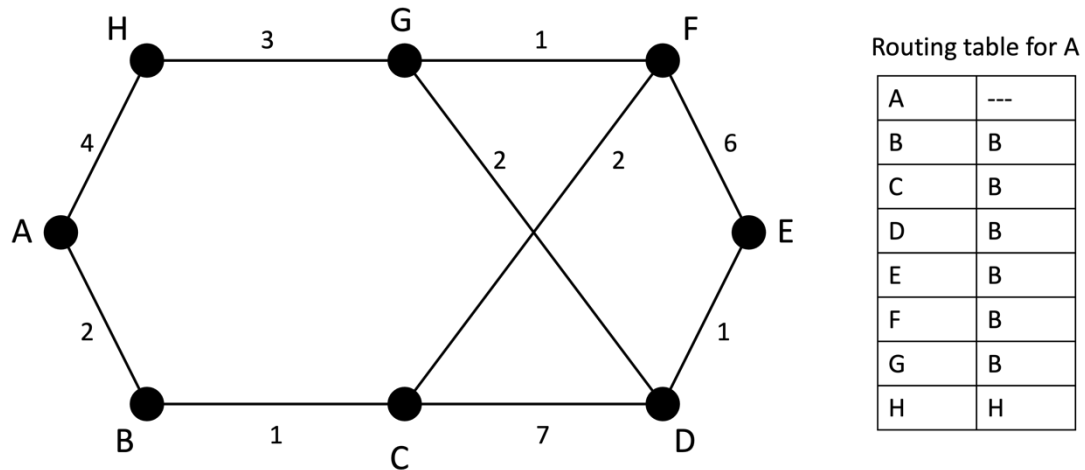


The link between F and G becomes congested and is downgraded from 1 to 3 (packets now take longer to be transmitted over this link).

i)     Compute the distances to each node from node A taking this link change into account, using Dijkstra's algorithm. Complete the table below (adding rows as necessary) to give your answer:

| Round | A | B | C | D | E | F | G | H |
|-------|---|---|---|---|---|---|---|---|
| 1 | <u>0</u> | ∞ | ∞ | ∞ | ∞ | ∞ | ∞ | ∞ |
| 2 | - | <u>2</u> | ∞ | ∞ | ∞ | ∞ | ∞ | 4 |
| 3 | - | <u>-</u> | <u>3</u> | ∞ | ∞ | ∞ | ∞ | 4 |
| … | … | … | … | … | … | … | … | … |

ii)    Compute the new routing table for A

iii)   If Link State Routing is used, give the Link State Packet(s) that will be generated by the downgrade on the FG link.

iv)    If Distance Vector Routing is used instead, how many rounds of the algorithm are needed for node A to become aware of the downgraded link? Briefly explain your answer.

**Question 5: [8 Marks]**

The routing table for a router is shown below:

| Prefix Address | Subnet Mask | Interface |
|---|---|---|
| 128.32.0.0 | 255.255.128.0 | eth0 |
| 128.32.64.0 | 255.255.192.0 | eth1 |
| 128.32.96.0 | 255.255.254.0 | eth2 |
| default | | eth3 |

Packets are addressed to the following destinations. For each packet determine which interface that the router will send the packet on, give a brief explanation for each answer.

i)      128.32.192.65
ii)     128.32.4.4
iii)    128.32.80.5
iv)     128.32.97.10

**Question 6: [6 Marks]**

A server is sending data to a client using TCP. The client has a transport buffer window containing 8000 Bytes. The server has sent packets 1, 2 and 3 each containing 1000 Bytes of data which have both arrived at the client. The client application then reads 1000 Bytes of data from the buffer.

1) What are the ACK and WIN values in the ACK packet that the client sends back to the server after it reads 1000 Bytes from the buffer?
2) The server then sends packets 4 and 5, but packet 5 arrives first What are the ACK and WIN values in the ACK packet that the client sends back to the server after the arrival of the packet 5?
3) Packet 4 now arrives. What are the ACK and WIN values in the ACK packet that the client sends back to the server after the arrival of this packet?

Please provide the values of the requested quantities alone. A diagram for these is not required.

**Question 7: [6 marks]**

A user at their home in France requests a web page from www.unimelb.edu.au. Their web browser must first find the IP address of the web server and then request a web page.

1)      The user's local DNS server does not have any IP addresses in its cache.  List the sequence of steps needed for the user's computer to obtain the IP address of the web server.

2)      The web page returned by www.unimelb.edu.au contains many images.  Why might the client prefer to use a persistent HTTP connection rather than a non-persistent connection to load this web page?

**Question 8: (8 marks)**

Alice and Bob wish to generate a shared secret key using Diffie-Helman key exchange using the prime modulus p=19 and generator g=2.

1)      Assume that Alice chooses a number which is 2 added to the last digit of your student ID and that Bob chooses a number which is 2 added to the second last digit of your student ID.

For example if your student ID is 1234567 then the last digit is "7" so Alice chooses 7+2 = 9 and the second last digit is "6" so Bob chooses 6+2 = 8.

Show the process that Alice and Bob go through to obtain a shared secret key.  Make sure you identify the information that Alice and Bob send to each other in this process.

2)      List the differences between the Diffie-Helman key exchange with the method using public key cryptography, shown in the diagram below using brief dot points. What are the assumptions and benefits of each method?