COMPSCI 314 S1C 06 Assignment 3

Department of Computer Science
The University of Auckland

Posted 12 April 2006
Due 11:59pm, Wednesday 3 May 2006
in https://adb.ec.auckland.ac.nz/adb/

- This assignment will contribute 40/300 = 13.33% to your coursework mark, and 4% to your overall course mark.
- There are 40 marks available on "regular" questions, and 3 bonus marks are available on very difficult questions.
- Bonus marks will not cause any student's total to exceed 40 marks. However bonus marks will improve the total marks of any student who is not awarded all 40 marks from the regular questions.
- No marks will be awarded if you merely state a correct answer. To obtain full credit, your script must clearly explain *why* your answer is correct.
- Plagiarism will not be tolerated. Your explanations must be in your own words.
- If you require additional information in order to answer a problem, you should briefly explain why this information is necessary and why your assumptions about the "missing values" or "missing facts" are reasonable.
- You may submit your assignment either in PDF format (preferred) or in MS Word.

The first questions refer to Figure 3.7 of your textbook, which is reproduced in lecture slide #20 of set #3. In this figure, "RH" is a repeater hub. You should assume the bridging hub uses the routing procedure described on lecture slides #15, #16 and #17 of set #3.

Q1. Consider what would happen if the Ethernet cables leading to stations #1 and #9 of Figure 3.7 were swapped, so that station #1 is connected to the right-hand repeater hub, and station #2 is connected to the left-hand repeater hub. Note: you may safely disconnect and reconnect Ethernet cables without shutting down a station.

a. Immediately after the network connection of station #1 is changed, station #2 attempts to send a frame to station #1. Will this frame cause the bridging hub to change its forwarding database? Will this frame be received by station #1?
[2 marks]

b. Immediately after the network connection of station #1 is changed, station #1 attempts to send a frame to station #2. Will this frame cause the bridging hub to change its forwarding database? Will this frame be received by station #2?
[2 marks]

Q2. If the NIC of station #3 in Figure 3.7 is operating in promiscuous mode (so that it receives and buffers all frames appearing on its port), would station #3 be able to eavesdrop on data sent from station #1 to station #2? **[2 marks]**

Q3. If the Bridging Hub in Figure 3.7 is replaced by a VLAN switch, and if *none* of the NICs are IEEE802.1Q compliant, would station #1 be able to send data to station #2 without risk of eavesdropping from station #3? Would station #9 also be able to eavesdrop? **[2 marks]**

Q4. If the Bridging Hub in Figure 3.7 is replaced by a VLAN switch, and if *all* of the NICs are IEEE802.1Q compliant, would station #1 be able to send data to station #2 without risk of eavesdropping from station #3? Would station #9 also be able to eavesdrop? **[2 marks]**

Q5. If all the equipment in Figure 3.7 is IPsec-compliant, would station #1 be able to send data to station #2 without risk of eavesdropping from station #3, using AH in transport mode? **[2 marks]**

Q6. If all the equipment in Figure 3.7 is IPsec-compliant, would station #1 be able to send data to station #2 without risk of eavesdropping from station #3, using ESP with NULL encryption, in tunnel mode? **[2 marks]**

To answer the following questions, you must refer to part 3 of the IEEE 802.3-2002 standard, which is available for download at http://standards.ieee.org/getieee802/download/802.3-2002_part3.pdf. Warning: this is a 3.6 MB document, which will cost you about $0.10 to download on NetAccount during off-peak hours, and about $0.25 during peak hours. So you may wish to save it to a file system, rather than downloading it multiple times.

To receive full marks on these questions, you must support your explanation with one or more direct quotations from IEEE Standard 802.3-2002, giving section and page number(s) for each of your quotations. Your quotations must be accurate, appropriate, and clearly delimited by quotation marks.

Q7. According to your textbook, at page 193, "[t]he choice of 25m [for the limiting length of a drop cable] was rejected by the standards committee as being too small and, after much debate and lobbying, the maximum length of drop cable was set at 200m." Is this an accurate statement about 1000Base-T, as defined in IEEE 802.3-2002? (Hint: see section 40.1 and section 42.) **[3 marks]**

Q8. According to your lecture slide #25 of set #3, in"Gigabit Ethernet ... [the] maximum channel length [is] reduced to 25 metres". Is this an accurate statement about any of the gigabit Ethernet media defined in IEEE 802.3-2002? **[3 marks]**

Q9. Is it possible to use gigabit Ethernet to communicate over distances longer than 200m? (Hint: look through all of section 42.) **[3 marks]**

The following questions refer to your textbook Figures 10.2 and 10.3, which are reproduced in lecture slides #14, #15, and #16 of set #4. The Caesar cipher is described nicely in Wikipedia at http://en.wikipedia.org/wiki/Caesar_cipher.

Q10. What key will set the P-box of Figure 10.2.a(i) to a nibble-swap permutation, that is, one in which the 8-bit character 0xXY is mapped to the 8-bit character 0xYX, for any hex digits X and Y? **[2 marks]**

Q11. Does there exist a key which will set the P-box of Figure 10.2.a(i) to perform a "Caesar cipher" substitution, that is, one in which the 8-bit character 0xXY is mapped to the 8-bit character (0xXY + 5) mod 256, for any hex digits X and Y? **[Bonus: 1 mark]**

Q12. Does there exist a key which will set the product cipher of Figure 10.3 to perform a "Caesar cipher" substitution? **[Bonus: 2 marks]**

The following question refers to lecture slides #19 and #20 of set #4.

Q13. According to Moore's law, the price-performance of computer hardware is improved by a factor of two, every eighteen months. Approximately how much would it cost today, to build a machine that can crack a DES key in 56 hours? **[2 marks]**

Q14. A simple authentication protocol is illustrated in your textbook's Figure 10.10. This is reproduced on lecture slide #25 of set #4.

a. Would Trudy be able to authenticate successfully as "Alice", by using all three steps of this protocol? **[2 marks]**

b. Would Trudy be able to gain service from the Server, by replaying a copy of message #3 that she has copied from a previous, successful, authentication by Alice? **[2 marks]**

Q15. If the Bank of America sends you their public key in an email message, and then sends you another message that is authenticated by this public key, should you follow the instructions in this email to visit a website that will allow you to open a free bank account and have a chance of winning a valuable prize? **[2 marks]**

Q16. To answer the following questions, you should read the Wikipedia article on https (http://en.wikipedia.org/wiki/Https), and you must have access to a web browser with SSL (or TLS) support.

a. Open a connection to a website whose URL has the prefix "https". Inspect the website's digital certificate – you may need to read your browser's helpfile to find out how to do this. Now answer the following questions: What browser are you using, what website are you visiting, and what did find out about this website by inspecting its certificate? **[4 marks]**

b. Try to verify the authenticity of the digital certificate you have found, using only the information available to you from the following sources: your textbook, your lectures in this class, the website you are visiting, and the helpfiles of your browser. Now answer the following questions. Were you able to gain confidence in the validity of this certificate? Do you think it is reasonable to expect non-expert users to inspect certificates? **[3 marks]**
