Computer Networks 2021 Exercises - Unit 4

FAN: lewi0231

NOTE: Each student's work unit is unique. You *must* use the work that has been generated for your FAN. If you do not, then you will fail this work unit.

NOTE: You must record your answers in the answer file EXACTLY as required, and commit and make sure your changes have been pushed to the github server, as they will otherwise not be counted.

NOTE: The topic coordinator will periodically run the automatic marking script, which will cause a file called unit4-results.pdf to be updated in your repository. You should check this file to make sure that your answers have been correctly counted. That file will contain the time and date that the marking script was last run, so that you can work out if it has been run since you last changed your answers. You are free to update your answers as often as you wish, until the deadline for the particular work unit.

1 Demonstrate an understanding of current methods for secure information transfer

For each question, you must record your answer in the unit4-answers.txt file in your git repository. Write a **single paragraph of not more than 250 words** *on each of the following topics Templates for each answer are provided in* `unit4-answers.txt` *for your convenience.*

NOTE: You are required only to demonstrate that you have an understanding *of the listed topics. You do not need to demonstrate mastery or a deep understanding of the listed topic. A credit-level response will correctly explain what the topic is, in relation to computer networking, and how secure network communications are enabled (or hindered) by it.*

A DN level response will demonstrate an increased familiarity with the topic, and an HD level response will demonstrate the ability to accurately describe the topic and some aspect of its

interaction with secure information transfer on the internet.

In all cases some basic research will be required. In most cases a simple web search on the topic will reveal many potential sources of information, and within 30 minutes of searching and reading you should be able to find more than sufficient information to enable to you write your answer.

Question	**Topic**
ab	*digital signatures*
ac	*cryptographic algorithm vulnerabilities (eg those faced by RC4)*

2 Demonstrate an understanding of emerging methods for secure information transfer

For each question, you must record your answer in the unit4-answers.txt file in your git repository. Write a **single paragraph of not more than 250 words** on each of the following topics Templates for each answer are provided in `unit4-answers.txt` for your convenience.

NOTE: You are required only to demonstrate that you have an *understanding* of the listed topics. You do not need to demonstrate mastery or a deep understanding of the listed topic. A credit-level response will correctly explain what the topic is, in relation to computer networking, and how secure network communications are enabled (or hindered) by it.

A DN level response will demonstrate an increased familiarity with the topic, and an HD level response will demonstrate the ability to accurately describe the topic and some aspect of its interaction with secure information transfer on the internet.

In all cases some basic research will be required. In most cases a simple web search on the topic will reveal many potential sources of information, and within 30 minutes of searching and reading you should be able to find more than sufficient information to enable to you write your answer.

Question	Topic
ad	Any item on the time-line at https://www.feistyduck.com/ssl-tls-and-pki-history/. **Make sure to include the name of the item in your answer**

3 Lecture Material Comprehension

The following questions are designed with two purposes in mind:

1. *To help you engage with the lecture materials; and*
2. *To help generate a wide range of questions for the quizzes in this topic.*

The second goal is not mandatory for you. However, if you are willing for the answers you provide to the questions in this section to be used in future quizzes in this topic, you are requested to answer the following question as follows you will not be penalised if you do not give this permission

Question#	Description
ae	*Are you willing to release your following answers in this section from all copyrights, i.e., release them into the public domain, including so that they can be included in quizzes in this topic?* you will not be penalised or treated any differently if you do not choose to give this permission

It is important that you answer this question with 'y', if you do decide that you would like to do this (but again, you have no obligation to do so, and you will not be treated differently whether or not you give permission).

The entry in unit4-answers.txt *would thus look like:*

```
# Question 'ae': Do you commit the following answers to the public domain
#  and disclaim all copyrights in them?
ae=y
```

For each question, you must record your answer in the unit4-answers.txt file in your git repository. For each question, you are required to write a statement that is either true or false about the material in the indicated lecture slide.

For example, if you were asked 'write a **true** statement about the content of Slide 2 of Chapter 1', you would put the statement at the end of the `rj=` line in the file `unit4-answers.txt`. For example, if your statement was 'One of the problems addressed in this chapter is how to build scalable networks', you would write:

Question#	**Description**
`pz`	Write a **true** statement about the content of Slide 2 of Chapter 1

The entry in `unit4-answers.txt` would thus look like:

```
# Question 'pz': Write a true statement about the content of Slide 2 of Chapter 1

pz=One of the problems addressed in this chapter is how to build scalable networks
```

Templates for each answer are provided in `unit4-answers.txt` *for your convenience.*

If you are asked to write a statement that is false, i.e., untrue, think about statements that someone who has not worked through the material might think would be true. Be creative! Be devious!

Question#	Description
af	*Write a* **false** *statement about the content of Slide 30 of Chapter 1*
ag	*Write a* **false** *statement about the content of Slide 39 of Chapter 3*
ah	*Write a* **false** *statement about the content of Slide 22 of Chapter 3*
ai	*Write a* **true** *statement about the content of Slide 56 of Chapter 3*
aj	*Write a* **false** *statement about the content of Slide 42 of Chapter 4*
ak	*Write a* **false** *statement about the content of Slide 111 of Chapter 2*
al	*Write a* **false** *statement about the content of Slide 2 of Chapter 4*
am	*Write a* **false** *statement about the content of Slide 43 of Chapter 3*
an	*Write a* **false** *statement about the content of Slide 9 of Chapter 4*
ao	*Write a* **true** *statement about the content of Slide 95 of Chapter 3*