cs3235:7: - Laboratory #7 (Homework), October 16th, 2019

This laboratory is homework, which must be done individually. It is very easy, and I suggest you use the extra time to meet up with your project group members, and work on your project. It will finish on Sunday evening at midnight. You do not need to attend the lab, but Hugh and Ray Yan will be there if needed for consultation. You can also pick up your last marked laboratories in the lab.

1 Lab7, part 1: (individual homework question) Protocol...

(Like previous exam question) An instructor wishes to grade submissions from the 96 students taking his course anonymously. Any students at the institute can submit submissions anonymously to a digital drop-box, but of course the instructor wants to ensure that only the 96 students on his course can make a submission.

(a) Devise a simple protocol for the instructor that ensures that only the 96 students taking his course can make a submission. That is, the instructor must be assured that none of the other students at the institute can *forge* a submission, even if they are able to intercept someone else's submission. You can, if you wish, assume that the instructor has access to a secure course mailer which can send a single secure message to all the students taking his course at once.

(b) Consider the situation where the bad-guys could listen in on the messages (including the "single secure message"). Devise a protocol that ensures that only the 96 students taking his course can make a submission. You can, if you wish, make (and state) other assumptions.

Access the cs3235 grading website, and enter your username, password, and your explanation for part (a) and part (b). Clearly identify the (a) and (b) parts of your answer.

`https://hugh.comp.nus.edu.sg/cs3235/lab7/gradeslab7-1.php`

2 Lab 7, part 2: (individual homework question) Weak protocol...

(Not really like old exam question) Identify a low level protocol (i.e. not an application layer protocol) that your laptop/computer uses continuously, and that is *weak* (in security terms). Identify the protocol, and briefly describe what the weakness is. For this protocol, describe how an unscrupulous person could make use of this weakness. Finally, describe a possible improvement to prevent the kind of attacks on the particular weakness you identified.

Access the cs3235 grading website, and enter your username, password, and your answer:
`https://hugh.comp.nus.edu.sg/cs3235/lab7/gradeslab7-2.php`

3 Lab 7, part 3: (individual homework question) Reversing a MD5 hash function

A website available on the Internet provides a reverse-MD5 hash lookup service (https://md5.gromweb.com/ for example). The service can be used to (for instance) discover a shortish hashed password if you forget your password. To use the service you fill in a form with the MD5 hash, and the website may return your original file. In class it seemed like MD5 is not reversible. What are the limits of this system? How is it likely to work?

Access the cs3235 grading website, and enter your username, password, and your explanation:
`https://hugh.comp.nus.edu.sg/cs3235/lab7/gradeslab7-3.php`