ECE101: Exploring Digital Information Technologies **Spring 2024**
Week 9 Exercises (with solutions in red) **Tested on Exam II**

Ethics, Privacy, and Authentication

These exercises are intended to help you master and remember the material discussed in lectures and explored in labs. In future semesters, we may make some or all of these exercises required, but for now they remain optional. We suggest that you do them as we go over the material, but you may also want to use them to review concepts before the exam.

Rather than using this version directly, we suggest that you use the version without solutions to solve the problems before looking at the answers. Many studies have shown that people often trick themselves into believing that they know how to solve a problem if they are presented with the answer before they try to solve the problem themselves.

1. [L16] Some international high schools (and standardized testing services!) have started to use artificial intelligence for grading. Explain two drawbacks of such an approach relative to human-based grading. *(Hint: what if you submit a correct but never-before-seen answer to this question?)*

   (from the hint) AI-based grading is unlikely to be able to identify valid responses to open-ended questions unless those answers are included within their training data sets. In contrast, a human is able to understand the intent of an answer and to evaluate it in the context of the question, allowing the human to give some or all credit to novel responses when appropriate.

   AI is not explainable, so the actual reasons for any partial credit will be a mystery to both the student and the staff. Since students generally learn from their mistakes, but only when those mistakes can be understood, AI-based testing is likely to be less effective in helping students to learn.

2. [L16] Have you ever been in a situation in which another human incorrectly allowed a computer's output or answer to override their own understanding or intuition? Explain. *If not, imagine such a scenario.*

   Many non-native speakers of a language accept computer-generated spelling and grammar corrections to their writing without checking them against their own knowledge (this fact become apparent when a native speaker points such errors out and the writer makes it clear that the fact that the change is a mistake is not a surprise). Sadly, native speakers of a language sometimes do the same.

   Another example comes from summing the totals of graded exams across problems. Today, people often rely on computers to find each exam's total score, failing to realize that computers do not correct for mis-typed problem scores (see the next problem). Fortunately, students are quick to return an exam when they see that staff have added 2 and 4 to obtain 5. Unfortunately, they are less quick when staff have added 2 and 4 to obtain 7.

   Many people do not even look at the prices charged by computers at checkout, whether or not they have deliberately chosen to purchase an item because of an advertised sale price or regular price that made the item attractive. In fact, challenging the computer's price often results in delays and flustered staff members, since most employees have no idea as to the current price of any item in a store. The computer, of course, simply returns the price entered (or not entered as an update) by some other human, and is far from infallible.

3. [L16] Due to the ubiquitous availability of calculators, elementary schools have reduced their emphasis on basic arithmetic. Are a calculator's answers always correct? Explain.

   Of course not! A calculator merely computes the expression entered by the human user. If the user makes mistakes in values or operators, the answer is unlikely to be correct.

   This fact is used routinely by currency exchange operators in some parts of the world to defraud customers. By transposing digits in an exchange rate, they can leverage the buyer's trust in calculators to trick them into accepting less money than they have purchased. For example, if the exchange rate is 1.324 local to 1 of the buyer's, and the buyer gives 5, the agent can type 1.234 x 5 quickly into the calculator and show the result to the buyer.

   This fact has also seriously undermined accounting practices in a wide ranges of businesses, including universities. Rather than using tradition double-entry accounting, which was designed to tolerate human error, values are entered exactly once, and any mistakes simply appear in the sums that are then "validated" by those in charge of overseeing the expenditures. Go figure!

4. [L16] If cost were not an issue, would you pay a company to record several views of your home, including your bedroom and bathrooms, 24/7 (24 hours a day, 7 days a week—in other words, at all times)? Assume that the company is not allowed to sell or distribute the recordings—they are just providing you with protection by capturing any intruders to your home. Explain your answer.

   (Your answer may vary, of course!) I wouldn't. I don't feel comfortable having a camera watching me in my bedroom nor in my bathroom, nor really in any part of my home. I also don't trust the company's employees with such videos, regardless of the company's legal obligations. Finally, while I do use cameras to detect intruders when I am out of my home, the value of capturing them on camera while I'm at home for me is small compared with the loss of privacy.

5. [L17] A lawyer claims that because a document contains a date and the document (including the date) has been hashed with SHA, the fact that the SHA hash can be checked proves that the document's date is correct. As a student of ECE101, explain the lawyer's error.

   A document can be written to include any date—even something like 14 October 174 B.C.—at any point in time, then hashed with SHA. Having a SHA hash says nothing about the date.

   However, this scheme is similar to a common approach to documenting copyright in the 1980s: put a copy of your document in an envelope and mail it to yourself. If necessary, the postmark on the envelope, issued by the US post office, establishes the existence of the envelope's contents to a US court so long as the envelope remains unopened (and no evidence of tampering exists). So you could challenge copyright infringement by bringing the envelope and having it opened in court.

   The difference is perhaps subtle, so don't be too surprised if one day this happens to you in real life.

6. [L17] Explain why symmetric keys are not useful when trying to verify that a particular person authored a document.

   In order to decrypt a document with a symmetric key, one needs the key. However, once one has the key, the same key can be used to encrypt a different version of the document, which could then be decrypted, again using the same (symmetric) key. At that point, without any other evidence of authorship, the two encrypted document versions are completely equivalent to a third party, and the fact of encryption is irrelevant.