

CSCI E-2 Final Exam

May 16, 2009

All 7 problems are weighted equally

This exam is open book, open-Internet, but you must do all work alone without communicating with anyone else.

Please set aside a single 120 minute period in which to do the exam. You may use extra time for drawing and formatting. Send the exam immediately afterwards. The exam must be received by 6pm EDT, Sunday, May 17. NO EXAM SUBMITTED AFTER 6PM ON MAY 17 WILL BE ACCEPTED.

Please include the following statement with your exam: *Except for drawing and formatting my paper, I did this exam in the single 120-minute period from [state when], without assistance from anyone else.*

1. Early web browsers used 56 bit encryption keys. In 1990 it took a week for a laptop, trying one key after another, to crack a code encrypted with a 56-bit key.
 - a) Assuming computers double in speed every 18 months, in what year could the average new laptop crack the code in an hour?
 - b) Suppose that at the point when a laptop can crack a 56-bit key, browsers increase key length to 128 bits. How long will it take the faster laptop to crack a 128-bit key?
2. A radio station owns a 100,000 W antenna that broadcasts in the range 104.2 MHz - 104.4 MHz. A nearby source of interference in the same frequency range is generated with a power of 20,000 W.
 - a) What is the channel capacity of the radio station's broadcast antenna?
 - b) If the radio station wanted to double its channel capacity by increasing the power of its broadcast signal, at what power should the signal be transmitted?
 - c) If the radio station decided instead to increase its bandwidth to double channel capacity, how much bandwidth is needed? Why would the FCC not allow this?
3. These questions are about modular arithmetic.
 - a) Compute $12^{35} \pmod{7}$. Show your work.
 - b) Suppose Alice and Bob decide to share a secret key using Diffie-Hellman key agreement. Publicly known to everyone is the "root" 29, and the "modulus" 59. Alice picks 47 as her private key. What is Alice's public key?
 - c) Why does Diffie-Hellman use modular arithmetic rather than ordinary arithmetic?
4. Copyright law has been part of our legal system since the nation began.
 - a) What balance was the copyright clause of the US Constitution intended to strike?
 - b) Give one example where US copyright law has succeeded in striking its intended balance.
 - c) Give one example where US copyright law has failed to strike its intended balance.
5. The President is going to give a global video address to be streamed over the Internet only.
 - a) Which would you recommend he use, TCP or UDP? Why?
 - b) After the address, the President's supporters receive an email with a link to the video. You notice:
 - The "From:" header reads barack@whitehouse.gov
 - The "To:" header lists your email address
 - The link to the video in the email reads <http://www.whitehouse.gov/videos.051509address.cn/video.html>

Does anything appear suspicious? Explain.

6. Section 230 of the Communications Decency Act deals with how website operators handle defamatory statements appearing on the website. The Digital Millennium Copyright act deals with how website operators handle copyright violations appearing on the website. What is the key difference between these laws as they affect operators of websites with allegedly illegal content?

7. 53,849 people are employed by or enrolled at Harvard. Each has a unique Harvard ID number (HUID).
 - a) Given an ordered list of HUIDs, how would you efficiently find a particular HUID?
 - b) How many steps would it take to determine that a particular ID number was not in the list?
 - c) What if the list of IDs was out of order?