CS 3501: ICS Exam 1, spring 2019

Name

You MUST write your e-mail ID on **EACH** page and bubble in your userid at the bottom of this first page. And put your name on the top of this page, too.

If you are still writing when "pens down" is called, your exam will be ripped up and not graded – even if you are still writing to fill in the bubble form. So please do that first. Sorry to have to be strict on this!

Other than bubbling in your userid at the bottom of this page, please do not write in the footer section of this page.

There are 6 pages to this exam. Once the exam starts, please make sure you have all the pages. Questions are worth different amounts of points.

If you do not bubble in this first page properly, you will not receive credit for the exam!

Answers for the short-answer questions should not exceed about 20 words; if your answer is too long (say, more than 30 words), you will get a zero for that question!

This exam is CLOSED text book, closed-notes, closed-calculator, closed-cell phone, closed-computer, closed-neighbor, etc. Questions are worth different amounts, so be sure to look over all the questions and plan your time accordingly. Please sign the honor pledge below.

> Serious error. All shortcuts have disappeared. Screen. Mind. Both are blank.

(the bubble footer is automatically inserted into this space)

Page 2: General

1. [3 points] You walk into a grocery store. *Briefly*, list three things that would occur to you if you were using the security mindset.

2. [3 points] *Briefly*, describe zombies and also describe botnets.

3. [3 points] *Briefly*, what is the difference between a virus and a worm?

4. [3 points] List four different types of encryption that a virus might use to encrypt itself.

Page 3: Ethics and Policy

5. [3 points] *Briefly,* what is the difference between Consequentialist ethics and Utilitarian ethics?

6. [3 points] *Briefly*, give one possible abuse of Virtue ethics and one possible abuse of Deontological ethics.

7. [3 points] Briefly, what one thing was the worst part of the SOPA and PIPA bills?

8. [3 points] *Briefly*, how did the recent US government (partial) shutdown hurt cybersecurity efforts?

Page 4: Encryption

9. [3 points] State the formuals for encryption and decryption of an RSA message.

10. [3 points] Describe the algorithm for signing an RSA message.

11. [3 points] *Briefly,* What were the problems with the development of the DES encryption algorithm? How were these resolved with AES?

12. [3 points] What three requirements are necessary to ensure that a one-time pad is perfectly secure?

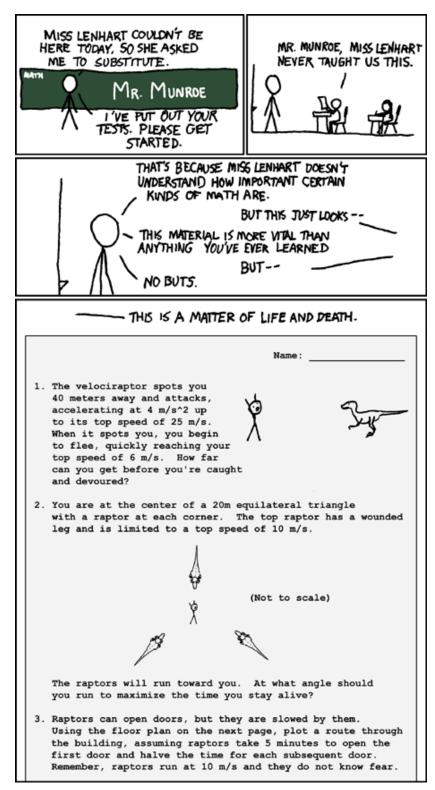
Page 5: More encryption

13. [6 points] Given a = 11, c = 7, m = 5, and a starting seed of 1, give the remaining terms of this random sequence using the linear congruential generator (LCG) method

14. [3 points] *Briefly*, what is a collision resistant hash?

15. [3 points] Using a standard Caesar cipher (with shift of 3), decode the following message: "gduwk ydghu lv ohld'v idwkhu".

Page 6: No questions here



This page unintentionally left blank.

xkcd #135