# CS 3710: ICS Exam 1, fall 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.

*In theory, there is no difference between theory and practice.*
*But, in practice, there is.*

(the bubble footer is automatically inserted into this space)

## Page 2: Intro and Policy

1. [3 points] What is a zombie? When and/or how would it be used?

2. [3 points] As per the security mindset, *briefly* name 4 things you would be looking at if you went into a grocery store.

3. [3 points] *Briefly* describe the biggest problem with U.S. cybersecurity policy today.

4. [3 points] *Briefly,* how would have SOPA and PIPA broken DNS?

## Page 3: RSA

5. [3 points] List the RSA encryption and decryption formulas.

6. [3 points] *Briefly*, give the two reasons why RSA is considered secure.

7. [3 points] *Briefly*, why do you pad a RSA message to the length of the block size? And what do you pad with?

8. [3 points] *Briefly* describe the steps for one to check the signature of a RSA signed message.

## Page 4: Encryption

9. [3 points] Decode this Caesar cipher (with the standard shift): `brx duh ehlqj zdwfkhg`

10. [3 points] *Briefly*, once a https session is fully established, why is AES used instead of RSA for the encryption?

11. [3 points] *Briefly*, what does *cryptographically secure pseudo-random number generator* mean?

12. [3 points] *Briefly*, what does *collision resistant hash* mean?
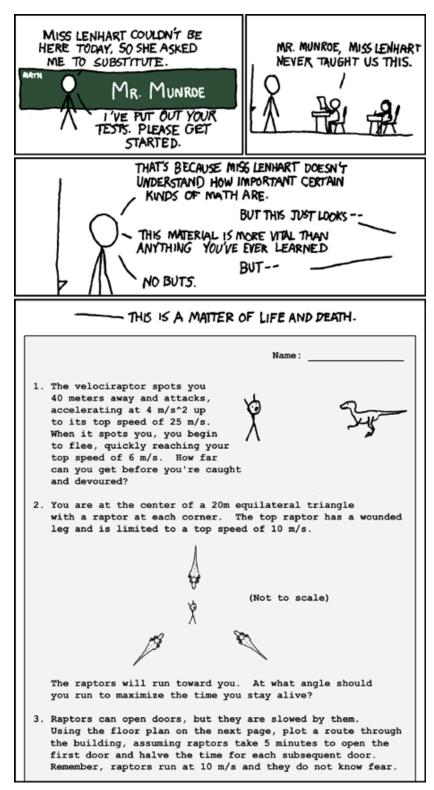
## Page 5: Miscellaneous

13. [4 points] Of the four ethical frameworks, which do you find the most useful? *Briefly*, why is that one more useful than the others?

14. [4 points] Given the values $a = 5$, $c = 7$, $m = 10$, and initial seed of 1, what is the random sequence generated via the linear congruential generator (LCG) method? Is this a good sequence? *Briefly*, why or why not?

15. [4 points] List and *briefly* describe the layers in the TCP/IP networking model (NOT the ISO model!).

# Page 6: No questions here

This page unintentionally left blank.



xkcd #135