# CS 3710: ICS Midterm, summer 2022

# Name

You MUST write your e-mail ID on **EACH** 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. So please do that first. Sorry to have to be strict on this!

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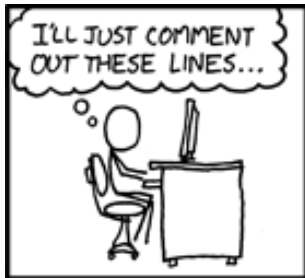
**Answers for the short-answer questions should not exceed about 20 words; if your answer is too long (say, more than 30 words), you will get a zero for that question!**

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.*

## Page 2: Introduction

1. [3 points] *Briefly*, what is the difference between a virus and a worm?

2. [6 points] List four things that come to mind when you apply the security mindset to thinking about how people could cheat on written midterm examinations.

3. [3 points] *Briefly*, what is the difference between a vulnerability and an exploit?

## Page 3: Ethics & Networks

4. [6 points] *Briefly* describe one abuse of each of the four ethical frameworks we studied in lecture.

5. [3 points] Other than brute force, name and (briefly!) describe one of the Denial of Service (DoS) attacks discussed in lecture.

6. [3 points] *Briefly*, what is necessary to properly secure your WiFi network with WPA2?

## Page 4: Encryption

7. [3 points] What is the LCG (linear congruential generator) formula for determining the next number in a pseudo-random number sequence? Make sure you label your variables!

8. [3 points] List the steps necessary to sign a message with an RSA key pair.

9. [3 points] *Briefly*, what is a *collision resistant hash*?

10. [3 points] *Briefly*, why aren't rainbow tables effective anymore?

## Page 5: Web Security

11. [3 points] *Briefly*, what prevents an eavesdropper ("Eve") from determining the shared private key in the Diffe-Hellman key exchange?

12. [3 points] *Briefly*, what is *forward secrecy*?

13. [3 points] How is the Master Secret (MS) determined in the TLS protocol? *Briefly* describe each part that contributes to the MS.

14. [3 points] *Briefly*, name and describe one of the attacks on https discussed in lecture.

# Page 6: No questions here

This page unintentionally left blank.



xkcd #424