

## CS 3710: Intro to Cybersecurity Final Exam, spring 2023

**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.

---

---

---

---

*Thank you for leaving  
your computer unsecured  
your data is mine*

**Page 2: Encryption and Networks**

1. [4 points] Consider the random sequence from the LCG (Linear Congruential Generator) with modulus  $m = 7$ , multiplier  $a = 3$ , and increment  $c = 2$ . Given seed 0, generate the first three terms of this sequence. Show your work, but put the term values in order in the boxes shown.

2. [4 points] What is the formula to encrypt a plain text message  $m$  with RSA? Put your answer in the box!

3. [4 points] *Briefly*, what two properties make RSA hard to crack?

4. [4 points] List three things that makes the TLS protocol secure.



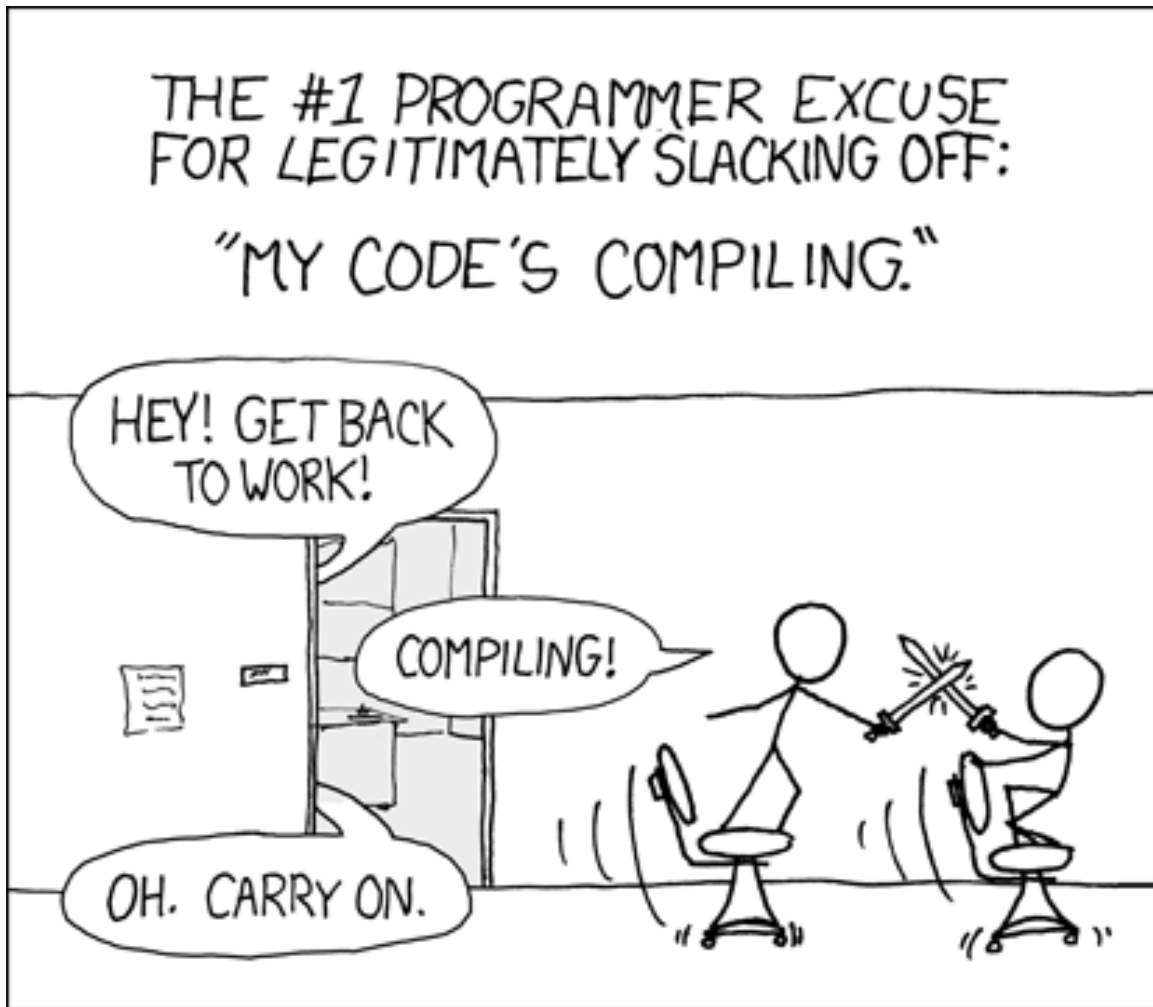


**Page 5: Non-technical (ethics, policy, security mindset, forensics, etc.)**

13. [4 points] *Briefly*, When can the government force you to reveal your encrypted hard drive password?
14. [4 points] *Briefly*, What is the biggest vulnerability to UVA security?
15. [4 points] Which ethical framework do you find most compelling? *Briefly*, why?
16. [4 points] Using the security mindset, how would you prevent future students from cheating, by using a generative AI system such as ChatGPT, on programming assignments?

**Page 6: No questions here**

This page unintentionally left blank.



xkcd #303

(title text: Are you stealing those LCDs? "Yeah, but I'm doing it while my code compiles.")