CS 3710: Introduction to Cybersecurity Midterm, summer 2024

Name _____

Be sure to write your name and e-mail ID on top of this page.

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.

_____

_____

_____

_____

Plz enable me

I'm just a tiny macro

Docs wiped. Kthnxbai.

Page 2: Security mindset, Ethics, & Policy

1. [6 points] Apply the security mindset to analyze how to prevent students in collegiate courses from cheating on exams. This means prevention from any and all viable forms of cheating (you don't need to list them, but your response should work against all forms of cheating). This analysis should just list the countermeasures: actionable steps to take to decrease cheating – we aren't looking for the assets or threats part of this analysis.

2. [6 points] Consider the ethical dilemma of whether one should use cryptocurrency, considering that it is (a) used to commit crime online, and (b) hurting the environment with all the computing resources put into hashing. Analyze this dilemma with each of the ethical frameworks (you can combine consequentialist and utilitarian, so it's really three frameworks). For each of these analyses, describe how the framework would judge this dilemma, and what the result would be. We realize there needs to be a bit more writing on this one, but you still have to keep it as brief as possible!

Page 3: Encryption

3. [3 points] *Briefly,* describe a *viable* way to attack RSA. This can not be the drug-them-and-beat-them-with-a-wrench idea shown in the xkcd on the last page of this exam.

4. [3 points] *Briefly,* what was the motivation to develop the SHA-3 (Keccak) hash?

5. [6 points] Consider the linear congruential generator (LCG) where $m = 8$, $a = 5$, $c = 3$, and $X_0 = 1$ (recall that a is the multiplier, c is the increment, and m is the modulus). What is the random number sequence generated by this LCG? Write out all the terms until it repeats.

Page 4: Networks

6. [6 points] *Briefly,* list the 5 layers in the TCP/IP network stack (*not* the ISO network stack), and briefly explain the purpose of each layer.

7. [3 points] *Briefly,* what is Cipher Block Chaining (CBC)? This is the same thing as encryption with Initialization Vectors (IVs). Briefly, how does it work?

8. [3 points] *Briefly* describe three different ways firewalls work to keep out ”bad” traffic.

Page 5: Miscellaneous

9. [3 points] *Briefly,* describe how the Diffe-Hellman key exchange (DHE) works.

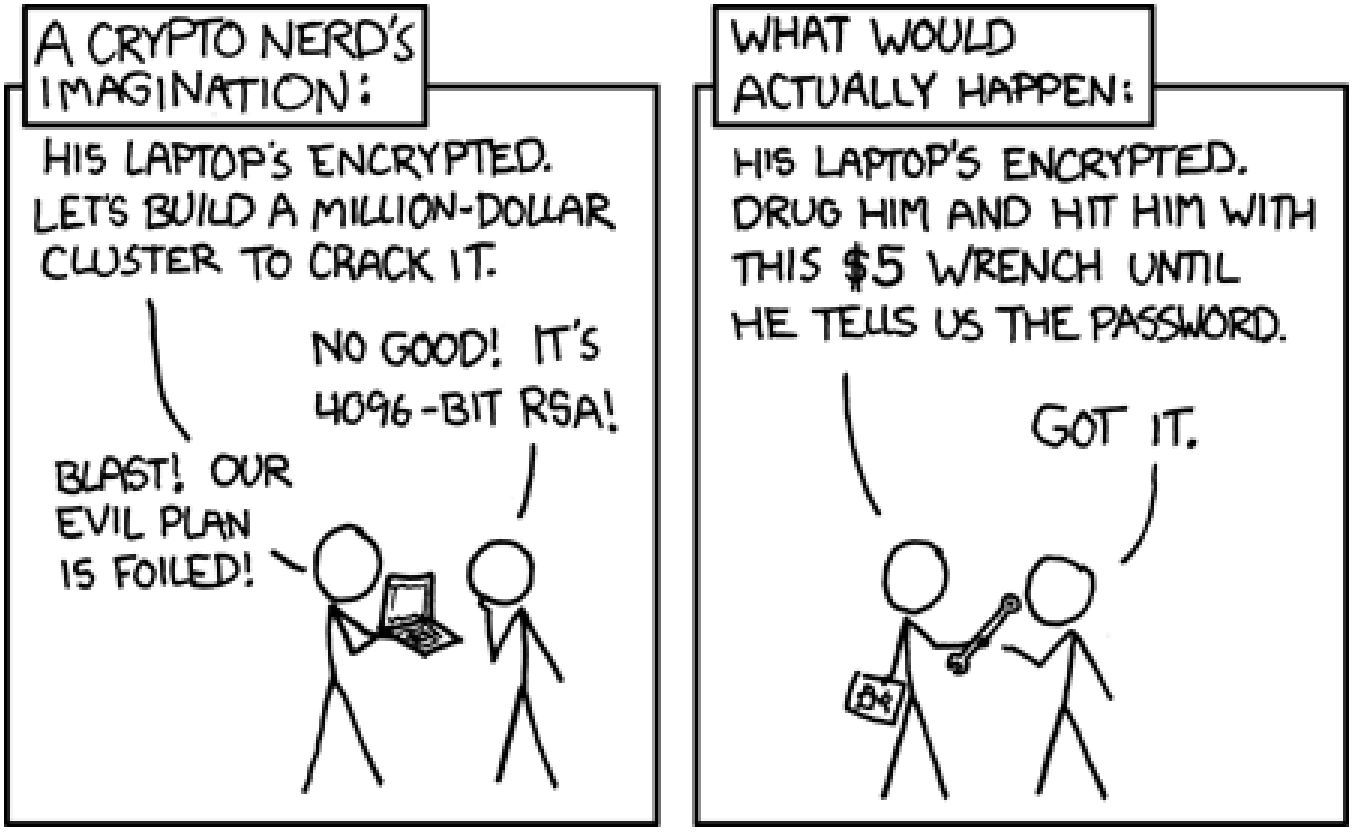
10. [3 points] *Briefly,* what is the difference between authorization and authentication?

11. [3 points] What is the biggest security vulnerability today? Back up your answer with a (*brief*) justification.

12. [3 points] *Briefly* describe one of the malware case studies we have covered in lecture this summer term, and why it was effective. You can't use the Morris Worm for this.

Page 6: No questions here

This page unintentionally left unblank.



xkcd #538