CS 3710: Introduction to Cybersecurity Midterm, fall 2023

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

2. [3 points] Pick one of the security leaks from a 3-letter agency (NSA, FBI, CIA, etc.) discussed in class. Those are: Chelsea Manning, Edward Snowden, Shadow brokers, and Reality Winner. State which one you chose, and *briefly* state the primary lesson learned from that situation.

3. [3 points] List the four ethical frameworks and *briefly* describe each.

4. [3 points] Is analyzing security weaknesses by using the security mindset ethical? Why or why not?

Page 3: Encryption

5. [3 points] State the formula for RSA encryption and also the formula for RSA decryption.

6. [3 points] State the formula to determine the next term in a LCG (linear congruential generator) pseudo-random number generator. Explain what each of the variables is in your answer.

7. [3 points] Decrypt this ciphertext using a Caesar Cipher with a shift of 3: `grrugrqrwwkhuhlvqrwub`. (Although not required, it will be much cooler if you put the spaces in the right spots).

8. [3 points] What is the point of the joke in the XKCD comic on the last page of this exam?

Page 4: Networks

9. [6 points] Explain how Diffe-Hellman prevents an eavesdropper from finding the shared secret key.

10. [3 points] Why isn't TLS 1.2 (the version we studied in-depth in lecture) forward-secret?

11. [3 points] What is a certificate (as it relates to network security)?

12. [3 points] List two reasons why all DoS (Denial of Service) attacks are always distributed.

Page 5: Miscellaneous

13. [3 points] *Briefly* differentiate between authentication and authorization.

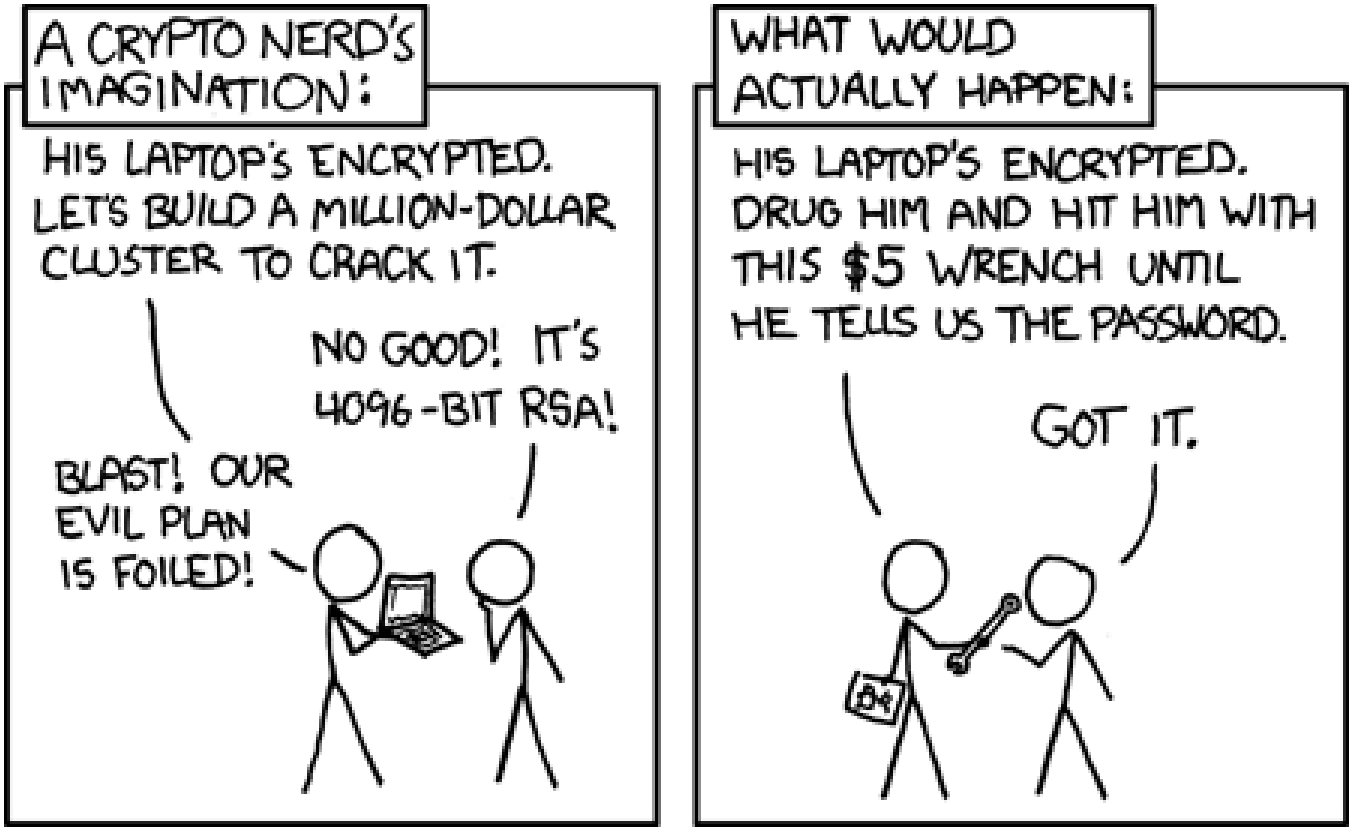
14. [3 points] Write a fork bomb (aka rabbit). You can pick the programming language, but state which one, as it may not be obvious. You can omit `import` and `include` lines. For partial credit, you can write this in pseudo-code.

15. [3 points] *Briefly* describe the the difference between a network switch and a router.

16. [3 points] How does modern WiFi encryption (WPA and WPA2) prevent the same data being sent twice from appearing as the same ciphertext?

Page 6: No questions here

This page unintentionally left unblank.



xkcd #538