CS 3710: Intro to Cybersecurity Midterm, 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.

Plz enable me

I'm just a tiny macro

Docs wiped. Kthnxbai.

Page 2: Security mindset, Ethics, & Policy

1. [4 points] Using the security mindset, *briefly* discuss how you would detect and/or prevent cheating using ChatGPT (or similar) on an essay assignment. You cannot use the structure of the ethics assignment (have ChatGPT generate an answer and analyze it) as your response.

2. [4 points] *Briefly* list one abuse of each of the ethical frameworks discussed in class.

3. [4 points] List four of the challenges discussed in class that are facing US cybersecurity policy.

Page 3: Encryption

4. [3 points] *Briefly*, what feature(s) of RSA make it secure?

5. [3 points] Given the LCG (Linear Congruential Generator) with $c = 3$, $a = 5$, and $m = 8$, compute the first 4 pseudo-random numbers with a starting seed of 1.

6. [3 points] *Briefly* explain, in English, how a man-in-the-middle (MITM) attack works against RSA.

7. [3 points] What is required for a one-time pad (OTP) to be secure? If those thing(s) is/are provided, how secure is an OTP?

Page 4: Networks

8. [6 points] List the layers in the OSI network model, and *briefly* describe each or explain what each does (no more than 10 words description per level!)

9. [3 points] List and *briefly* describe three different types of Denial of Service (DOS) attacks.

10. [3 points] How does the Diffe-Hellman key exchange ensure that an eavesdropper cannot figure out the shared private key?

Page 5: Miscellaneous

11. [3 points] *Briefly,* how does the TLS protocol prevent man-in-the-middle attacks?

12. [3 points] *Briefly,* what is a collision-resistant hash?

13. [3 points] *Briefly,* what is a certificate (as it relates to cybersecurity)?

14. [3 points] *Briefly* define both vulnerability and exploit.

Page 6: No questions here

This page unintentionally left blank.

DEAR VARIOUS PARENTS, GRANDPARENTS, CO-WORKERS, AND OTHER "NOT COMPUTER PEOPLE."

WE DON'T MAGICALLY KNOW HOW TO DO EVERYTHING IN EVERY PROGRAM. WHEN WE HELP YOU, WE'RE USUALLY JUST DOING THIS:
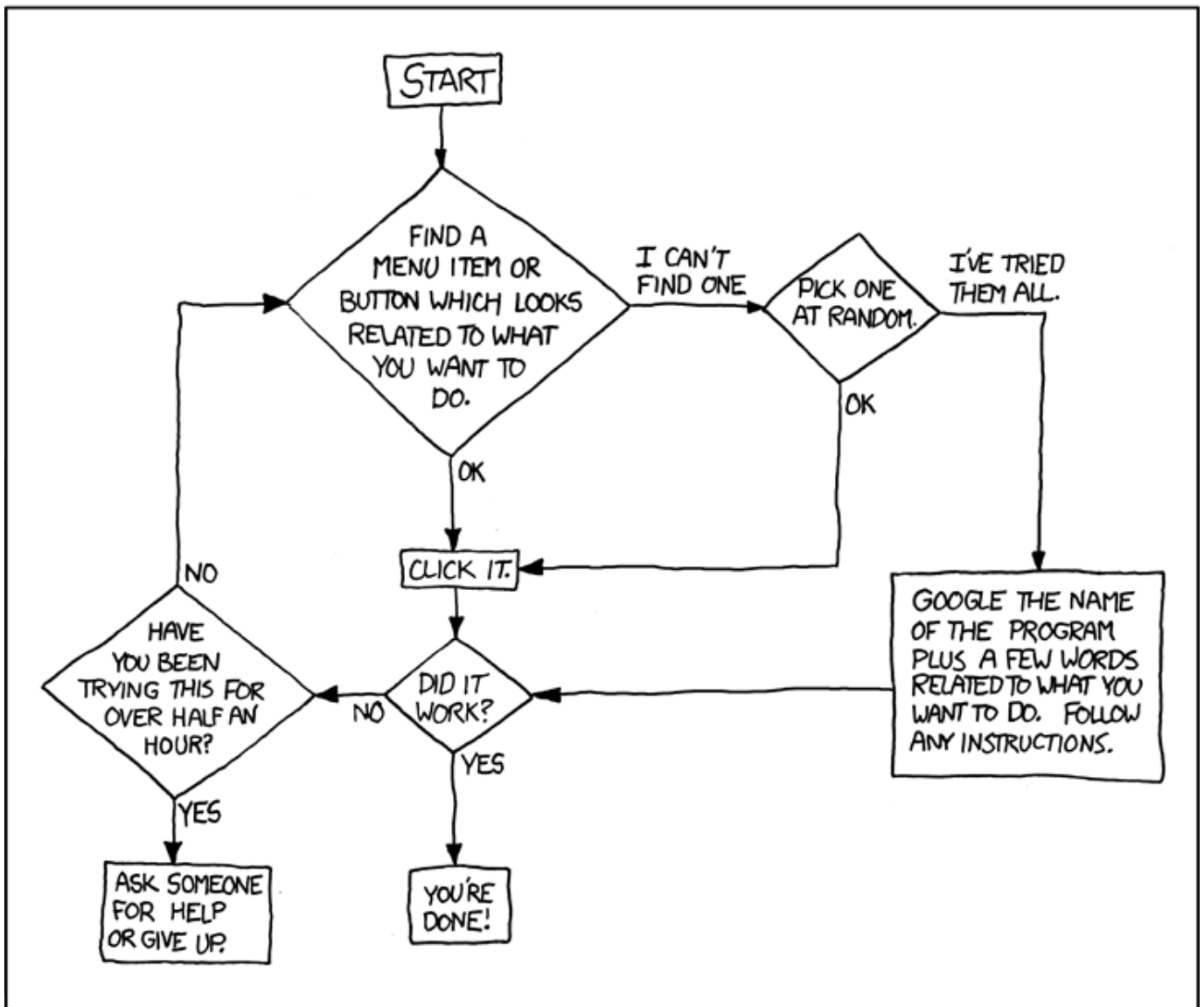
PLEASE PRINT THIS FLOWCHART OUT AND TAPE IT NEAR YOUR SCREEN. CONGRATULATIONS; YOU'RE NOW THE LOCAL COMPUTER EXPERT!

xkcd #627