CS 3710: Intro to Cybersecurity Midterm, summer 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. [6 points] *Briefly,* list one abuse of each of the four ethical frameworks discussed in class.

2. [3 points] *Briefly,* what is the security mindset?

3. [3 points] *Briefly,* what was the worst part of SOPA / PIPA?

Page 3: Encryption

4. [3 points] *Briefly,* how would you break RSA via integer factorization? How would you do so via discrete logs?

5. [3 points] *Briefly,* explain what password salting is, and why it is necessary.

6. [3 points] *Briefly,* what is the difference between a code and a cipher?

7. [3 points] *Briefly,* What is *forward secrecy*, and why do we care about it?

Page 4: Networks

8. [3 points] *Briefly,* what part(s) of the TLS protocol prevent an entity (”Mallory”) from modifying the network data sent in order to perform a man-in-the-middle attack, or cause other problems?

9. [3 points] *Briefly,* how is a MAC (Message Authentication Code) different from a RSA digital signature?

10. [3 points] *Briefly,* what is *forward secrecy*, and why do we care about it?

11. [3 points] *Briefly,* why can an eavesdropper (”Eve”) not determine the shared private key when using the Diffe-Hellman key exchange?

Page 5: Miscellaneous

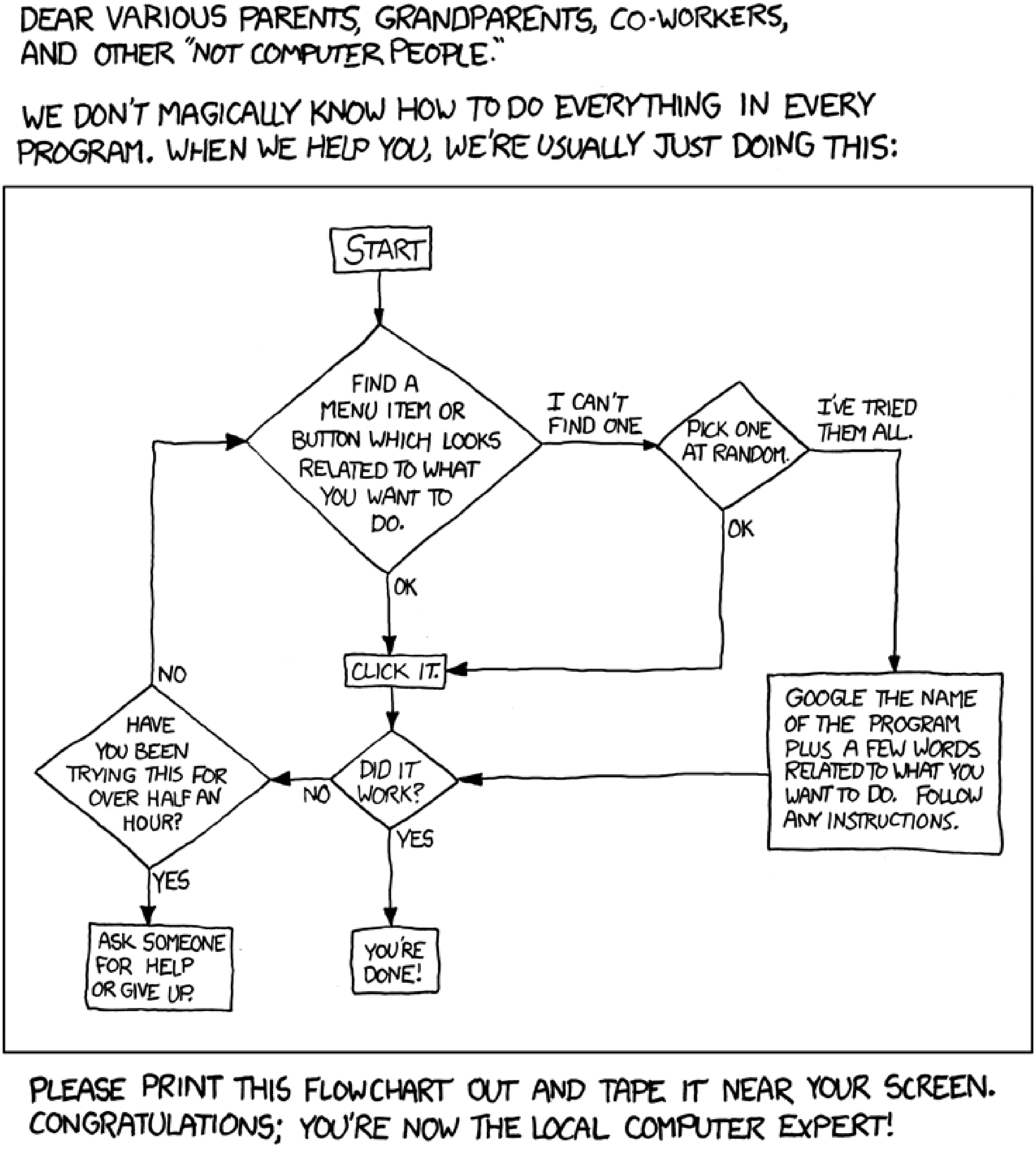
12. [6 points] *Briefly,* Using the LCG (Linear Congruential Generator) method, what is the pseudo-random number sequence generated by using multiplier $a = 5$, increment $c = 7$, and modulus $m = 8$, starting with a seed value of 0?

13. [3 points] *Briefly,* what is the difference between a virus and a worm?

14. [3 points] *Briefly,* what is a zombie? (In terms of cybersecurity, not an undead entity)

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:
START
FIND A MENU ITEM OR BUTTON WHICH LOOKS RELATED TO WHAT YOU WANT TO DO.
I CAN'T FIND ONE
PICK ONE AT RANDOM.
I'VE TRIED THEM ALL.
OK
OK
CLICK IT.
GOOGLE THE NAME OF THE PROGRAM PLUS A FEW WORDS RELATED TO WHAT YOU WANT TO DO. FOLLOW ANY INSTRUCTIONS.
NO
HAVE YOU BEEN TRYING THIS FOR OVER HALF AN HOUR?
NO
DID IT WORK?
YES
YES
ASK SOMEONE FOR HELP OR GIVE UP.
YOU'RE DONE!
PLEASE PRINT THIS FLOWCHART OUT AND TAPE IT NEAR YOUR SCREEN. CONGRATULATIONS; YOU'RE NOW THE LOCAL COMPUTER EXPERT!

xkcd #627