CS 3710: Introduction to Cybersecurity Midterm, fall 2025

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.

_____

_____

_____

_____

Free public WiFi

Is it really safe to use?

Ask Man in Middle

Page 2: Security mindset, terminology, & ethics

1. [3 points] *Briefly* define the security mindset.

2. [3 points] Give two uses for a botnet.

3. [6 points] List the four ethical frameworks, and *briefly* describe one abuse of each.

Page 3: Encryption

4. [3 points] There are two mathematical problems that make RSA hard to crack. List them, and *briefly* indicate what actual part of the math is the hard part (this can be prose or formulas).

5. [6 points] LCG: consider the linear congruential generator with parameters $m = 8$, $a = 5$, and $c = 7$. With a seed of 1, compute the rest of the terms in this sequence.

6. [3 points] *Briefly* describe what characteristics make a good *password salt*.

Page 4: Encryption and Networks

7. [3 points] *Briefly* describe how you sign a message with RSA.

8. [3 points] Name the part(s) of the OSI networking model that are not in the TCP/IP model, and *briefly* explain what they do.

9. [3 points] *Briefly,* when a network packet arrives at a computer, how does the computer know what application to send it to?

10. [3 points] *Briefly,* why do we use IVs (initialization vectors) when encrypting a stream of network packets?

Page 5: Web security

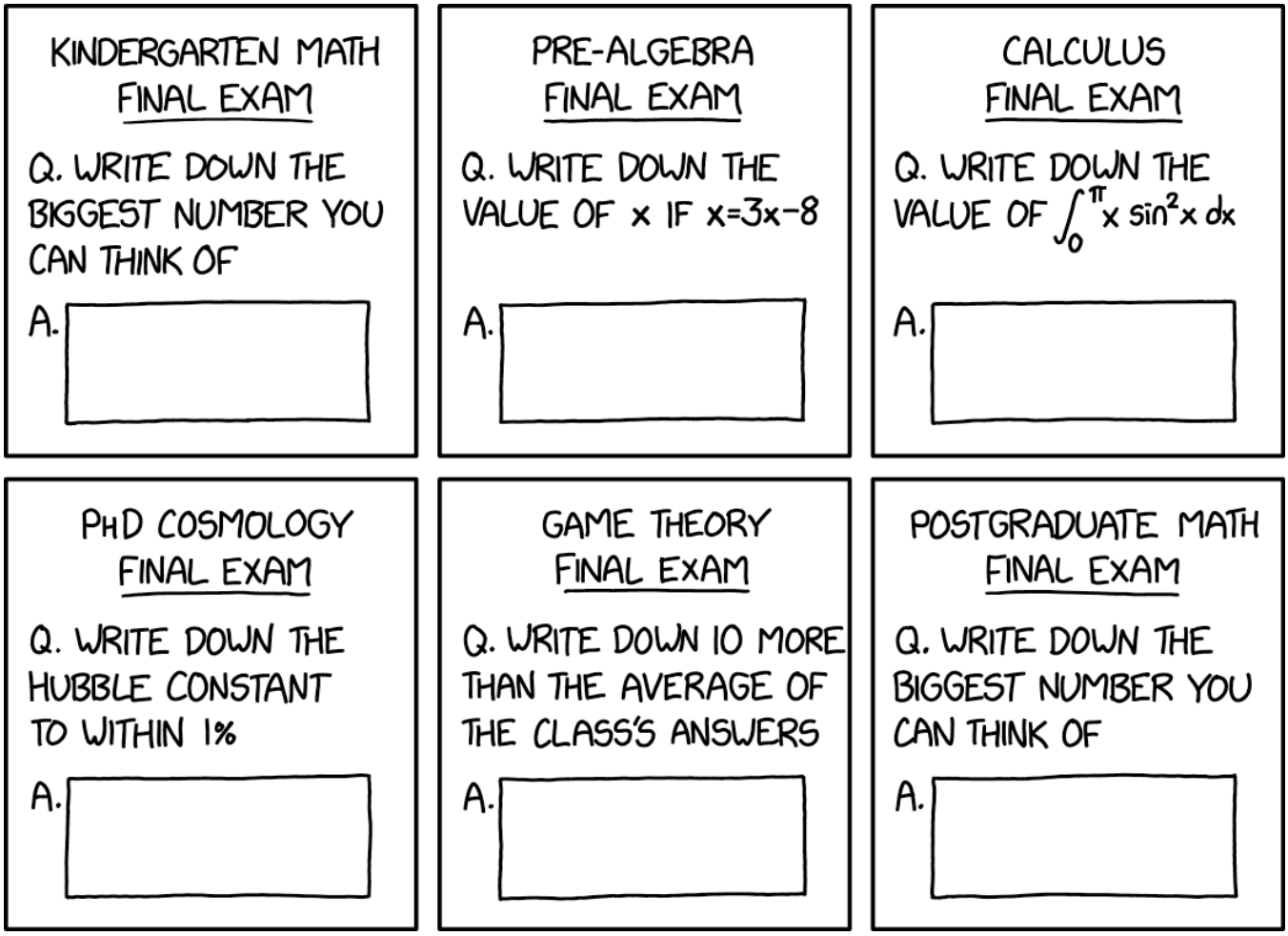
11. [6 points] Summarize the steps of the TLS algorithm. This can be in prose or a bulleted list. If it's easier, you can also create a network diagram (with arrows back-and-forth) such as was presented in lecture – but be sure to indicate what data is transferred for each arrow.

12. [3 points] *Briefly* what is a MAC (Message Authentication Code)? How do you compute one?

13. [3 points] Name and *briefly* explain three different attacks on 2FA (two-factor authentication).

Page 6: No questions here

This page unintentionally left unblank.



xkcd #2966