CS 3501: ICS Final Exam, spring 2019

Name _____

You MUST write your e-mail ID on **EACH** page and bubble in your userid at the bottom of this first 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 – even if you are still writing to fill in the bubble form. So please do that first. Sorry to have to be strict on this!

Other than bubbling in your userid at the bottom of this page, please do not write in the footer section of this page.

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.

If you do not bubble in this first page properly, you will not receive credit for the exam!

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.

_____

_____

_____

_____

You step in the stream,
But the water has moved on.
This page is not here.

(the bubble footer is automatically inserted into this space)

Page 2: Exam 1 material

1. [4 points] Name and *briefly* describe the four ethical frameworks discussed in lecture.

2. [4 points] For each of the ethical frameworks discussed in lecture, *briefly* specify how it can be abused.

3. [4 points] Public key cryptosystems can be implemented using prime numbers, discrete logs, or elliptical curves. Let's consider the first two (primes and discrete logs). For each of those, what is the "easy" part that is used for encryption and decryption, and what is the "hard" part that one must accomplish to crack an encrypted message?

Page 3: Exam 2 material

4. [3 points] What is the value of a stack canary? If not obvious, also state it's size.

5. [3 points] *Briefly* describe the difference between oligomorphic, metamorphic, and polymorphic viruses.

6. [3 points] Write a single `printf()` statement that writes the value 32,769 (0x8001) to pointer address 0x12345678. Your answer obviously can not be 32 thousand characters or so.

7. [3 points] Name the layers in the TCP/IP networking model

Page 4: Web Security

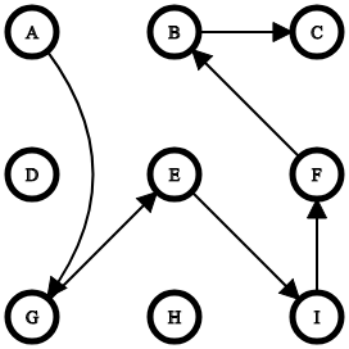
8. [6 points] Explain how the Diffie-Hellman key exchange works. This can be an English explanation, series of algorithmic steps, or an example usage.

9. [3 points] *Briefly,* what is forward secrecy?

10. [3 points] What are 3 properties of message authentication codes and – *briefly* – why are those properties important?

Page 5: Cryptocurrency and Anonymity

11. [3 points] Consider the graph showing the routing *within* a Tor network – A is the entry node and C is the exit (or destination) node. Using the `encrypt()` and `sendTo()` primitives discussed in class, what is the message sent to the entry node A for destination C?



12. [3 points] *Briefly,* why is Bitcoin mining so hard?

13. [3 points] *Briefly,* how does one access a hidden service in Tor?

14. [3 points] *Briefly,* how could a government detect that you are using Tor?

Page 6: Miscellaneous

15. [3 points] Name and *briefly* describe the 4 levels of virtual machines.

16. [3 points] Other than a biologist handling DNA matching, name and *briefly* describe three forensic sciences.

17. [3 points] *Briefly,* what is the *Foregone Conclusion Doctrine*, and why is it relevant?

18. [3 points] *Briefly,* how would SOPA and PIPA have negatively affected how the Internet works?