Name: _____ E-mail ID: _____@virginia.edu

Pledge: _____

_____

_____

Signature: _____

There are 75 minutes for this exam and 100 points on the test; don't spend too long on any one question!

The 12 short answer questions require only a sentence or two for full credit; the two long answer questions have their own page, and obviously require more. There are 12 short-answer questions worth 5 points each, and two long-answer questions worth 20 points each.

All work must be on these exam pages.

Good luck!

Page 2	_____ / 15
Page 3	_____ / 15
Page 4	_____ / 15
Page 5	_____ / 15
Page 6	_____ / 20
Page 7	_____ / 20
Total	**_____ / 100**

Short answer questions (5 points each): these questions only require a sentence or two for full credit.

1. Why is cracking (i.e. decrypting without the authorized decryption key) an RSA-encrypted message very hard to do?

2. Explain, using English only (i.e. no equations or formula), what it means when it is said that a given problem is NP-complete.

3. Explain, using English only (i.e. no equations or formula), what Big-Oh notation means. For example, if a function is said to be $O(n^2)$, what does that mean? Explain for the general case, though – not just the $O(n^2)$ case.

4. Solve the halting problem. Explain your answer. And while you're at it, explain what the halting problem is. Use the last page of this exam if you need more space.

5. A license plate can consist of the digits 0-9 and the letters A-Z. Consider license plates of the form *dde-edd* and *eel-lee*, where *d* is a digit, *l* is a letter, and *e* can be either a digit or a letter. How may possible combinations of license plates can be formed using these two patterns? You can leave your answer as the product of numbers – you don't have to multiply the values out.

6. Determine the greatest common divisor (gcd) and least common multiple (lcm) of 30,030 and 484,704. For your reference, the factorization of 30,030 is 2*3*5*7*11*13, and the factorization of 484,704 is $2^5*3^4*11*17$. Leave your answer is factored form (i.e. 2*3*5*7*11*13 instead of 30,030).

7. Explain the difference between countable and uncountable sets. Don't just give an example!

8. What is the difference between weak induction and strong induction?

9. What is the cardinality of a power set of a set of n elements?

10. Explain, using English only (i.e. no pseudo-code), how the bubble sort XOR the insertion sort works. Include the Big-Oh estimate of the running time as well. We're looking for a general overview here, not all the specific details.

11. Explain, using English only (i.e. no equations or formula) how one goes about doing a structural induction proof. Specifically, how is it different than mathematical induction? Don't just list the three steps for structural induction – explain how those steps are different from the other induction types (or, if they are not different, state such).

12. What (physical) prop did Professor Bloomfield use in class to illustrate how a binary search works?

13. (20 points) Using weak mathematical induction, prove that 5^n+3 is divisible by 4 for $n \geq 0$.

14. (20 points) Give a recursive definition for each of the following sequences. For this question, the first term of the sequence is $n = 1$, not $n = 0$.

a) (5 points) $a_n = n^2$

b) (5 points) $a_n = \sum_{i=0}^{n} i$

c) (5 points) The Fibonacci sequence

d) (5 points) The sequence that generates the terms 3, 6, 12, 24, 48, 96, 192, …

This page intentionally left blank

(you can use this space to solve the halting problem, though)