MA/CSSE 473 – Design and Analysis of Algorithms **In-class Quiz Day 11**

Name:_____ Score:____/ 11 circle your Section # 01(3rd) 02 (4th)

1. In the RSA cryptosystem, how do we pick … ?

   N

   N'

   e

2. Once we have chosen e, how do we find d?

3. Suppose you are given the public key (15, 3), how would you encode the message 4?

4. With the same public key as in the previous problem, how would you decode the message 5?

5. If e and d are as in problem 2, and $0 \leq x < N$, how do we know that $(x^e)^d \equiv x \pmod{N}$?

6. What does *amortize* mean?

7. (3) Suppose we are implementing ArrayList, starting with a capacity of 12 elements, and increasing the capacity as needed. If we start with an empty ArrayList and add elements, one at a time, until we have N elements, (we don't know N in advance), what is the amortized cost of adding each element if we use the following strategies for resizing the underlying array?

– add one element to the capacity each time we need to grow the array,

– double the capacity each time [just do the special case where N is $12(2^k) + 1$]

8. What became clear to you as a result of today's discussion? (or write N/A)

9. Is there anything from today's discussion that was unclear, do you have questions, or is there anything else you want to tell me? (or write N/A)