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

Name:_____Solution_____ Score:____/ 11 circle your Section # 01(3^{rd}) 02 (4^{th})

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

   N **product of 2 primes: p & q** N' **(p-1)(q-1)** e **any number relatively prime to N'**

2. Once we have chosen e, how do we find d? **inverse of e, mod N'**

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

   4^3 %15 = 64 % 15 = 4.

4. With the same public key as in the previous problem, how would you decode the message 5?
   p=5, q=3, so (p-1)(q-1) = 8. The inverse of 3 (mod 8) is 3, so d = 3.

   5^3 % 15 = 125 % 15 = 5.

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

First of all, since e is relatively prime to (p-1)(q-1), it has an inverse, d. so $ed \equiv 1 \pmod{(p-1)(q-1)}$.
By definition of congruence, $ed - 1 = k(p-1)(q-1)$ for some integer k, so $ed = 1 + k(p-1)(q-1)$.
Thus $x^{ed} - x = x^{1 + k(p-1)(q-1)} - x$. Show that this is $\equiv 0 \pmod N$.
By Fermat's little theorem, $x^{p-1} \equiv 1 \pmod p$, so any power of that (in particular $xk(p-1)(q-1)$) $\equiv 1 \pmod p$.
Similarly for q. Thus both p and q divide $x^{1 + k(p-1)(q-1)} - x$. Since they are both prime, pq also divides this number, so that expression is congruent to 0 mod N. Thus $x^{ed} \equiv x \pmod N$

6. What does *amortize* mean?
   To spread the cost over several applications of an operation by calculating the average.

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 did not get to this problem today, so give everyone the three points. And because we did not get to #7, apparently many students missed that there were a #8 and #9, so you don't need to look at the back at all. Give everyone who took the quiz the f5 points for the back page.**

Total number of element copies:
$12+13+14+\ldots+N-1$ = sum(i, i=1..N) – sum(i, i=1..11) = $N(N-1)/2 - (11)(12)/2$, which is $O(N2)$.
So the amortized average cost of adding each of the N elements is O(N).

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

$12 (1 + 2 + 4 + \ldots + 2^k)$ [geometric series]
$= 12 (2^{k+1} - 1) = 12 (2(N-1)/12 - 1)\ 2(N-1) - 12 = 2N - 14$, which is O(N).
So the amortized average cost for adding each of the N elements is O(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)