MATH/CSCI 408 Name: _____

CRYPTOGRAPHY MISSION 10 SOLUTIONS

Deadline: Thursday, 1 December 2016 at 3:05pm
This mission covers Sections 7.5, 9.1, and 9.2.

1. Graded Problems

1. Work through the code on Dr. Kate Stange's cryptography website: `http://crypto.katestange.net/solutions-to-discrete-log-practice-session/`.
   a. What is $L_5(11)$ mod 197?

73

   b. What is $L_5(10)$ mod 197?

186

2. (RSA Signature) Suppose a message is $m = 12$. It is publicly known that $e_A = 7$ and $n = 253$.
   a. If Bob receives the information $y = 81$. Compute $z \equiv y^{e_A} \bmod n$. Did Alice sign the document or not? Justify.

$z = 81^7 \bmod 253 \equiv 16 \not\equiv 12$, so no, she didn't.

   b. Suppose that Bob receives the information $y = 100$ instead. Again, compute z. Did Alice sign the document or not? Justify.

$z = 100^7 \bmod 253 \equiv 12 \not\equiv 12$, so yes, she did.

3. Fill out the course evaluations (in your g.coastal.edu email). Please write meaningful and specific feedback. I will read these to improve my teaching, and they are also used as a way to evaluate how I'm doing at my job.
   Things to keep in mind: which activities did you like most and which worked best? Did you feel like I tried to address your questions throughout the semester? Which aspects of class do you think can be improved upon? **Forward the confirmation email to me to get two points for this mission.**

4. (Optional) I won't see the course evaluations until much later. If you'd like to give some specific feedback now, please do so. In particular, I'd like to hear back about the following questions:
   - Do you feel like we had a sufficient balance of math and computer science topics?
   - What did you think of the Escape Room activity?
   - What did you think of the Current Issues debate?
   - Do you think there was a sufficient mix of teaching styles in the class (e.g. lectures, group work time, presentations)?
   - What is something that you will take away from this class after 10 years?