MATH/CSCI 408 Name: _____

CRYPTOGRAPHY MISSION 09

Deadline: Thursday, 9 November 2017 at 10:50am
This mission covers Sections 7.1, 7.2, and 7.5

Check one:

☐ I received help from the following classmate(s) on this assignment:

_____.

☐ I did not receive any help on this assignment.

1. Graded Problems

1. (Final Project) Provide a document with your brainstorming ideas and logistics (electronic submission or paper submission are both fine). Some ideas of things to address:
   - What is the format of your presentation?
   - What is the mathematical content in your project (this is required)?
   - Who are you going to invite, and how are you going to convince them to show up? Note: one of the projects involves advertising.
   - There will be tables, and Dr. Ho can provide poster boards to the groups that had requested them. If you're using a computer, are there enough outlets in the space (go check it out)? If not, make sure you have your devices charged ahead of time.
   - For those of you who have thought about prizes or other supplies, who exactly do you need to contact? How are you going to contact them and by when?
   - Do you have a clear sense of how you're communicating with your team members? Have you organized logistics?

2. For each of the following, determine the parity of x in the discrete log problem

$$\alpha^x \equiv \beta \bmod p.$$

Then, depending on the parity, write some code (and email it) to do a brute-force search through only the even or only the odd numbers to find all values of x up to the prime p.
a. $5^x \equiv 75 \bmod 107$

b. $11^{23} \equiv 98 \bmod 349$

3. Use the Baby Step, Giant Step algorithm to determine x for $4^x \equiv 20 \bmod 61$.

4. ElGamal
   a. Mallory is sending Sterling Archer a message using ElGamal. His public key is $(p, \alpha, \beta) = (89, 6, 31)$. If Mallory's message is $m = 77$ and she chooses $k = 3$, show the encryption process to determine r and t.

   b. What is the computation Archer does to decrypt the message? Verify that this equals the original message of $m = 77$.

c. Cheryl and Pam are also sending their own ElGamal message but they use $p = 17$ and $\alpha = 3$. Pam chooses her secret to be $a = 6$, so $\beta = 15$. Cheryl sends the ciphertext $(r, t) = (7, 6)$. Determine the plaintext m.

5. (Honors) When proving the Index Calculus method in class for the Discrete Log problem, we showed that

$$\beta\alpha^r = \prod_i p_i^{b_i} \bmod p \text{ implies } L_\alpha^\beta = -r + \sum_i b_i L_\alpha(p_i) \bmod (p-1)$$

where L_α denotes the log base α function. Show the missing steps to get from the first to the second equation. (Hint: use properties of the log function).

2. Recommended Exercises

These will not be graded but are recommended if you need more practice.

- Section 7.6 # 1, 2, 3, 4, 6, 12
- Section 7.7 # 1, 2, 3