MATH/CSCI 408 Name: _____

CRYPTOGRAPHY MISSION 06

Deadline: Thursday, 12 October 2017 at 10:50am
This mission covers Sections 3.7, 3.9, 3.10, 4.1, 4.2.

1. Graded Problems

1. Write a short `for` loop program in CoCalc to compute powers of a number a mod p where p is a prime. In other words, the input of your code should be a and p. The output should be all powers of a^i mod p for $i = 1, 2, \cdots, p-1$. Email this code to Dr. Ho.

2. Using the previous problem, are the following values are primitive roots (i.e. the order is $p-1$) or not?
   a. $a = 4, p = 23$

   b. $a = 5, p = 47$

3. Given an integer a and an odd prime p. Determine if a is a quadratic residue mod p or not. Justify.
   a. $a = 4, p = 11$

   b. $a = 2, p = 19$

   c. $a = 3, p = 29$

4. Given an integer a (not congruent to 0 mod p) and an odd prime p, recall that the Legendre symbol is defined as:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ is a quadratic residue mod } p \\ -1 & a \text{ is a quadratic non-residue mod } p \end{cases}$$

Evaluate the following by using CoCalc's `kronecker(a,b)` function, which is the same as the Legendre symbol:

a. $\left(\frac{7}{13}\right)$

b. $\left(\frac{7}{19}\right)$

c. $\left(\frac{2}{13}\right)$

d. $\left(\frac{14}{13}\right)$

5. Recall that the Law of Quadratic Reciprocity says: Let p and q be odd primes. Then

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & p \equiv 1 \bmod 4 \text{ or } q \equiv 1 \bmod 4 \\ -\left(\frac{q}{p}\right) & p \equiv q \equiv 3 \bmod 4 \end{cases}$$

Compute the following. Be sure to show all work.

a. Compute $\left(\frac{97}{101}\right)$.

b. Explain using Quadratic Reciprocity what the value will be for $\left(\frac{101}{97}\right)$.

c. Compute $\left(\frac{3}{107}\right)$

d. Explain using Quadratic Reciprocity what the value will be for $\left(\frac{107}{3}\right)$

6. Play with the Simplified DES code (written by Dr. N. McNew at Towson): `https://tinyurl.com/fa17-crypto-DES`. Specifically, type in a 12-bit input `100100100100`, a key $K =$ `11111110`, and 7 rounds. Write your output here:

7. (Honors) Read Section 4.7 (Meet-in-the-Middle Attacks) and summarize what you learned in a paragraph or two: