Homework 3, Due Thu July 14, 2016

WARNING: THIS HW IS TWO PAGES LONG, SO DO NOT MISS THE SECOND PAGE

1. (0 points) What is your name? Write it clearly. STAPLE your HW.

2. (10 points)
   Alice and Bob are going to use a 1-time pad. When they meet Alice and Bob agree on the key

   0010101111111111000000000000001111100100

   After that is established Alice and Bob communicate:

   (a) Alice wants to send 0011001. What does she send?
   (b) THEN Bob wants to reply by sending 111100110. What does he send?
   (c) THEN Alice wants to send a really long response. What is the LENGTH of the longest message he can send?

3. (20 points) Compute the following and show all work.

   (a) $2^{40} \pmod{200}$
   (b) $8^{2000} \pmod{200}$.

4. (20 points) Test $g = 2, 3, 4, 5, 6, 7, \ldots$ for being generators mod 23 until you find 3 generators. Show your work.

5. (20 points) Let $g$ be the third generator found in the last problem.

   (a) Do a table of $i$ and $g^i \pmod{23}$.
   (b) Do a table of $i$ and $DL_g(i)$ (the discrete log mod $i$).
6. (20 points)

(a) Find all of the primes \( p \) in \( \{60, 61, \ldots, 120\} \). How many are there? What fraction of numbers in \( \{60, \ldots, 120\} \) are primes?

(b) (You can use your list from part a to help do this part.) Find all of the primes \( p \) in \( \{60, 61, \ldots, 120\} \) such that \( p - 1 = 2q \) where \( q \) is a prime (these are called safe primes). How many are there? What fraction of numbers in \( \{60, \ldots, 120\} \) are safe primes?

7. (10 points) Give a solution to THE HATS PROBLEM with three colors of hats such that the people do pretty well. Make your answer CLEAR AND EASY TO READ. Its okay if its not the best possible- I just want you to think about the problem and do something interesting.