Homework 3, Due Thu July 16, 2015

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. (20 points) Alice and Bob are using the Playfair cipher. (RECALL-this is the one that takes a word and makes a 5×5 square of letters out of it, and uses it to map pairs of letters to pairs of letters.) The keyword is *probability*.

   (a) Write the 5×5 square of letters that Alice and Bob use to both encode and decode.

   (b) Alice wants to send the phrase *this hw has typos*. What does she send?

   (c) Bob gets the coded message. DESCRIBE how Bob recovers the original message. Your explanation should be so good it could be in my notes as an example.

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

   (a) $3^{100} \pmod{200}$

   (b) $7^{1000} \pmod{200}$.

4. (20 points) Test $g = 2, 3, 4, 5, 6, 7, \ldots$ for being generators mod 47 until you find 3 generators. Show your work.

5. (20 points)

   (a) Find all of the primes p in $\{50, 51, \ldots, 100\}$. How many are there? What fraction of numbers in $\{50, \ldots, 100\}$ are primes?

   (b) (You can use your list from part a to help do this part.) Find all of the primes p in $\{50, 51, \ldots, 100\}$ such that $p - 1 = 2q$ where q is a prime (these are called *safe primes*). How many are there? What fraction of numbers in $\{50, \ldots, 100\}$ are safe primes?

6. (20 points) Alice and Bob are going to use a 1-time pad. When they meet Alice and Bob agree on the key

0010101011111111111000000000000011111001000000001101011111111001010101

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 reply by sending 101001001111011.

(d) THEN Bob wants to send a really long response. What is the LENGTH of the longest message he can send?