Homework 4, Due Fri July 18, 2014

FOR THIS PROBLEM YOU MAY USE A CALCULATOR OR WOLFRAM ALPHA (look it up on the web) BUT YOU MUST SHOW YOUR FINAL RESULTS.

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

2. (10 points) Find all primes $p \leq 100$ such that $(p-1)/2$ is prime. For each such prime list p and also list $(p-1)/2$.

3. (10 points) Let $p = 59$. Find the first 2 generators mod p. For the next problem let g be the second one. (NOTE that $(p-1)/2 = 29$, a prime, so you can use that trick to shorten the check.)

4. (20 points) Let $p = 59$ and g be as in the last problem. Compute the following mod p. $g^1, g^2, g^3, g^4, g^5, g^6, g^7, g^8$. Put them in a table and sort the table on the second coordinate (note that we are going to do the Baby Step/Giant Step).

5. (10 points) Let $p = 59$ and g be as in the last problem. Find g^{-1}.

6. (20 points) Let $p = 59$ and g be as in the last problem. Compute the following mod p. $g^{-8\times 1}, g^{-8\times 2}, g^{-8\times 3}, g^{-8\times 4}, g^{-8\times 5}, g^{-8\times 6}, g^{-8\times 7}, g^{-8\times 8}$

   Put them in a nice table (no need to sort).

7. (30 points) Let $p = 59$ and g be as in the last problem. USING the Baby-step Giant-step method (and show ALL work) find the discrete log of 10, 11, and 12. (Use $m = 8$ as the tables are already geared towards that.)