Homework 4, Due Fri July 17, 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. (15 points) Fill in the XXX and YYY in the following sentence. Show your work.

   To test if g is a generator mod 29 I need to look at g^x for all $x \in XXX$. If any of them are YYY then g is NOT a generator. If NONE of them are YYY then g IS a generator.

3. (30 points) Alice and Bob are going to do the Diffie Helman protocol with $p = 29$ and $g = 2$.

   (a) If Alice picks $a = 4$ and Bob picks $b = 7$ then what is the shared secret key that Alice and Bob will share? Express it in binary.

   (b) If Alice picks $a = 7$ and Bob picks $b = 4$ then what is the shared secret key that Alice and Bob will share? Express it in binary.

   (c) The answers to the last two problems are the same. Explain why this is so.

   (d) It turns out that if Alice picks $a = 4$ and Bob picks $b = 7$ then Eve CAN find the shared secret key EASILY (very easily, not just because 29 is so small). Explain why.

   (e) Give some good advice for people using prime p and generator g to avoid this problem pointed out in part d.

4. (25 points) Write down an algorithm that will, given n, find a prime between n and $2n$ by picking numbers at random that are NOT divisible by 2,3, OR 5 and testing them. You can assume we have a quick test for primes.

5. (30 points) Calculate the following using the method shown in class. Show all work.

   (a) The mult inverse of 17 mod 52. (NOTE- since 17 is rel prime to 52, 1 DOES have an inverse mod 52 andthe method in class will find it.)

   (b) The mult inverse of 12 mod 29.

   (c) The mult inverse of 2 mod 13.