HW 7 CMSC 389. DUE Jan 14

1. (10 points) READ my NOTES on line. What is your name? Write it clearly.

2. (10 points) List all of the primes that are between 50 and 100. Note which ones are SAFE primes. (RECALL- a prime p is *safe* if $\frac{p-1}{2}$ is also a prime.)

3. (20 points) Let $p = 59$. Note that p is a safe prime. Find the first three generators of Z_p. Show all work. You may NOT use a calculator. (HINT1: Since p is safe you don't need to do that many calculations of g^a. HINT2: When computing g^a use the repeated squaring technique.)

4. (60 points) Let g be the third generator found in the last problem. Assume that Alice and Bob are going to do Diffie Helman with $p = 59$ and this value of g.

   (a) Assume that Alice's secret random number is 10. What does Alice send Bob? (You may NOT use a calculator and you must show all work. HINT: use repeated squaring.)

   (b) Assume that Bob's secret random number is 8. What does Bob send Alice? (You may NOT use a calculator and you must show all work. HINT: use repeated squaring.)

   (c) Assuming that Alice's secret random number is 10 and Bob's is 8, what is the message they send? Express both as a number in $\{0, 1, \ldots, 58\}$ and also as a number in binary.