Homework 6, MORALLY AND REALLY Due Mar 24

1. (10 points but you have to answer) What is your name? Write it clearly. Staple your HW.

2. (30 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.)

3. (30 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.

4. (30 points)

   (a) Show that if $z^4 \equiv 0 \pmod 7$ then $z \equiv 0 \pmod 7$.

   (b) show that $7^{1/4}$ is irrational.