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.)

   SOLUTION TO PROBLEM 2

   I won't really do this one but I'll say how to do it and start it.

   $p = 59$. So $p - 1 = 58 = 2 \times 29$.

   To test if g is a genreator mod 59 we only need to computer

   $g^2 \pmod{59}$ and $g^{29} \pmod{59}$. If NEITHER is 1 then g IS a generator

   SO, for $g = 2, 3, 4, \ldots$ compute $g^2 \pmod{59}$ and $g^{29} \pmod{59}$. Stop when you find three g's such that neither is 1.

   END OF SOLUTION TO PROBLEM 2.

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.

   SOL TO PROB 3

   I won't really do it I'll just show you HOW to do it. Assume g IS the third generator from the last problem.

   All arithmetic is mod 59.

a) Alice picks random 10. Alice sends g^{10} to Bob.

b) Bob picks random 8. Bob sends g^8 to Alice.

c) Alice KNOWS 10 and KNOWS g^8. She computer $(g^8)^{10} = g^{80}$. Bob KNOWS 8 and KNOWS g^{10}. He computer $(g^{10})^8 = g^{80}$. THIS is there secret shared key.

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.

SOLUTION TO PROBLEM FOUR

ALL $\equiv$ are $\pmod 7$.

a) We prove the CONTRAPOSITIVE: $z \not\equiv 0$ implies $z^4 \not\emptyset$.

Proof by cases.

$z \equiv 1 \Rightarrow z^4 \equiv 1 \not\equiv 0$

$z \equiv 2 \Rightarrow z^4 \equiv 2 \times 2 \times 2 \times 2 \equiv 8 \times 2 \equiv 21 \not\equiv 0$

$z \equiv 3 \Rightarrow z^4 \equiv 3 \times 3 \times 3 \times 3 \equiv 9 \times 9 \equiv 2 \times 2 \equiv 4 \not\equiv 0$

If $z \equiv 4, 5, 6$ then $z \equiv -3, -2, -1$. Since $(-1)^4 \equiv 1$ we get $z^4 \equiv 3^4, 2^4, 1^4$ which we know from the above is $\not\equiv 0$.

b) Assume, by way of contradiction, that $7^{1/4} = \frac{a}{b}$. WHERE a, b HAVE NOT COMMON FACTORS.

$7 = \frac{a^4}{b^4}$

$7b^4 = a^4$

$a^4 \equiv 0$

BY PART A $a \equiv 0$.

$a = 7x$

$7b^4 = a^4 = (7x)^4 = 7^4 x^4$

$b^4 = 7^3 x^4$

$b^4 \equiv 0$

BY PART A $b \equiv 0$.

SO, 7 divides both a, b. This contradicts a, b having no common factors.