Homework 05, MORALLY Due March 10

1. (0 points) What is your name.

GO TO THE NEXT PAGE

2. (40 points)

(a) (0 points) Write a program that will, given p, g, a, b computes the following:

$g^a \pmod p$, $g^b \pmod p$, $g^{ab} \pmod p$

(The intended input is that p is a prime and g is a generator; however, the program still works if this is not the case.) Do not hand anything in.

(b) (20 points) Alice and Bob are carrying out the Diffie-Helman Protocol with $p = 521$ and $g = 3$. Output a table of the following form where you generate the 50 (a, b)'s at random. We give the first 3 rows of what the table might look like. Note that the numbers are fictional and you may have different pairs then we have.

a	b	Alice Sends 3^a	Bob Sends 3^b	Secret 3^{ab}
2	17	33	191	330
33	44	55	200	40
18	344	500	201	47

How often does each secret occur?

(c) (20 points) Alice and Bob are carrying out the Diffie-Helman Protocol with $p = 521$ and $g = 292$. Output a table of the following form where you generate 50 (a, b)'s at random (they can and will be different from the (a, b)'s you used on the problem 2b). We give the first 3 rows of what the table might look like. Note that the numbers are fictional and you may have different pairs then we have.

a	b	Alice Sends 292^a	Bob Sends 292^b	Secret 292^{ab}
7	29	37	391	130
13	14	15	100	10
98	349	509	291	97

How often does each secret occur?

(d) (0 points, do not hand anything in) Does one of the g values seem better than the other? (The answer will be YES) Why is one better than the other?

GO TO NEXT PAGE

3. (30 points)

   (a) (10 points) Prove that $10^{1/3}$ is irrational WITHOUT USING unique factorization.

   (b) (10 points) Prove that $10^{1/3}$ is irrational USING unique factorization. (10 points)

   (c) Prove $101^{1/4}$ is irrational USING unique factorization

   (d) (0 points, don't hand anything in) Would the proof that $101^{1/4}$ have been longer or shorter if you did it WITHOUT USING unique factorization.

GO TO NEXT PAGE

4. (30 points)

   (a) (15 points) Let $\mathbb{D} = \{a + b\sqrt{5} \colon a, b \in \mathbb{Z}\}$. Give an infinite set of numbers in $\mathbb{N}$ that do not have square roots in $\mathbb{N}$ but do have a square root in $\mathbb{D}$. No proof required.

   (b) (15 points) Prove that, for every prime p, $\sqrt{p}$ is irrational. Use Unique Factorization.