Homework 3, Due Thu July 17, 2014

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. (10 points) Test $g = 2, 3, 4, 5, 6, 7, \ldots$ for being generators mod 53 until you find 3 of them. Show your work, and do NOT use a calculator.
3. (20 points) Let g be the third smallest generators mod 53. In this problem we will use this g, and the prime 53, to go through an example of Alice and Bob doing the Diffie Helman Key Exchange. All calculations are mod 53.
   (a) If Alice picks $a = 10$ and Bob picks $b = 14$ then what is the shared secret key that Alice and Bob will share? Express it in binary.
   (b) If Alice picks $a = 14$ and Bob picks $b = 10$ 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.
4. (10 points) Test $g = 2, 3, 4, 5, 6, 7, \ldots$ for being generators mod 23 until you find 5 of them. Show your work, and do NOT use a calculator. Let g be the firth largest generator.
5. (20 points) Using the g from the last problem, and working mod 23, write a table of powers.

   IF it was mod 11 and generator 2 then the table would look like this:

i	2^i
1	$2^1 = 2$
2	$2^2 = 4$
3	$2^3 = 2^2 \cdot 2 = 4 \cdot 2 = 8$
4	$2^4 = 2^3 \cdot 2 = 8 \cdot 2 = 16 = 5$
5	$2^5 = 2^4 \cdot 2 = 5 \cdot 2 = 10$
6	$2^6 = 2^5 \cdot 2 = 10 \cdot 2 = 20 = 9$
7	$2^7 = 2^6 \cdot 2 = 9 \cdot 2 = 18 = 7$
8	$2^8 = 2^7 \cdot 2 = 7 \cdot 2 = 14 = 3$
9	$2^9 = 2^8 \cdot 2 = 3 \cdot 2 = 6$
10	$2^{10} = 2^9 \cdot 2 = 6 \cdot 2 = 12 = 1$

6. (20 points) Using the table of powers, write a table that will help you find discrete logs.

   IF it was mod 11 and generator 2 then the table would be formed by taking the table and inverting it.

i	$\log_2(i)$
1	10
2	1
3	8
4	2
5	4
6	9
7	7
8	3
9	6
10	5

7. (20 points) Alice and Bob are going to use a 1-time pad. When they meet Alice and Bob agree on the key

   00011101010100101000100101010100000011111110101010101010101010

   After that is established Alice and Bob communicate:

   (a) Alice wants to send 0011001. What does she send?

   (b) THEN Bob wants to reply by sending 111100110. What does he send?

   (c) THEN Alice wants to reply by sending 101001001111011.

   (d) Bob wants to send a really long response. What is the LENGTH of the longest message he can send?