Homework 5, Due Mon July 20, 2015

WARNING: THIS HW IS TWO PAGES LONG, SO DO NOT MISS THE SECOND PAGE

1. (20 points) Calculate $3^{123,456}$ (mod 101). (NOTE- You DO NOT need to do 100,000 or even $\log_2(100,000)$ calculations! Use the trick from class!)

2. (20 points) $p = 47$, $g = 2$, Eve wants to solve the discrete log problem. All equations in this problem are mod 47. All of the numbers are made up— I am only interested in following the method.

   (a) Eve wants the discrete log of 10. She finds out that $10^7 \equiv 2^5$. Show how she can use this to find the discrete log of 10. (HINT: You will need to calculate the inverse of 7 mod 46.)

   (b) Eve wants the discrete log of 20. She finds out that $20^7 \equiv 2^5$. Show how she can use this to find the discrete log of 20. (HINT: You will need to calculate the inverse of 7 mod 46. OH, you already know that from the prior problem. Great!)

3. (30 points) Alice and Bob are using Diffie-Helman with $p = 11$ and $g = 2$. Eve wants to use the Baby-Step–Giant-Step algorithm for Discrete Log to intercept messages. Write out the tables that Eve will need to do this. (There are two tables. One of them you need to sort). Use these tables to find the discrete log of 5. Show all work.

4. (30 points) (NOTE- For this problem we GIVE YOU the tables you need.) We use $p = 103$ and generator $g = 20$. We use $m = 11$. Find the discrete log of 50 and of 60. Even though its NOT TRUE you should assume that $(50)^{-1}$ (mod 103) us You may use the FOUR tables on the next two pages. These table are the usual TWO tables PLUS TWO more that will help you later in the algorithm. USE THESE TABLES ONLY. DO NOT USE ANY CALCULATION. Your numbers will NOT be correct but you will still use them since all I care about is knowing the method.

   SHOW all of your work. That is, go through the loop on r and check that the first few r's DO NOT work until you get to one that does, and then you can stop. Be neat!

   In the tables all $\equiv$ are mod 103

$20^0 \equiv 1$

$20^1 \equiv 20$

$20^2 \equiv 91$

$20^3 \equiv 69$

$20^4 \equiv 41$

$20^5 \equiv 99$

$20^6 \equiv 23$

$20^7 \equiv 48$

$20^8 \equiv 33$

$20^9 \equiv 42$

$20^{10} \equiv 16$

$20^{11} \equiv 11$

(THIS IS THE TABLE BUT UNSORTED, SO YOU DON"T REALLY USE THIS ONE. THE NEXT ONE IS THE SAME TABLE SORTED.)

$20^{-1\times 11} \equiv 67$

$20^{-2\times 11} \equiv 68$

$20^{-3\times 11} \equiv 30$

$20^{-4\times 11} \equiv 92$

$20^{-5\times 11} \equiv 83$

$20^{-6\times 11} \equiv 76$

$20^{-7\times 11} \equiv 82$

$20^{-8\times 11} \equiv 18$

$20^{-9\times 11} \equiv 14$

$20^{-11\times 11} \equiv 91$

$20^{-11\times 11} \equiv 25$

TABLE OF $20^{-i \times 11}$ BUT SORTED BY RESULT.

$20^{-9 \times 11} \equiv 14$

$20^{-8 \times 11} \equiv 18$

$20^{-11 \times 11} \equiv 25$

$20^{-3 \times 11} \equiv 30$

$20^{-1 \times 11} \equiv 67$

$20^{-2 \times 11} \equiv 68$

$20^{-6 \times 11} \equiv 76$

$20^{-7 \times 11} \equiv 82$

$20^{-5 \times 11} \equiv 83$

$20^{-11 \times 11} \equiv 91$

$20^{-4 \times 11} \equiv 92$

THERE ARE MORE TABLES ON THE NEXT PAGE WHICH WILL SAVE YOU ALOT OF TIME!!!

$20^1 \times 50^{-1} \equiv 90$

$20^2 \times 50^{-1} \equiv 12$

$20^3 \times 50^{-1} \equiv 32$

$20^4 \times 50^{-1} \equiv 34$

$20^5 \times 50^{-1} \equiv 27$

$20^6 \times 50^{-1} \equiv 43$

$20^7 \times 50^{-1} \equiv 99$

$20^8 \times 50^{-1} \equiv 24$

$20^9 \times 50^{-1} \equiv 14$

$20^{10} \times 50^{-1} \equiv 3$

$20^{11} \times 50^{-1} \equiv 13$

$20^1 \times 60^{-1} \equiv 43$

$20^2 \times 60^{-1} \equiv 18$

$20^3 \times 60^{-1} \equiv 24$

$20^4 \times 60^{-1} \equiv 45$

$20^5 \times 60^{-1} \equiv 46$

$20^6 \times 60^{-1} \equiv 47$

$20^7 \times 60^{-1} \equiv 48$

$20^8 \times 60^{-1} \equiv 49$

$20^9 \times 60^{-1} \equiv 50$

$20^{10} \times 60^{-1} \equiv 4$

$20^{11} \times 60^{-1} \equiv 51$