Homework 6, Due Tue July 21, 2015

WARNING: THIS HW IS FIVE PAGES LONG- THOUGH MOST OF IT IS TABLES.

1. (10 points) Write down TWO things you learned from Dr. Purtilo's lecture.

2. (10 points) The Martian alphabet has 30 letters.

   (a) Martians want to use an affine cipher. That is, they code their letters into the numbers $\{0, \ldots, 29\}$ and want to encode the number x by the number $ax + b \pmod{30}$. List all of the values of a that can be used.

   (b) Martians want to use a general substitution cipher. How many ways can they do that? (You may leave your answer in a form that uses factorials. That is, if you have (say) 10! in your answer you can leave it that way and need not give the actual number.)

3. (15 points) Alice is using a shift cipher that shifts by 4 (SEE THE NOTE IN PART C- THE ALPHABET IS LARGER THAN 26).

   (a) Write the table that Alice uses to ENCODE a message.

   (b) Write the table that Alice uses to DECODE a message.

   (c) How is

   CMSC 198 ROCKS!

   encoded? (NOTE- you have to break the message into groups of five.) (NOTE- The alphabet is now $a, b, c, \ldots, z, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9$ and you can ignore the exclamation point.)

4. (15 points) Alice and Bob are going to use the Diffie-Helman key exchange to obtain a shared secret key. They use $p = 11$ and $g = 2$.

   (a) If Alice picks $a = 8$ and Bob picks $b = 8$ then what is their shared secret key? Write it in binary.

   (b) If Alice picks $a = 7$ and Bob picks $b = 9$ then what is their shared secret key? Write it in binary.

   (c) Give a value of a and b such that Eve can EASILY find out the secret.

5. (15 points) Present a quadratic polynomial which, over mod 15, has at least THREE roots (you must have the square term be nonzero). Also give the roots.

6. (15 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.

7. (20 points) (NOTE- For this problem we GIVE YOU ALL OF 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. 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 for the particular problem we give you. 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.)

$20^{-1\times11} \equiv 67$

$20^{-2\times11} \equiv 68$

$20^{-3\times11} \equiv 30$

$20^{-4\times11} \equiv 92$

$20^{-5\times11} \equiv 83$

$20^{-6\times11} \equiv 76$

$20^{-7\times11} \equiv 82$

$20^{-8\times11} \equiv 18$

$20^{-9\times11} \equiv 14$

$20^{-10\times11} \equiv 91$

$20^{-11\times11} \equiv 25$

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

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

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

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

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

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

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

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

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

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

$20^{-10\times 11} \equiv 91$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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