HW 6 CMSC 389. DUE Jan 11
This is a modified version of the W16 Midterm for CMSC 389

1. This is a closed book exam, though ONE sheet of notes is allowed. **You may NOT use a Calculators**. If you have a question during the exam, please raise your hand.
2. There are 6 problems which add up to 100 points. The exam is 1 hours 30 minutes.
3. In order to be eligible for as much partial credit as possible, show all of your work for each problem, **write legibly**, and **clearly indicate** your answers. Credit **cannot** be given for illegible answers.
4. After the last page there is paper for scratch work.
5. Please write out the following statement: "*I pledge on my honor that I will not give or receive any unauthorized assistance on this examination.*"

6. Fill in the following:

NAME :
SIGNATURE :
SID :

SCORES ON PROBLEMS (FOR OUR USE)

Prob 1:
Prob 2:
Prob 3:
Prob 4:
Prob 5:
Prob 6:
TOTAL

1. (10 points) Alice and Bob are going to use the Diffie-Helman key exchange to obtain a shared secret key. They use $p = 13$ and $g = 2$. (On the next page you will see ALL powers of 2 mod 13. You should use this table.)

   (a) If Alice picks $a = 4$ and Bob picks $b = 8$ then what is their shared secret key?

   (b) If Alice picks $a = 8$ and Bob picks $b = 5$ then what is their shared secret key?

All $\equiv$ on this page are mod 13

$2^0 \equiv 0$

$2^1 \equiv 1.$

$2^2 \equiv 4.$

$2^3 \equiv 8.$

$2^4 \equiv 3.$

$2^5 \equiv 6.$

$2^6 \equiv 12.$

$2^7 \equiv 11.$

$2^8 \equiv 9.$

$2^9 \equiv 5.$

$2^{10} \equiv 10.$

$2^{11} \equiv 7.$

$2^{12} \equiv 1.$

2. (10 points) Alice and Bob use the alphabet

$$\{a, b, c, \ldots, z, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, \$\}.$$

Note that there are 37 symbols, and a is 0, b is 1, c is 2, ..., z is 25, 0 is 26, 1 is 27, ..., 9 is 35, and \$ is 36.

(a) How many affine ciphers are there?

(b) Alice and Bob want to use a 2×2 Matrix Cipher. Give an example of a matrix using entries in $\{0, \ldots, 36\}$ that WORKS.

(c) Alice and Bob want to use a 2×2 Matrix Cipher. Give an example of a matrix using entries in $\{0, \ldots, 36\}$ that DOES NOT WORK.

(d) IF Alice and Bob wanted to use a quadratic cipher

$$f(x) = ax^2 + bx + c$$

then what property would f have to have in order to work?

3. (20 points)
Consider the following variant of the 1-time pad: The alphabet is

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}.$$

The KEY is a random string of elements of the alphabet (for example: $(3, 4, 9, 0)$). Alice and Bob agree on a KEY $b_1, b_2, \ldots, b_N$. Later, if Alice wants to send Bob (m_1, m_2, m_3, m_4) then Alice sends Bob

$$(m_1 + b_1 \bmod 10, m_2 + b_2 \bmod 10, m_3 + b_3 \bmod 10, m_4 + b_4 \bmod 10)$$

(a) Assume the key is $(3, 4, 9, 0)$. If Alice wants to send $(4, 5, 1, 9)$ what does she send?

(b) When Bob gets the message (x_1, x_2, x_3, x_4) how does he decode it?

4. (20 points) Let p be a prime. Let $p-1 = 2qr$ where q and r are primes. Write an efficient (that is, time $O(\log p)$) program that will, on input g,

   - output YES if g IS a generator mod p
   - output NO if g IS NOT a generator mod p

5. (20 points)

   (a) Alice and Bob meet and agree on a 10-bit sequence of bits $b_1 \cdots b_{10}$. They will use the 1-time pad BUT once they get use the first 10 bits they will REUSE THEM! This is a REALLY BAD IDEA. Explain why. Be COHERENT, CLEAR, and CONCISE!!!!!!!!

   (b) Alice and Bob will use Diffie-Helman to share the secret key K, a sequence of bits. They arrange things so that the LENGTH of k is divisible by 4 (this is easy to do). Say $K = K_1K_2K_3K_4$. Then K_1, K_2, K_3, K_4 are sequences of bits. Hence each K_i is a NUMBER in binary. They will then use these four numbers for a, b, c, d for a 2×2 matrix that they will use for a matrix code for messages over the alphabet $\{a, b, c, \ldots, z\}$. Assume that Eve is NOT able to crack 2×2 matrix ciphers. Even so, using Diffie Helman in this way is a REALLY BAD IDEA! Explain why. Be COHERENT, CLEAR, and CONCISE!!!!!!!!

6. (20 points) Alice and Bob are going to use the Autocode. Eve KNOWS they are going to use the Autocode. Describe how Eve can crack the code. Your description should be such that someone who has never seen any of the material in this course (except what the autocode is) can use it. (I may have it graded by such a person.)

   If there is a parameter that you need then describe how you would determine that parameter.

Scratch Paper