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

$2^0 \equiv 0$

$2^1 \equiv 1$.

$2^2 \equiv 4$.

$2^3 \equiv 8$.

$2^4 \equiv 3$.

$2^5 \equiv 6$.

$2^6 \equiv 12$.

$2^7 \equiv 11$.

$2^8 \equiv 9$.

$2^9 \equiv 5$.

$2^{10} \equiv 10$.

$2^{11} \equiv 7$.

$2^{12} \equiv 1$.

SOLUTION TO PROBLEM 1

All $\equiv$ are mod 13.

1) $a = 4$ and $b = 8$ then $(2^4)^8 \equiv 3^8$

We need to compute 3^8.

$3^0 \equiv 1$

$3^1 \equiv 3$

$3^2 \equiv (3^1)^2 \equiv 3^2 \equiv 9.$

$3^4 \equiv (3^2)^2 \equiv 9^2 \equiv (-4)^2 \equiv 16 \equiv 3$

$3^8 \equiv (3^4)^2 \equiv 3^2 \equiv 9$

SO answer is 9.

2) $a = 8$ and $b = 5$ then $(2^8)^5 \equiv 9^5$.

We need to compute 9^5.

$9^0 \equiv 1$

$9^1 \equiv 9$

$9^2 \equiv (9^1)^2 \equiv 9^2 \equiv (-4)^2 \equiv 16 \equiv 3$

$9^4 \equiv (9^2)^2 \equiv 3^2 \equiv 9$

$9^8 \equiv (9^4)^2 \equiv 9^2 \equiv 3$

SO answer is 3.

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?

SOLUTION TO PROBLEM TWO

(a) We need a LIST Of numbers that are rel prime to 37. Thats ALL numbers except 0, so $\{1, 2, 3, \ldots, 36\}$.

So we have 36 choices for a and 37 for b, so thats $36 \times 37 = 1332$.

(b) We need a, b, c, d such that $ad - bc$ is rel prime to 37. Since ALL numbers are rel prime to 37 except 0, just use $a = 1$, $b = 2$, $c = 3$, $d = 4$, so $ad - bc = 4 - 6 = -2 \equiv 35 \pmod{37}$, which is rel prime to 37.

(c) We need to make $ad - bc = 0$ so take $a = b = c = d = 1$ and note that $ad - bc = 1 - 1 = 0$.

(d) We need the function $f(x)$ to be 1-1 and onto.

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?

SOLUTION TO PROBLEM THREE

(a) Alice sends (all mod 10) $(3 + 4, 4 + 5, 9 + 1, 0 + 9) = (7, 9, 0, 9)$.

(b) Bob takes each x_i and computes (all mod 10)

$$x_i - b_i \equiv m_i + b_i - b_i \equiv m_i.$$

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

   SOLUTION TO PROBLEM 4

   (a) Input(g)

   (b) Compute g^2, g^q, g^r, g^{2q}, g^{2r}, g^{qr}.

   (c) If any of the quantities in part (b) are 1 then output NOT A GENERATOR. Otherwise output IS A GENERATOR.

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!!!!!!!!

SOLUTION TO PROBLEM 5

(a) Lets say Alice sends a 10-bit message to Bob. Eve intercepts it but of course cannot decode it. The next day Eve finds out what the message was. THEN Eve can take the REAL MESSAGE and the ENCODED MESSAGE and the XOR of them is the KEY. Now Eve knows the KEY!

(b) When Alice and Bob use Diffie Helman they have NO CONTROL over what the key will be. Hence it is possible that $ad - bc$ is NOT rel prime to 26.

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.

   SOLUTION TO PROBLEM 6

   (NOTE- what is below is CORRECT given the version of autocode I have in the notes. A student pointed out to me that (a) the version I have in the notes is NOT the same as on Wikipedia, and (b) the version I have in the notes is EASILY crackable. I will revise the notes soon. Neither the revised nor the original version of autocode will be on the midterm; however, the ideas below may be.)

   Let $\vec{p}$ be the prob vector of English. We know that $\vec{p} \cdot \vec{p} \sim 0.68$. Let $\vec{q}$ be the prob vector if you use the autocode. We need to know what $\vec{q} \cdot \vec{q}$ is (approx)

   Recall that the autocode relies on ONE number s that we will call *the auto-shift*. To find the parameter do the following

   We omit the code that will, given T and an autoshift s, outputs what happens if you use the Autocode on T with autoshift s. We call that $AUTOCODE(T, s)$.

   (a) Let $T_1, \ldots, T_N$ be a large set of large English Texts.

   (b) For $i = 1$ to N

      i. For $s = 0$ to 25

         A. Let $T_{i,s} = AUTOCODE(T_i, s)$

         B. Compute prob vector $\vec{q}_{i,s}$ for $T_{i,s}$.

         C. $dot_{i,s} = \vec{p} \cdot \vec{q}_{i,s}$.

   (c) We now have $dot_{i,s}$ for $1 \le i \le N$ and $0 \le s \le 25$. Let M be the max of these numbers. Output M as your parameter.

   We will assume that when you have an autocoded text with prob vector $\vec{q}$ then $\vec{q} \cdot \vec{q} \le M + .02$.

It turns out that $M + .02$ is much smaller than 0.68.

NEXT PAGE has more of the solution- we are not done yet.

We need a few more programs to make all of this work.

IS-ENGLISH?:

(a) Input (long) text T (that we assume is an auto-shifted text).

(b) Find $\vec{q}$, the vector of probabilities of letters in T (how to do this with just one pass through T is a Homework Assignment).

(c) Compute $DOT = d(\vec{p}, \vec{q})$. (how to do this easily is a very easy Homework Assignment).

(d) If $DOT \geq 0.66$ then output YES THIS IS ENGLISH. If $DOT \leq M + 0.2$ then output NO THIS IS NOT ENGLISH. If $M + 0.2 < DOT < 0.66$ then output THIS WAS NOT CODED USING AUTOSHIFT!

NOTE- The finding of M and the adjusting of IS-ENGLISH are the only things that really differ from the shift, hence they are graded most heavily.

DECODE-AUTOCODE:

(a) Input (long) text T (that we assume is an autocode coded text).

(b) For $s = 0$ to 25

   i. $T' =$ AUTOCODE(T, s).

   ii. Compute $b =$IS-ENGLISH(T').

   iii. If $b = YES$ then Output(T') and halt.

   iv. If $b =$THIS IS NOT AN AUTOSHIFTED TEXT then output THIS IS NOT A AUTOSHIFTED TEXT and halt.

(c) (If you got to this step then none of the texts were thought to be correct.) Output THIS IS NOT AN AUTOSHIFTED TEXT and halt.

Scratch Paper