CMSC 389 Midterm

1. This is a closed book exam, though ONE sheet of notes is allowed. **You may use a Calculators**. If you have a question during the exam, please raise your hand.
2. There are 5 problems which add up to 100 points. The exam is 2 hours.
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. If you need extra scratch paper **after** you have filled these areas up, please raise your hand.
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 :

You may use the following table throughout which has the convention that A is 0, B is 1, etc.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

You may use the following table of numbers in $\{0, 1, \ldots, 26\}$ that have inverses, and what those inverses are.

NUMBER:	1	3	5	7	9	11	15	17	19	21	23	25
INV MOD 26:	1	9	21	15	3	19	7	23	11	5	17	25

SCORES ON PROBLEMS (FOR OUR USE)

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

1. (20 points) Alice and Bob are going to use a Faux-1-time-pad. They are going to agree on a fraction that is < 1, expand it out in decimal as $0.d_1d_2d_3\ldots$ and then let $b_i = d_i \pmod 2$. Then $b_1b_2\cdots$ will be their key. For example, if the fraction is $1/3 = 0.33333\ldots$. then their key is $1111\ldots$. Another example: if the fraction is $1/4 = 0.2500000\ldots$ then their key is $01000000000\ldots$.

   (a) If Alice and Bob use 1/6 for their fraction then How would they encode 11010101000010101?

   (b) If Alice and Bob use 1/7 for their fraction then How would they encode 11010101000010101?

   (c) Which Faux-1-time-pad is better to use?

   SOLUTION TO 1c

   1/7 is better than 1/6 because the key for 1/7 has a longer period.

   GRADING: If you wrote 'more random' or some such, still full credit. If you wrote just '1/7 is better than 1/6' but not why, that's MINUS 5.

2. (20 points)

   (a) Alice wants to use a linear cipher, that is $f(x) = ax+b \pmod{26}$. Are there any restrictions on what a, b is aside from $a, b \in \{0, \ldots, 25\}$? If so, why do we need that restriction?

   (b) Alice wants to use a 2×2 Matrix cipher, that is, pairs of letters are encoded by

   $$f(x, y) = (ax + by, cx + dy).$$

   Are there any restrictions on what a, b, c, d is aside from $a, b, c, d \in \{0, \ldots, 25\}$? If so, why do we need that restriction?

   (c) Alice wants to use a function $f : \{0, 1 \ldots, 25\} \to \{0, 1, \ldots, 25\}$ for her cipher. Are there any restrictions on what the function f can be aside from $f : \{0, 1 \ldots, 25\} \to \{0, 1, \ldots, 25\}$? If so, why do we need that restriction?

SOLUTION TO 2a

a has to be rel prime to 26. b can be anything. We need this so that the function is invertible.

SOLUTION TO 2b

The matrix has to be invertible. Equivalently, we need that $ac - bd$ is rel prime to 26.

GRADING: Saying that $ac - bd$ is not 0 mod 26 is NOT good enough. Has to be rel prime to 26.

SOLUTION TO 2c

The function f has to be 1-1 and onto so that its invertible.

For ALL of the above you need the function to be invertible so that the code can be decoded unambiguously.

3. (20 points)

   (a) Describe a modification of the VIG cipher where we use a linear cipher instead of a shift cipher. Do a small example. We denote this cipher by VIG-linear.

   (b) Describe a method to find the key length of a VIG-linear cipher that is NOT trying all lengths.

   (c) Describe how to crack the VIG-linear cipher once you know the keylength.

   SOLUTION TO 3a

   The KEY that Alice gives Bob is TWO sequences words of the same length. Take the first word and for every letter which decodes to a number rel prime to 26, keep adding one until you get to a number rel prime to 26. The first word decodes to a sequence of numbers. The second word does also without modification. These give us a sequence of linear functions, with the first word (after modification) providing the a and the second word the b.

   EXAMPLE: First word DOG, second word CAT. DOG is (3,14,6). By adding ones to the 14 and to the 6 until you get to a number NOT rel prime to 26 we end up with (3,15,7). CAT is (2,0,19).

   This codes the sequence of linear functions $(3x + 2, 15x + 0, 7x + 19)$.

   Assume the key is of length L.

   We encode the FIRST letter using the FIRST linear function. We encode the SECOND letter using the SECOND function. ... We encode the Lth letter using the Lth function. We eoncde the $(L + 1)$st letter using the FIRST Function. We eoncde the $(L + 2)$st letter using the SECOND Function. etc.

   Formally if x_i is the ith letter of the plaintext, then we encode x_i using the $(i \bmod L)$-th function.

   For example, using the above we will code DOUG IS AWESOME (OMITTED from this solution, but do yourself).

   GRADING: If your key was NOT 2 sequences of numbers, it was WRONG. If you were UNCLEAR then it was WRONG.

SOLUTION to 3b

OMITTED– but identical to just using normal VIG.

SOLUTION TO 3c:

If the key if of length L then do freq analysis on all letter in positions $\equiv 0 \pmod{L}$, to get that linear function, do freq anal on all letters in positions $\equiv 1 \pmod{L}$, etc and $\equiv L-1 \pmod{L}$.

GRADING: If you just said FREQ ANAL not quite good enough- you have to be clear that its freq analysis on every Lth letter. Some people tried to be fancy and do the $\sum_{i=1} p_i q_{ai+b}$ thing, which is fine. Some people tried to be fancy and do the $\sum_{i=1} p_i q_{i+s}$ thing. This is NOT correct since this just looks for shifts, but we let it slide this time since they had the EVERY LTH LETTER thing right.

4. (20 points) In the problem below you are asked, in three scenarios, if Eve can crack the code in a reasonable amount of time. This is an informal question. We mean using the techniques shown in class. If she CAN then tell us HOW. If she CAN"T tell us what difficulties she would encounter.

   (a) Alice and Bob are using a 2×2 matrix cipher to transmit T, a very long text. Eve intercepts and gets the ciphertext only. Can Eve crack the code in a reasonable amount of time?

   (b) Alice and Bob are using a 100×100 matrix cipher to transmit T, a very long text. Eve intercepts and gets the ciphertext only. Can Eve crack the code in a reasonable amount of time?

   (c) Alice and Bob are using a 100×100 matrix cipher to transmit T, a very long text. Eve intercepts and gets the ciphertext. Eve already has another long ciphertext S and what it decoded to. Can Eve crack the code in a reasonable amount of time?

   SOLUTION TO 4a

   There are only 26^4 matrices to check (actually LESS since we only nee to look at those with det rel prime to 26). Eve can try all of them. By "Trying" we mean look at the freq anal of the decoding and see if it conforms to English (can use the $\sum_{i=1}^{26} p_i q_j$ thing.)

   Also Eve can look at 2-letter Freq analysis.

   SOLUTION TO 4b

   If Eve ONLY has the ciphertext then in order to crack the code (NOTE- this is informal, there may be better ways that we don't know about) she must find the matrix (This isn't quite true- see later in this answer). Hence Eve has to go through all $26^{100 \times 100}$ possible matrices (actually LESS because of det thing, but not much less). This is impossible.

   Actually we can do better, but it won't help much. We can guess the first ROW of the matrix and then look at every 100th letter freq dist. This gets it down to 26^{100}. Still quite large.

   SOLUTION to 4c

Eve sets up a a 100×100 matrix of variables x_{ij}. Apply this to the first 100 chars of S and set it equal to the first 100 chars of S' (what S decoded to). This gives 1 linear equation in 100 variables. Then do the next 100 chars. Etc. You eventually get 100^2 equations in 100^2 variables. This IS solvable using current techniques of Linear Algebra.

5. (20 points)

   (a) Alice wants to use a linear cipher to send messages to Bob. For some reason she wants to send a to p and b to w. CAN she do this? If so then say how she can do this, if not say why she cannot.

   (b) Alice wants to use a linear cipher to send messages to Bob. For some reason she wants to send a to p and c to w. CAN she do this? If so then say how she can do this, if not say why she cannot.

SOLUTION TO 5a

a is 0, p is 15

b is 1, w is 22

We need A and B such that $f(x) = Ax + B$ does this AND A is rel prime to 26.

$f(0) = 15$ so we need $15 = A \times 0 + B$, or $B = 15$.

$f(1) = 22$ so we need $22 = A \times 1 + B$, or $22 = A + 15$, so $A = 7$.

Hence the linear function $f(x) = 7x + 15$ works.

SOLUTION TO 5b

a is 0, p is 15

c is 2, w is 22

We need A and B such that $f(x) = Ax+B$ does this and A is rel prime to 26.

$f(0) = 15$ so we need $15 = A \times 0 + B$, or $B = 15$.

$f(2) = 22$ so we need $22 = A \times 2 + B$, or $22 = 2A + 15$, so $2A = 7$.

This is the KEY POINT: IS there an $A \in \{0, \ldots, 25\}$ rel prime to 26 such that $2A = 7$.

There is NOT since $2A \pmod{26}$ is always EVEN.

GRADING: To say $A = 3.5$ does not make sense since there is no 3.5 in mod 26. Saying "can't solve since 2 has no inverse" is not correct since, for example $2A = 8$ CAN be solved.

PROBLEMS FROM LAST YEARS SECOND MIDTERM THAT ARE RELEVANT TO YOUR FIRST AND ONLY MIDTERM

1. (a) If Alice and Bob use Diffie-Helman with prime p what is the LENGTH of the secret key they will share?

   (b) If Alice and Bob use Diffie-Helman with prime p ROUGHLY how many steps will this take? (Assume that any operation mod p takes $\log p$ steps).

2. 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) Computer all of the following mod 11: $2^0, 2^1, 2^2, 2^3, 2^4$.

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

   (c) If Alice picks $a = 8$ and Bob picks $b = 9$ then what is their shared secret key?