CMSC 389 Midterm, Winter 2018

1. This is a closed book exam, though ONE sheet of notes is allowed. **You CANNOT 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 90 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. (15 points) Alice and Bob use the shift cipher with shift 13.

   (a) Write the coding table (That is tell us how to code $a, b, c, \ldots.$)

   (b) Write the decoding table (That is tell us how to decode $a, b, c, \ldots.$)

   (c) If you've done this problem correctly then the coding and decoding table are the same. Is there any other s for which this is true? Either give such an s or show there is no such s.

SOLUTION TO PROBLEM ONE

a)

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M

b)

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M

c) $s = 13$ is the only one. Coding sends x to $x + s$. Decoding sends x to $x - s$. So we need So if these are the same then

$x - s \equiv x + s \pmod{26}$

$2s \equiv 0 \pmod{26}$.

The only s for which $2s \equiv 0 \pmod{26}$ is $x = 13$.

END OF SOLUTION TO PROBLEM ONE

2. (15 points) Plutonians use alphabet with p symbols where p is a prime. How many affine ciphers are there as a function of p? Explain your reasoning briefly.

SOLUTION TO PROBLEM TWO

The number of numbers that are $\le p$ that are rel prime to p is $p-1$. SO there are $(p-1) \times p = p^2 - p$ affine ciphers.

3. (15 points) Alice and Bob want to use a 2×2 Matrix Cipher with a 7-letter alphabet which is $\{0, 1, 2, 3, 4, 5, 6\}$.

   (a) (5 points) Alice and Bob need to use a matrix that is invertible. Why?

   (b) (5 points) Give an example of a matrix with entries in $\{1, 2, 3, 4, 5, 6\}$ that is invertible mod 7. Explain how you know its invertible (you do not need to invert it).

   (c) (5 points) Give an example of a matrix with entries in $\{1, 2, 3, 4, 5, 6\}$ that is NOT invertible mod 7. Explain how you know its NOT invertible.

SOLUTION TO PROBLEM TWO

a) They need the matrix to be invertible so that message are encoding uniquely and hence can be decoded uniquely.

b) Omitted

c) Omitted

END OF SOLUTION TO PROBLEM TWO

4. (20 points) Alice and Bob have a way to test if a 5th degree polynomial over mod 26 is invertible. They have found that

$$ax^5 + bx^4 + cx^3 + dx^2 + ex + f$$

is invertible iff

$$a + b + c + d + e + f \text{ is a multiple of 3.}$$

(NOTE- this is not true but assume it is for this problem). They want to use a variant of Vigenere where they code a sequence of fifth degree polynomials rather than a sequence of shift ciphers.

(a) Explain what Alice and Bob do. MAKE SURE YOUR ANSWER IS COHERENT, CLEAR, AND SHORT. PRETEND THE GRADER DOES NOT KNOW THE VIG CIPHER

(b) Explain how Eve may crack this cipher. MAKE SURE YOUR ANSWER IS COHERENT, CLEAR, AND SHORT. PRETEND THE GRADER DOES NOT KNOW THE WAY TO CRACK USUAL VIG. PRETEND THE GRADER will take what you say and really code it up.

SOLUTION TO PROBLEM THREE

a) The key word will be a phrase that Alice and Bob chop up into blocks of six. For example

Sina, Alex, and Justin are great TAs ya

becomes

sinaia lexand justin aregre ttasya

Then try to use each of these to code a fifth degree polynomial. Add up the coefficients and if they do not add up to a multiple of 3 then change the last one by adding one or two to it. So you now have a sequence of 5th degree polynomials which we call $f_0, \ldots, f_{L-1}$ ($L = 5$ in the above example).

For all $0 \le a \le L-1$, for all letters in a position that is $\equiv a \pmod{L}$, code the letter by applying f_a.

b) Eve looks for sequences of 5 letters in a row that happen 4 times. Take the difference between them. The keyword length will likely divide all of the differences. Assume that $L_1, \ldots, L_m$ are the candidate key lengths. We say what do do for each one. Only one will work.

Let L be the guess at the keylength. For each $0 \le\le L-1$ look at the letters that are in positions $\equiv a \pmod{L}$ do the following:

For all polynomials of degree 5 f that are invertible do the following:

END OF SOLUTION TO PROBLEM THREE

5. (20 points) For each of the following give BOTH an intelligent argument of why it is TRUE and an intelligent argument of why it is FALSE.

   (a) If Alice and Bob use a 100 × 100 matrix cipher than Eve cannot crack it.

   (b) The Affine Cipher is more secure than the Shift cipher.

   (c) The 1-time pad is an awesome cipher!

   (d) Diffie-Helman is secure.

SOLUTION TO PROBLEM FOUR

(a) If Alice and Bob use a 100 × 100 matrix cipher than Eve cannot crack it.

TRUE: Eve would have to look at all 26^{100} matrices.

FALSE: Eve has access to old messages and what they decode to so she can use that and linear algebra to find the matrix.

(b) The Affine Cipher is more secure than the Shift cipher.

TRUE: There are only 26 options for shift but there are 312 for affine

FALSE: Both are easily cracked.

(c) The 1-time pad is an awesome cipher!

TRUE: Its info-theoretic secure!

FALSE: Its hard to use since you need LOTS of RANDOM bits.

END OF SOLUTION TO PROBLEM FOUR

6. (15 points) Alice and Bob do the Diffie-Helman Key Exchange with $p = 13$ and $g = 2$. Alice picks $a = 3$ and Bob picks $b = 4$.

   (a) What does Alice send Bob?

   (b) What does Bob send Alice?

   (c) What is the shared secret?

SOLUTION TO PROBLEM FOUR

Alice sends $g^a = 2^3 = 8$.

Bob sends $g^b = 2^4 \equiv 3$

They both share $g^{ab} = (g^b)^a = 3^3 \equiv 27 \equiv 1$.

END OF SOLUTION TO PROBLEM FOUR

Scratch Paper