## CMSC 456 Midterm, Fall 2020

1. This is an open-book, open-slides, open-web exam. If you have a question please go to class Zoom site or post to private piazza.
2. There are 5 problems which add up to 100 points. The exam is 120 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 :
UID :

**THERE ARE FIVE PROBLEMS**
**MAKE SURE YOU DO ALL FIVE**

**FOR EACH PROBLEM WE HAVE A BLANK PAGE AFTER IT SO YOU CAN DO THE PROBLEM ON BOTH THE PAGE IT WAS GIVEN ON, AND THE NEXT PAGE IF YOU NEED MORE SPACE.**

**THE LAST PAGE IS BLANK SCRATCH PAPER.**

1. (20 points) Throughout this problem we use the 36-letter alphabet $\{A, \ldots, Z, 0, \ldots, 9\}$. Hence everything is mod 36. You may want to use the tables on the next page. For BOTH PARTS of the problems SHOW YOUR WORK.

   (a) (10 points) Using the Vig cipher with key 7UP, how do you encode MATH4?

   (b) (10 points) If you want to use the affine cipher with $ax + b$, then how many pairs $(a, b)$ work if we DO NOT WANT to just have a shift cipher?

   **THE NEXT PAGE HAS A TABLE YOU WILL NEED FOR THIS PROBLEM**

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $A$ | $B$ | $C$ | $D$ | $E$ | $F$ | $G$ | $H$ | $I$ | $J$ | $K$ | $L$ | $M$ |
| 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 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 |

2. (20 points) Assume the alphabet is $\{0, \ldots, 100\}$ so we are doing everything mod 101.

   Alice and Bob want to use the the $2 \times 2$ matrix cipher.

   (a) (5 points) Give a $2 \times 2$ matrix $A$ with four **distinct non-zero elements** that they CAN use.

   (b) (5 points) Give a $2 \times 2$ matrix $B$ with four **distinct non-zero elements** that they CANNOT use.

   (c) (5 points) Take the matrix $B$ from part b. Use it to code

   ED

   (Use the table from Part 1 for the number-to-letter conversion)

   Present your answer as two letters.

   (d) (5 points) In Part c you used a matrix $B$ that Alice and Bob CANNOT USE to code ED. So Alice CAN code messages! Why should they not use the matrix $B$?

3. (20 points) (You may use this page and the next page for this problem.) Alice and Bob are using the **Vig Cipher with alphabet** $\{0, \ldots, 9\}$. (See HW 3, Problem 4 OR problem 5 on THIS midterm.) Eve learns that the message

   *54321 12345*

   was coded by

   *12389 18141*

   What is the shortest possible key? (Don't just give us the length, give us the key.)

   SHOW YOUR WORK.

4. (20 points) For this problem the $\Sigma$ is an alphabet with $p$ letters in it where $p$ is a prime. Alice and Eve play the following game.

   - Alice flips a coin to get either RP (for Random Perm) or AF (for Affine).
     - If she gets RP then she generates a random perm of $\Sigma$ and sends it to Eve.
     - If she gets AF then she generates a random pair $(a, b)$ such that $ax+b \pmod p$ can be used as an affine cipher, and sends that perm to Eve. (The random Affine cipher CAN just be a shift cipher).
   - Eve looks at the perm she gets and yells out either RP or AF. If she is correct she wins. If not then Alice wins.

   Note that it is the *permutation* that is being transmitted in both cases.

   AND NOW for the problem.

   Assume an Eve with unlimited computational power.

   (a) (5 points) Come up with a strategy for Eve that will win most of the time.

   (b) (15 points) Using your strategy, what is the probability that Eve wins (as a function of $p$)?

5. (20 points) You want to encrypt a sequence of digits 0 through 9 inclusive $x_1, x_2, \ldots x_n$ (this is your plaintext).

   You generate a random key $k_1, k_2, \ldots k_n$, also consisting of digits 0 through 9.

   You generate your ciphertext by adding each individual digit mod 10 to its corresponding key digit:

$$c_i = x_i + k_i \pmod{10}$$

   Include probabilities to support your answers:

   (a) (5 points) Is this cryptosystem info-theoretic secure?

   (b) (5 points) Is it info-theoretic secure if you change the plaintext digits to be 0-8 instead of 0-9 (but still do everything base-10)?

   (c) (5 points) Is it info-theoretic secure if you change the key digits to be 0-8 instead of 0-9 (but still do everything base-10)?

   (d) (5 points) Is it info-theoretic secure if we use 11 digits for the ciphertext so $c_i = x_i + k_i \pmod{11}$ (but still use 10 digits for the plaintext and key?)

   Hint: You may NOT assume that the distribution of letters in plaintext is uniform.

SCRATCH PAPER