Math 314 - Fall 2016 **Name:**

Mission 3 Due September 20, 2016

Cryptography succeeds when its no longer the weakest link.

— Ron Rivest

Guidelines

- All work must be shown for full credit.
- You can choose to use SageMath code to help you solve the problems. If you do, print out your code (or use the same folder as the latex code on SMC).
- Either print out this assignment and write your answers on it, or edit the latex source on SMC and type your answers in the document. Make sure you still show your work! There is one point of extra credit available on this assignment if you use LaTeX.
- You may work with classmates, but be sure to turn in your own written solutions. Write down the name(s) of anyone who helps you.
- Check one:
  □ I worked with the following classmate(s): ____________________
  □ I did not receive any help on this assignment.

1. Graded Problems

1. Let a, b, c, d, e, f be integers mod 26. Consider the following comination of the Hill and affine ciphers: represent a block of plaintext as a pair (x, y) mod 26. The corresponding cipher text is

$$(x\ y)\begin{pmatrix} a & b \\ c & d \end{pmatrix} + (e\ f) \equiv (u\ v) \pmod{26}.$$

Describe how to carry out a chosen plaintext attack on this system (with the goal of finding the key a, b, c, d, e, f) You should state explicitly what plaintexts you chose and how to recover the key.

2. Suppose a system has 2 possible messages, “Yes” and “No.” “Yes” gets sent 60% of the time, “No” 40% of the time. There are 4 Keys, which encrypt the message as follows:

key	“Yes”	“No”
k_1	a	b
k_2	b	a
k_3	c	a
k_4	c	b

Bob chooses a key at random and sends a message using it to Alice. Eve intercepts the message and finds that it is ”a”. What is the probability that the message she was trying to send was ”No”? Does this system have perfect secrecy? Why or why not?

3. Use the Euclidean algorithm to find integers x and y such that $19x + 79y = 1$. What is $19^{-1} \pmod{79}$? Show all of your steps!

2. Recommended Exercises

These will not be graded but are recommended if you need more practice.

- Section 2.13: # 15, 23
- Section 3.13: # 1