Math 314 - Fall 2019 **Name:**

Mission 1 Due September 9, 2019

I must study politics and war that my sons may have liberty to study mathematics and philosophy.

—John Adams

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 and attach it with the assignment.
- Either print out this assignment and write your answers on it, or edit the latex source and type your answers in the document. Make sure you still show your work!
- 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. Encrypt `letters` using the affine function $15x + 3 \pmod{26}$. What is the decryption function? Check that it works.

2. Consider an affine cipher (mod 26). You do a chosen plaintext attack using `hahaha`. The ciphertext is `NONONO`. Determine the encryption function.

3. This problem involves the Dancing Men code from a Sherlock Holmes story.
   a. Read Section 2.5 (Sherlock Holmes), and describe (in a paragraph) how Sherlock figures out which dancing man represents the letter `e` as well as the letter `r`.

   b. Explain in one sentence what the little flags mean.

4. (T&W 2.14 # 6) Suppose you encrypt using an affine cipher $E_1(x) = \alpha_1 x + \beta_1$, then encrypt the encryption using a second affine cipher $E_2(x) = \alpha_2 x + \beta_2$ (both are working mod 26). What is the resulting (combined) double encryption Is there any advantage to doing this rather than using a single affine cipher? Why or why not?

5. Decrypt the ciphertext `DRLUKDOSGDASACAOF`, which was encrypted with a Vigenère cipher using the key `CRAB`.

2. Recommended Exercises

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

- Section 2.13: # 1, 5, 7