Math 314 - Spring 2020 **Name:**
Mission 1 Due February 4, 2018

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 `itishere` using the affine function $3x + 12 \pmod{26}$. What is the decryption function? Check that it works.

2. You learn that the plaintext `math` encrypts to `AEPT` using an affine cipher. Find the key being used.

3. Using the definitions of ”divides” and ”congruence” prove the following: If $a \equiv b \pmod{n}$, and $m|n$, then $a \equiv b \pmod{m}$.

4. (T&W 2.14 # 6) Suppose you encrypt using an affine cipher, then encrypt the encryption using another affine cipher (both are working $\bmod 26$). Is there any advantage to doing this rather than using a single affine cipher? Why or why not?

2. Recommended Exercises

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

- Section 2.13: # 1, 2, 4, 7