Math 314 - Fall 2016 **Name:**

Mission 4   Due September 27, 2016

It used to be expensive to make things public and cheap to make them private. Now its expensive to make things private and cheap to make them public.

— Clay Shirky

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. Use modular exponentiation to compute 5^{268} (mod 23). Make sure to show your steps.

2. Compute 8^{20} (mod 21). Does this contradict Fermat's Little Theorem? Why or why not?

3. Suppose you write a message as a number m (mod 17). You encrypt the message using the encryption function $E(x) = x^{11}$ (mod 17). What function could you use as the decryption function? (Hint: Decryption is done by raising the ciphertext to a power mod 17. Fermat's Little Theorem will be useful.)

2. Recommended Exercises

These will not be graded.

- Section 3.13: # 9, 11