Math 314 - Fall 2016 **Name:**
Mission 3 Due September 28, 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.
- 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. 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?

2. 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!

3. Use modular exponentiation to compute $5^{268} \pmod{23}$. Make sure to show your steps.

4. Compute $8^{20} \pmod{21}$. Does this contradict Fermat's Little Theorem? Why or why not?

5. Suppose you write a message as a number $m \pmod{17}$. You encrypt the message using the encryption function $E(x) = x^{11} \pmod{17}$. 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 but are recommended if you need more practice.

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