Math 314 - Fall 2018 **Name:**

Mission 3 Due September 24, 2018

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. Use the Euclidean Algorithm to find the gcd of 217 and 1078.

2. Use the Euclidean algorithm to find integers x and y such that $23x + 77y = 1$. What is $23^{-1} \pmod{77}$? Show all of your steps!

3. Use modular exponentiation to compute $5^{268} \pmod{17}$. Make sure to show your steps.

4. Alice wants to send a message to Bob using the 3-pass protocol. She decides to use the prime $p = 43$, and picks her key, $a = 11$. Bob picks his key, $b = 13$.
   (a) What are Alice and Bob's decryption keys? Work them out using the Euclidean algorithm.

   (b) Alice wants to send the message m=3. Find the values of each of the messages that Alice and Bob send back and forth. Does Bob recover Alice's plaintext at the end?