Math 314 - Fall 2016 **Name:**

Mission 7 Due October 25, 2016

As an inventor of one of the algorithms, I feel like the mother whose son has been brainwashed and is off to become a jihadist in Syria.

— 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 (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. Here we will show that RSA still works (Bob can still decrypt Alice's message) even if the message m has $\text{GCD}(m, n) \neq 1$. Suppose we have the usual setup, Bob's public key is $n = pq$, with encryption exponent e, and decryption exponent d, with $de \equiv 1 \pmod{\varphi(n)}$.

   Suppose that Alice wants to send a message m where $\text{GCD}(m, n) \neq 1$. She doesn't know this (since she doesn't know how to factor n) so she computes $c = m^e$ and sends this to Bob. Bob computes $c^d = m^{ed}$. We want to see that he still successfully recovers m.

   (a) What are the possible values of $\text{GCD}(m, n)$ if it isn't 1?

   (b) Let $z = m^{ed} - m$. For each of the cases you found in part a show that both $z \equiv 0 \pmod{p}$ and $z \equiv 0 \pmod{q}$.

(c) Explain how the Chinese remainder theorem can be used now to show, using part b, that $z \equiv 0 \pmod{n}$, and thus that $c^d = m^{ed} \equiv m \pmod{n}$.

2. Exercise 6.8.1.

2. Recommended Exercises

These will not be graded.

- Section 6.8.: # 3, 8