Math 314 - Fall 2016 **Name:**

Mission 7 Due October 25, 2016

In some ways, cryptography is like pharmaceuticals. Its integrity may be absolutely crucial. Bad penicillin looks the same as good penicillin. You can tell if you spread sheet is wrong, but how do you tell if your cryptography package is weak? The ciphertext produced by a weak encryption algorithm looks as good as ciphertext produced by a strong encryption algorithm. Theres a lot of snake oil out there. A lot of quack cures. Unlike the patent medicine hucksters of old, these sofwtare implementors usually dont even know their stuff is snake oil. They may be good software engineers, but they usually havent even read any of the academic literature in cryptography. But they think they can write good cryptographic software. And why not? After all, it seems intuitively easy to do so. And their software seems to work ok.

— Philip Zimmermann

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. Using the handout (posted to sagemath) on Differential cryptanalysis, peform the steps we did in class on a random key. (First execute the random key line, then use the tools below to figure out what k_3 is without looking at K.)

   You must clearly write down all of your steps and explain what you are doing. Include each of your choices of plaintext, what the resulting values of each of the relevant components are, and how that allowed you to narrow down the possible choices for the key.

2. Exercise 4.9.6.

2. Recommended Exercises

These will not be graded.

- Section 4.9: # 7, 15