Math 314 - Fall 2016   **Name:**

Mission 10   Due December 8th, 2016

The driving force behind modern computer ciphers isnt security, but efficiency. The question is not can you create a secure cipher. You can. The question is whether you can create one that will work efficiently on huge data sets, or on very limited hardware.

— Jeff Dege.

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): _____
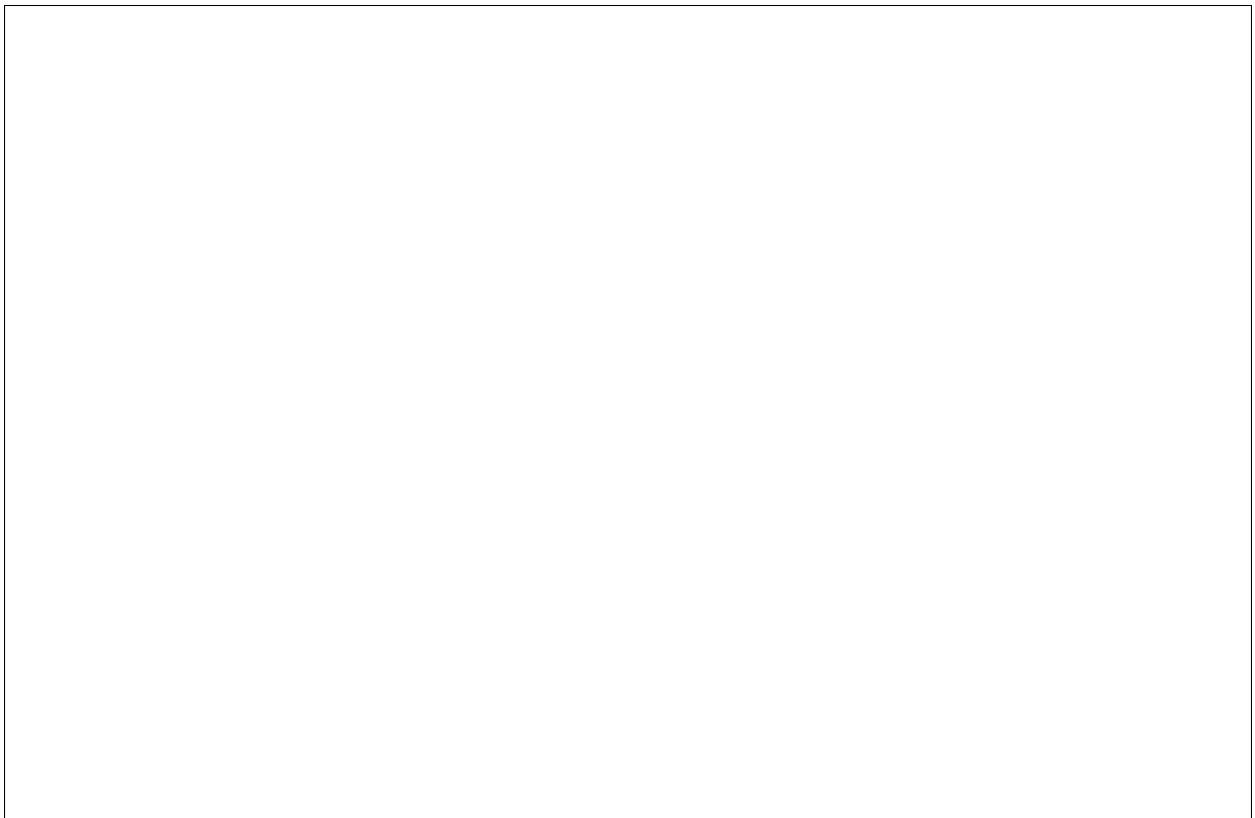 ☐ I did not receive any help on this assignment.

1. GRADED PROBLEMS

1. Describe how Eve could perform a Man-in-the-middle attack against the three-pass-protocol. (Page 83)

2. Let p be a large prime, and α a primitive root $\pmod{p}$. Let $h(x) \equiv \alpha^x \pmod{p}$. Why is $h(x)$ not a good cryptographic hash function?

3. Exercise 9.6.3

4. Exercise 9.6.5