Math 314 - Fall 2018   **Name:**

Mission 8   Due Nov 6th, 2019

Lots of people working in cryptography have no deep concern with real application issues. They are trying to discover things clever enough to write papers about.

— Whitfield Diffie

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. The ciphertext 2943 was obtained from the RSA algorithm using $n = 11413$ and $e = 7467$. Using the factorization $11413 = 101 \times 113$ find the plaintext. (Use Sage or a calculator to do the computations...)

2. In order to increase security in RSA, Bob chooses $n = pq$ and two encryption exponents, e_1 and e_2. He asks Alice to encrypt her message m to him by first computing $c_1 \equiv m_1^e$ (mod n), and then computing $c_2 \equiv c_1^{e_2}$ (mod n). Alice then sends c_2 to Bob. Does this double encryption increase the security over single excryption? What if Bob used *triple* encryption instead? Explain why or why not.

3. Problem 6.8.13 from the book (Also, do the calculation, use sage or a calculator.).

2. RECOMMENDED PROBLEMS

The following problems are recommended for extra practice: 6.8.2, 6.8.12, 6.8.20.