Math 314 - Spring 2020 **Name:**

Mission 7 Due April 20th, 2020

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. To decrypt the mix columns step in SAES it is necessary to multiply by the inverse of the encryption matrix, $E = \begin{bmatrix} 1 & x^2 \\ x^2 & 1 \end{bmatrix}$ over the finite field $\mathbb{F}_{16}$ with irreducible polynomial $x^4 + x + 1$. Compute the decryption matrix $D = E^{-1}$.

2. The ciphertext 2943 was obtained from the RSA algorithm using $n = 11413$ and $e = 1987$. Using the factorization $11413 = 101 \times 113$ find the plaintext.

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

4. Test whether 65 is prime using the Solovay Strassen test with the bases $a = 14$ and $a = 15$.

5. Test whether 85 is prime using the Miller Rabin test with the bases $a = 13$ and $a = 16$.