Math 314 - Spring 2018 **Name:**

Mission 8 Due April 18th, 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 $n = 11639$ and $e = 257$. Using the factorization $11639 = 103 \times 113$ find the plaintext.

2. 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 $c_1 \equiv m_1^e \pmod{n}$, and then $c_2 \equiv c_1^{e_2} \pmod{n}$. 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. Read section 6.5 and give a brief summary of it. What is a squeamish ossifrage, and what does it have to do with cryptography?

4. Alice Bob and Carlie are each using RSA, but they are lazy and decide to share the work of generating prime numbers. They find 3 large primes p,q and r, then Alice uses the modulus $n_A = pq$, Bob uses the modulus $n_B = pr$ and Carlie uses the modulus $n_C = qr$. The prime numbers used are much too large for factoring to be feasible, but Eve learns that they shared prime numbers (and knows their public keys) how does she obtain p, q and r?

5. Problem 6.8.17 from the book.

2. Recommended Exercises

These will not be graded but are recommended if you need more practice.

- Section 6.8: # 2, 3, 10