Math 314 - Spring 2019 **Name:**
Mission 9 Due April 25th, 2019

Few false ideas have more firmly gripped the minds of so many intelligent men than the one that, if they just tried, they could invent a cipher that no one could break.

— David Kahn

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. You want to factor $n = 667$ and you learn that $52^2 \equiv 36 \pmod{667}$. Use this information to factor 667.

2. Test $n = 85$ for primality using the Solovay-Strassen Primality test using first the base $a = 13$, and then the base $a = 5$. Compute the Jacobi symbols by hand but you can use sage to do the exponentiation.

3. 6.8.13 (Describe the steps, then use SAGE to do the numerical calculations.)

4. With $p = 13$ and $\alpha = 2$, suppose Alice chooses the secret value $x = 5$ and Bob chooses $y = 11$. Show and explain all of the steps of the Diffie-Hellman Key exchange. What value do they agree on for their key?

2. Recommended Exercises

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

- Section 6.8: # 1, 4, 22