Math 314 - Spring 2020 **Name:**

Mission 9 Due May 12th, 2020

A signature always reveals a man's character - and sometimes even his name.

— Evan Esar

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. Alice sets up an RSA key with the primes $p = 31$ and $q = 43$ and exponent $e = 13$. Determine what her signature on the message $m = 100$ would be. (Use a calculator/cocalc to do the exponentiation, but explain your steps!) Verify that the signature is valid.

2. Alice sets up an DSA key with the primes $p = 67$, $q = 11$, and the primitive root $g = 2$. Suppose she picks the secret number $a = 5$. Determine the rest of her public key, and sign the message $m = 17$ (supposing she picks $k = 3$. Verify that the signature is valid.

3. Use the discrete log hash with $p = 53$, $q = 107$, $\alpha = 82$, $\beta = 2$, $h(a_1 p + a_0) \equiv \alpha^{a_0}\beta^{a_1} \pmod{q}$. You find the collision $h(2312) = h(662)$. (Here $2312 = (43) \times 53 + 33$, $662 = (12) \times 53 + 26$.) Use this information to solve the discrete log problem $\alpha \equiv \beta^x \pmod{107}$.