Math 314 - Fall 2019 **Name:**

Mission 9 Due November 13th, 2018

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. Alice Bob and Carl are generating public keys for RSA, but they are lazy and decide to share some of the work of generating prime numbers. They find 3 large prime numbers p,q and r, then Alice uses the modulus $n_A = pq$, Bob uses the modulus $n_B = pr$ and Carl uses the modulus $n_C = qr$. The prime numbers used are much to large 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?

2. With $p = 101$ and $x = 27$, suppose Alice chooses the secret value $a = 53$ and Bob chooses $b = 12$. Show and explain all of the steps (but use a calculator/sage to do the exponentiations) of the Diffie-Hellman Key exchange. What value do they agree on for their key?

3. Now Alice and Bob decide to use El Gamal. With $p = 101$ and $\alpha = 27$, suppose Alice chooses the secret value $k = 13$. What is her public key? Bob wants to send her the message $m = 50$, and chooses the ephemeral key $b = 72$. What is his ciphertext?

4. Use the steps of Baby-Step-Giant-Step to solve the equation

$$5^x \equiv 20 \pmod{47}$$

for the value of x. Use a calculator/Sage to do the computations, but make sure to show your tables.

2. Recommeneded Problems

The following problems are recommended, but won't be collected: 7.6.10, 7.6.11