Math 314 - Spring 2018 Mission 9

Name:

Due April 30th/May 1st, 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.

• \underline{Check} one:

- \square I worked with the following classmate(s): _____
- I did not receive any help on this assignment.

1. Graded Problems

1. 6.8.13 (Describe the steps, then use SAGE to do the numerical calculations.)

2. 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?

3. Exercise 6.8.20

4. With p = 11 and $\alpha = 2$, suppose Alice chooses the secret value x = 5 and Bob chooses y = 12. Show and explain all of the steps of the Diffie-Hellman Key exchange. What value do they agree on for their key?