Math 314 - Spring 2020 **Name:**

Mission 8 Due April 27th 2020

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 CoCalc to help you solve the problems. If you do, include the code you used.
- 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. Use Dixon's algorithm to factor 943. Use $B = 12$ and the "a" values $a = 31, 35, 39, 44, 51, 57, 62, 74, 83, 88$ (Note not all of the values will work). Describe the steps, then use CoCalc to do the numerical calculations.

2. Alice is generating keys for RSA, and wants to create two different public keys (n_1, e_1) and (n_2, e_2). She is feeling lazy however and and decides to reuse one of the large prime numbers that she finds in both moduli, so she only finds three prime numbers p, q and r and then generates $n_1 = pq$, and $n_2 = pr$. The numbers used are much to large to factor, but Eve knows that Alice is lazy. How does she obtain p, q and r (assuming she knows n_1 and n_2)?

3. Alice and Bob use Diffie-Hellman to generate a key. Alice picks the prime 13, with the primitive root $r = 2$. If Alice picks the secret number $a = 4$ and Bob picks $b = 5$, what key do they agree on?

4. Use Baby-Step Giant-Step to solve the discrete log problem:

$$5^x \equiv 35 \pmod{47}.$$

Write down the tables of Baby-Steps and Giant steps and then use those tables to find the answer.