MATH/CSCI 408 Name: ______________________________

CRYPTOGRAPHY MISSION 01 DOSSIER

Deadline: Thursday, 24 August 2017 at 10:50am

This mission covers the syllabus, setting up CoCalc, and your first shift cipher.

Check one:

□ I received help from the following classmate(s) on this assignment:

____.

□ I did not receive any help on this assignment.

Homework Rules

- All work must be shown for full credit!
- 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.
- You can choose to use CoCalc code to help you solve the problems. If you use code, please email the code by the deadline with subject line: "Math 408 Mission 01"

1. Graded Problems

1. Read the syllabus in detail. Draw a picture of your favorite animal with a magnifying glass once you're done:

2. Do the FA17 Cryptography Intro Survey in your inbox. I will get a notification when you're done, so no need to email me.

3. This problem will help you set up a CoCalc account (`https://cocalc.com/`)–this was formerly known as SageMath or Sage, so some of the names haven't changed yet. Go to the website, and create a username and password.

   a. Create a new project (Cryptography). You can use this project folder to hold all of your CoCalc code.

b. You can use CoCalc to do basic math, assign things (like numbers) to variables, utilize inbuilt functions, create lists, etc. Documentation is often helpful for programming. Bookmark this page: `http://doc.sagemath.org/html/en/tutorial/index.html`. If you are familiar with Python, you might notice that CoCalc/SageMath is Python-based and has some similarities. One particularly useful documentation page for us is the one on Classical Cryptosystems: `http://doc.sagemath.org/html/en/reference/cryptography/sage/crypto/classical.html`.

c. In your CoCalc project, create a Sage worksheet (.sagews named) "Mission01." Read the section on shift cipher. In "Mission01," follow the documentation and write a short block of code which encrypts the message, "The name is Bond, James Bond" with a shift of $k = 8$. Note that punctuation is ignored. Write the ciphertext here:

2. Recommended Exercises

If you aren't familiar with programming at all, go through the "Programming Basics" code (`https://tinyurl.com/ho-crypto-programmming-basics`). You can copy the public file over to your own CoCalc project, and run the code. In general, I will post .sagews files on Moodle too.