MATH/CSCI 408 Name: _____

CRYPTOGRAPHY MISSION 01 DOSSIER

Deadline: Thursday, 1 September 2016 at 3:05pm
This mission covers Sections 2.1, 2.2, and 2.3.

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 SageMath code to help you solve the problems. If you use code, please send the code to Dr. Ho.

1. Graded Problems

1. Do the following survey: `http://tinyurl.com/16AnneHoSurvey`

2. (T&W 2.13 # 4) Consider an affine cipher (mod26). You do a chosen plaintext attack using `hahaha`. The ciphertext is `NONONO`. Determine the encryption function.

3. This problem involves the Dancing Men code from a Sherlock Holmes story.

(Image from `http://www.cultbox.co.uk/reviews/episodes/sherlock-2016-special-review-the-abominable-bride`.)

a. Read Section 2.5 (Sherlock Holmes), and describe (in a paragraph) how Sherlock figures out which dancing man represents the letter `e` as well as the letter `r`.

b. Explain in one sentence what the little flags mean.

c. Draw the dancing men figures that would correspond to the plaintext: `math`.

4. (T&W 2.14 # 2) The following ciphertext was the output of a shift cipher:

   `LCLLEWLJAZLNNZMVYIYLHRMHZA`

   By performing a frequency count, guess the key used in the cipher. What is the decrypted plaintext?

5. SageMathCloud:

   a. Set up a SageMathCloud account (`https://cloud.sagemath.com`). Create a new project (Cryptography). You can use this project folder to hold all of your SageMath code.

   b. From Moodle (`https://moodle.coastal.edu/`), download Dr. Ho's Vigenere cipher code (Vigenere Cipher.sagews) and upload it to your SageMathCloud project folder.

   c. Run through the cells of code, and then encode the phrase, "Hey, Mr. Tambourine Man, play a song for me" by using the key word "DYLAN". Write down the ciphertext. Be sure to print your code or email it to Dr. Ho too.

2. Recommended Exercises

These will not be graded but are recommended if you need more practice.

- Section 2.13: # 1, 3, 7, 11
- Section 2.14: # 1, 6