MATH/CSCI 408 Name: _____

CRYPTOGRAPHY MISSION 02 DOSSIER

Deadline: Thursday, 31 August 2017 at 10:50am
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.

1. Graded Problems

1. (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.

2. 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`.

3. (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?

4. Read the Wikipedia article on the Pigpen cipher:
`https://en.wikipedia.org/wiki/Pigpen_cipher`.
a. Replicate the set of all graphical symbols on your homework here:

b. Encrypt the message "you only live twice" using the Pigpen cipher.

2. Honors Section Problem

(T&W 2.13 # 6) Suppose you encrypt using an affine cipher, then encrypt the encryption using another affine cipher (both are working $\bmod 26$). Is there any advantage to doing this, rather than using a single affine cipher? Why or why not?

3. Recommended Exercises

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

- Section 2.13: # 1, 3, 5, 7
- Section 2.14: # 1, 3, 5