MATH/CSCI 408 Name: ______________________________

CRYPTOGRAPHY MISSION 03 DOSSIER

Deadline: Thursday, 7 September 2017 at 10:05am
This mission covers Sections 2.3, 2.4, and 2.6.

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. (Vigenère cipher) Suppose there is a language that has only the letters a, b, and c. The frequency of the letter a is .1, the frequency of b is .3, and the frequency of c is .6. A message is encrypted using a Vigenère cipher (working mod3 instead of mod26). Suppose you are given the ciphertext `CBBBCACACB`.
   a. Make a Vigenère cipher table using only a, b, and c.

   b. Write out the three vectors $\vec{A_0}$ (corresponding to the frequencies of the letters with no shifts), $\vec{A_1}$ (correponding to the frequencies of the letters with one shift, starting with the frequency of "c"), and $\vec{A_2}$ (correponding to the frequencies of the letters with two shifts, starting with the frequency of "b").

c. Suppose you know that the key length is 2. The next three parts will walk you through the steps to find the first letter of the key word. First, circle every 1st, 3rd, 5th, etc. letter. You should have a total of 5 letters circled. Count the number of occurrences of a, b, and c out of those five.

d. Write a vector $\vec{W}$ of the frequencies of each of those letters from part c.

e. Compute the dot products $\vec{W} \cdot \vec{A}_0, \vec{W} \cdot \vec{A}_1$, and $\vec{W} \cdot \vec{A}_2$. Which one of these is the highest number (which corresponds to the probability)? Based on this, which letter is probably the first letter of the key word?

2. We're going to practice using some built-in functions for SageMath in this problem because you don't need to code everything from scratch!

a. Go to `http://doc.sagemath.org/html/en/reference/cryptography/sage/crypto/classical.html`. Read through the documentation of the TranspositionCipher. In a sentence or two, describe what the Transposition Cipher does to a plaintext phrase:

b. Use some SageMath code and the Transposition Cipher to encrypt: "`BABOUTHEOCELOT`" (note that normally, we use lowercase for plaintext, but we need all caps for this particular line of code).

c. There is also a built-in Vigenère cipher. An example of how to decipher is as follows:

```
alphabet = AlphabeticStrings() #Alphabet
ciphertext = alphabet.encoding("DILCSALPKIJGSTBP")  #Input ciphertext
system = VigenereCryptosystem(alphabet,5)  #Vigenere with length 5 key
key = alphabet("HELLO") #Input key
plaintext = system.deciphering(key, ciphertext)  #Decipher message
print plaintext #Display output
```

Run this code (you can download and copy it from the .sagews document on Moodle). Write down the plaintext here:

d. Modify the Vigenère cipher code to decrypt the following message:

```
XKMVYLFXGFEEDKBAFMVPXMARWGHDPGBAJXEIDQPUEXXFMCEEUTIJLZAULMSG
CIVYWAMDEPRKNBPKSIGSWGHFWQIKKTJKPZGNWFXYPOBUVBWFQBVTLXVIPLJO
LAXYPQEHGGIJDWYKLBXSPEVZZVEVDIE
```

with key word “STERLING” (also see the .sagews document on Moodle to copy this ciphertext). Email me your code with the plaintext.

3. Encrypt the plaintext “`It was Greek to me`” using the Playfair cipher with key word “SHAKESPEARE.”

5. (Honors) The way that we found the key length in the Vigenère cipher is using the Kasiski analysis method. Work through the example on this page: `http://crypto.interactive-maths.com/kasiski-analysis-breaking-the-code.html`.

   a. Write down what the keyword is here:

   b. In a sentence or two, write something new that you learned from working through the details of the Kasiski analysis example.

2. Recommended Exercises

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

- Section 2.13: # 10, 11
- Section 2.14: # 7, 9