MATH/CSCI 408 Name: _____

CRYPTOGRAPHY PRIORITY MISSION 01

Deadline: Thursday, 29 September 2016 at 11:59pm

1. Rules for Take-Home Exam

1. You may use the following resources:
   - Anne
   - your notes
   - the textbook
   - handouts from class
   - SageMath code and any SageMath or Python documentation
   - solutions to previous missions
2. You may NOT use the following:
   - Internet solutions
   - classmates
   - other professors
   - any other source that isn't listed above
3. You may submit solutions electronically or by paper.
4. Be sure to show all work, and provide all code.
5. **Choose 5 out of the 6 problems**, and clearly denote which one is not going to be graded. Each problem is worth 20 points for a total of 100 points.

2. Problems

1. (Affine cipher) The following ciphertext used the affine cipher $x \mapsto 9x + 13$:
   `NRXOHLROKVRNKCHAHIXRJASXXITYNZXAAJCTCHKKXO`.
   Decrypt it.

2. (Affine cipher) Suppose you encrypt using an affine cipher, then encrypt the encryption using another affine cipher (both are working mod26). Is there any advantage to doing this? Why or why not? Explain in a paragraph, and give a specific, detailed example.

3. (Hill Cipher) Barry captures Archer's Hill cipher machine, which uses a 2×2 matrix M mod 26. He realizes that the plaintext `ba` encrypts to `HC`, and the plaintext `zz` encrypts to `GT`. What is the matrix M?

4. (Hill Cipher) Suppose you are given the following ciphertext:
   `ESIZEHAXPDILHJDTBQEHSJZXXHQFIBKZJYWUQWEDKDEUDMHJTWPVQLEHHMMFKBMUZXEUZTESIZYL`
   Given the encryption matrix:
   $$\begin{pmatrix} 1 & 5 \\ 2 & 3 \end{pmatrix}$$
   Decrypt the message.

5. (Proof) Write a proof for the following statements:

   a. Let a, b, n be integers. If $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$, then $\gcd(ab, n) = 1$.

   b. Let a, b, c, and n be integers with $n > 0$. If $a \equiv b \mod n$ and $b \equiv c \mod n$, then $a \equiv c \mod n$.

6. (SageMath) We are using a new alphabet $\{A, B, C, D, E, F, G\}$ (perhaps corresponding to musical notes). Associate the letters with the numbers $\{0, 1, 2, 3, 4, 5, 6\}$, respectively.

   a. Using the shift cipher with a shift of 5, encrypt the following sequence of notes for Twinkle Twinkle Little Star: `ccggaagffeeddcggffeedggffeedccggaagffeeddc`.

   b. Write a program that performs affine ciphers on the musical alphabet. Provide the code as well as an example of output.