MATH 587/CSCE 557: HOMEWORK 2, DUE FEB 1.

1. Suppose you encrypt using an affine cipher, then encrypt the encryption using another affine cipher. Is there any advantage to doing this, rather than using a single affine cipher? Why or why not? [Hint: if e.g. $f(x) = 3x + 1$ and $g(x) = 5x + 2$, what does $f(g(x))$ look like?]

2. The ciphertext CRWWZ was encrypted by an affine cipher. We know the plaintext starts HA. Decrypt the message.

3. Using MAMA as the key for a Vigenere cipher, encrypt BE COOL. What's the true length of this polyalphabetic cipher?

4. The ciphertext YIFZMA was encrypted by a Hill cipher with matrix

$$\begin{pmatrix} 9 & 13 \\ 2 & 3 \end{pmatrix}$$

- find the plaintext.