HOMEWORK 2, DUE FEB 13.

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

2. Using MAMA as the key for a Vigenere cipher, encrypt BE COOL. What's the minimum block-length of this polyalphabetic cipher?

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

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

- find the plaintext.

4. The following ciphertext was the output of a shift cipher:
LCLLEWLJAZLNNZMVYIYLHRMHZA
By performing a frequency count, guess the key used in the cipher (for full credit explain what you're doing). What is the plaintext?

5. (From Wikipedia) Unicity distance is a term used in cryptography referring to the length of an original ciphertext needed to break the cipher by reducing the number of possible spurious keys to zero in a brute force attack. That is, after trying every possible key, there should be just one decipherment that makes sense.

Let's investigate this for a ciphertext-only attack on a shift cipher. Considering the ciphertext ALIIP and its possible plaintexts, what does this say about the unicity distance? Texts claim that the unicity distance of a shift cipher is about 1.3. Reconcile this with your last answer.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX