HOMEWORK 2, DUE SEP 21.

Be sure to include brief explanations. You will not get full credit if you give only the final answer.

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) In cryptography, unicity distance is 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, i.e. expected amount of ciphertext needed to determine the key completely, assuming the underlying message has redundancy.

Critique this definition for ciphertext-only attacks on shift ciphers. In particular, consider the ciphertext ALIIP and its possible plaintexts. Does this imply anything about the unicity distance for shift ciphers? Note that the formula in textbooks gives that the unicity distance here is about 1.3 letters.