MATH 587/CSCE 557: HOMEWORK 3, DUE FEB 8.

1. 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?
[Note: the most frequent letters in English are E (12.7%), T (9.1%), A (8.2%), O (7.5%), I (7.0%), N (6.7%), S (6.3%), H (6.1%), R (6.0%), ...]

2. The following ciphertext was the output of an affine cipher:
FMXVEDKAPHFERBNDKRXRSREFMORUDSDKDVSHVUFEDKAPRKDLYEVLRHHRH
By performing a frequency count, guess the key used in the cipher (for full credit explain what you're doing). Note that your first attempt might not work - keep going!

3. (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.
Consider this for a ciphertext-only attack on a shift cipher. Considering the ciphertext ALIIP and its possible plaintexts, what is the unicity distance? Texts say that the unicity distance of a shift cipher should be about 1.3. Reconcile this with your last answer.