CIS 3362 Homework #3: Playfair, Hill, ADFGVX
Due: Check WebCourses for the due date.

1) (30 pts) The following ciphertext was encrypted using the Playfair cipher. The first eight letters of the plaintext are "themainr". Determine the secret key and decrypt the whole ciphertext. (Note: I may choose to reveal more of the plaintext, but I haven't made that decision yet.)

```
qknvbdradnrlbexrbmzilqkzenqkpbgqvnzwbgbnlazkfvnfybblqhybqhen
oqnzzspdpnlqkzenlwybkvlwbaimfdkeanliznrlbebmfdlubnlanzhaebko
kdblfdsfmrybsvzitzrfrlnihspczpyzmtosnednmlfdmqhsybmrmgnhnzmd
glizrttqchqlqgpfqknzmdgmwskeenwtvxpttmnpmdbnptenarqlowqpnffb
zkkqbpybbmfdogdmnffkbdsgmqnpbltlqlfdfbzkkqmqtqcyaeznfnbqkqqh
lkqhzbbrixlwyzmtmcebiqfdrttqht
```

2) (20 pts) The following question is more challenging, and I don't necessarily expect a lot of students to get it (which is why I have it worth as fewer points). Here is how I created this ciphertext:

a) Applied a substitution cipher to the plaintext and created an output I'll call c_1.

b) Applied a 2 x 2 Hill encryption key to c_1 to produce the final output.

The way I believe this can be broken is as follows:

1. Try all possible 2 x 2 matrices (with valid inverses).

2. For each, apply them to the ciphertext and just gather the letter frequencies of the resulting output, one of which, is guaranteed to be c_1. If we got the correct Hill key, we would expect these frequencies to mirror those of English. To detect this automatically, run the index of coincidence between each resulting output and English and rank as candidates for c_1 the ones that create the maximal index of coincidence with English. Then, take the top candidate, and use regular techniques to break substitution on it. Also, if you don't see any repeated n-grams that are kind of long, it's not going to be the answer, because I'll place at least one long repeated word in the plaintext.

For credit, I'll give a full 10 points for just generating all Hill keys, and another 5 points for calculating the corresponding frequencies for the supposed c_1's. Thus, even without cracking this one, you can get 15 out of 20 points and 45 out of 50 total.

```
pdyezowxbdlaprhualudbdgbdnpqgdnjwkhatovbgcvipqsutplfspooaxkwvakvukyjuuckih
yidwxzbypuprwejkahdwtqplnhphhgfvdohvhulfbypuxcjrfwzgvvjtqkdnwkzmefdltczmmo
gauwpumfyeiazrmblwhvpvwnexzowxbdchtphupqmhimqqmpidmbhulgmoqmbbnmvadjmfyvpr
pubdlsqaillhcirrebxhidxkphiwoqzgozofwjrxzfjtwhihupqmhimqqmpwxhallnkfiukbk
dxihjwkvsozodxtwxkxzaivyrdzovyhaewexdnzobcweezpqtywxkpinimwkhpyelfhfdjvu
```