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

1) The following ciphertext was encrypted using the Playfair cipher. The first eight letters of the plaintext are "THISTIME". Determine the secret key and decrypt the whole ciphertext.

```
etsypdqtgbrdbdafodpkftbadotlslsgwhyfetogkgwqlqnfedborhpvqtso
lqfbbuetsypdqtdpsyclltpfmylqpbbtrhgxornairemethndvhselsubknf
nhmpmknfpmflempdafpkybtktlqlnpdnqlvnugfbrgldnmadplbamotlaodv
fbiabouclqlnanetlqanelyferprhlbkiwzeolvbqcnwtfodelerptdsodfl
pvcmslsgwh
```

2) The following was encrypted using the Hill Cipher with a 2 x 2 matrix as the key. Determine both the decryption key as well as the message itself.

```
VGRHOSWQYGCEYEQYTVBEGVOXSNVQRHJAYRWDUKKIDWVZWAYESNMNTLDIHGPE
UKHCOKFDUQIQCDQSAZAZWRDWHXIYBEMGCEUOUBEIMRDUSTCRRHJAYRWDCDQF
BPJUYFKPEQNE
```

3) Let M = $\begin{pmatrix} 3 & 2 \\ 13 & 15 \end{pmatrix}$ be the encryption key for the Hill cipher. What is the corresponding decryption key?

4) You have intercepted a tiny portion of both the plaintext and matching ciphertext of a message encrypted using the Hill cipher with a 2 x 2 matrix key. The plaintext is "HILL" and the corresponding ciphertext is "CBPZ". What are the possible encryption keys based on this information only?

5) Decrypt the following message which was encrypted using a column transposition.

```
WTRTAOTSHAIWLSYESHEVHANSEHWHLLNPODETHOOELXLLOEYNUATYESEXVIOZ
ATZAUHTUTXIESHTURTAYZITXUOESHFSDTPRRLRHTWRUOWUEURYLXAHHIHUIS
MTOOOXOTPATEIRDTPEIE
```

6) Write a program to decrypt ciphertext created by the ADFGVX cipher. Please either write your code in C, C++, Python, or Java. You may edit the Java program adfgvx.java that is posted online. (This will be the easiest option and I prefer that you do this.) Your program should read input from a file with the following format:

```
1. 6 x 6 square, space separated on six lines
2. 7th line will be keyword all caps
3. 8th line will be n, # of messages to decrypt.
4. Next n lines will have each message, one by one. (ADFGVX only) Each of these
lines will have an even number of letters.
```

Your program should output to the screen the corresponding plaintext messages, one per line. (So, it should pretty much do exactly what the posted program does, but in reverse, taking in ciphertext and outputting plaintext.)