

**CIS 3362 Homework #3**  
**Polyalphabetic Ciphers**  
**Due: Check WebCourses for the due date.**

1) Decode the following message, which was encrypted using the Vigenere cipher. Make sure to discuss all the steps you took, the key you arrived at, and the decoded message.

grevezkmlqswnmewvclswksgkuswvklbcslwakcpmkocqswsiryrbllogneevwmx  
xjvltvpmoifyivlygdhkekuowgviudegisdqswgvhlezcpcviwcskwwweelgiagq  
rlxxbwaaiptitxhgffjqiqtdmmfxgtlgympycukyworrrkqkjwhexmfmvfrtnegdcd  
rwbcaacdvdviqmmrwhvyemissomncltfirgzgexnbimmxvfgekmlkllggvbjirzmuk  
mfosrzitkltxxfsvyikomqfxcecfyvucvkkmvkpggfjqiqtdmmfmpklbcqckwcxi  
zysbtcgesp

2) Decode the following message, which was encrypted using the Playfair cipher. Make sure to discuss all the steps you took, the key you arrived at, and the decoded message. (A couple days before the due date, some matching plaintext will be revealed.)

agsrepxithbstbesrqquxgkssikzaoagpibeorrzpuumkexpagrogxagtgxmhnea  
siaogtnqeaxotgoaxggsrebisiugsosrxqmigqrsiqsdtnxqlohszrtagsnqbyrb  
fedhtgqhbeahtuoboaxtaroirbsdenpklmnsagpisngpzrmuodbhsxqlgxbdzbvc  
rbogqhboisnaqgdtytggsrbebsbqpqnedgshamtebfkbtotbpeaqhaoagsroqxp  
tloboaqttryrksawkzpubptfbtnbmuodqhbepqrgbeirqumewnurtbsnagseqmnd  
zbvcrbktoboagsrsleoprbtspdenortalremdbduvqbuspaoagbaynxagsvqbutg  
gspedudhukqtpnealeoblisoqbbemtay

3) Decode the following message, which was encrypted using the Hill cipher with a 2 x 2 key. Make sure to discuss all the steps you took, the key you arrived at, and the decoded message.

yhgsgsyhdltnbnwguqakqerprdeyjfkmpmafdszcafytzlsawaxpuzauilrnxdz  
ritpzynknnzgaoqylcqodzycaxfowinuaotzqqqtmuxqsugeyyhgmhdrdedquou  
nkyhqgrxdp

4) Let  $M = \begin{pmatrix} 7 & 3 \\ 2 & 9 \end{pmatrix}$ . Determine  $M^{-1}$ , the corresponding decryption for the Hill cipher with an encryption key of  $M$ .

5) Write a program that reads in an input file (“hill.txt”) and outputs to the screen, the message in that file encrypted using the key designated in that file. Your output should have lowercase letters only. The input file format is as follows:

The first line of the file has a single positive integer,  $n$ , representing the length of one dimension of the Hill matrix. The next  $n$  lines each will have  $n$  integers each in between 0 and 25, separated by spaces, representing the corresponding row in the matrix. The following line of the file will have the message to encrypt. It will be a single line with lowercase letters only. A sample file is included below. Pad the end of your message with the character ‘x’ as necessary.

```
3
3 2 4
5 3 8
3 1 5
sallywenttotheseashoretocollectseashells
```

**Please write your program in C or Java.**

6) (Extra Credit) Write a program that encrypts text using the ADFGVX cipher. Read input from the file (“adfgvx.txt”) and output the ciphertext to the screen. The file format is as follows:

The first six lines of the file will contain 6 strings of length 6, containing each of the characters ‘a’ to ‘z’ and ‘0’ to ‘9’, exactly once. The next line of the file will contain a string of length 36 or less, containing some subset of the 36 characters designated previously. No characters will appear more than once in this string. The eighth and last line of the file will contain the message to encrypt. All characters on this line will be from the 36 previously mentioned characters. Write your ciphertext in uppercase. Here is a sample file:

```
qwertye
uiop12
asfdgh
jkl345
zxcv67
bnm098
compengir
thequickbrownfoxjumpedoverthelazydog0123456789
```