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

1) (10 pts) By hand, encrypt the plaintext "WAKEMEUPWHENSEPTMBERENDS" with the keyword "GREENDAY" and the padding character "Q".

2) (10 pts) For the Hill cipher, for a language with an **alphabet size of 37,** the encryption key is $\begin{pmatrix} 14 & 23 \\ 31 & 19 \end{pmatrix}$, what is the corresponding decryption key?

3) (30 pts) The following ciphertext was encrypted using the Playfair cipher. For the first few days, I won't give any matching plaintext. But, after a few days I'll reveal some characters or the plaintext, and then I'll reveal some more characters again before the due date. Determine the secret key and decrypt the whole ciphertext.

```
ranxrabuunimlgaelaumtienabovpdudnfaipbmlefsboctfmeztcxnlcix
cvrpzmcudapfpapmadktipabifllipabzanxcflzstlunzalozmbaauilpfb
iplmcqueidzpoztcxcqsabiqsufbiufsidkmtzsumlgsiadzbpnpamcnpaza
trosblarafvapcsosnuicsabimcotubpymcudvromaienabprpamcodsldys
ienlpaprpfimdeoudapepynalstdhfvaldapasidvapbsucapmadklgbutod
uztlglgcuzmbaautkpapamcnospudipfuhomadsbatisnlplgsmupilvolgd
uifqtsientkoqaplgsuhomadsticnprrfapvtykcfsdvroefqqiebcusiarp
ieaesbatapycixccsaqtbmcbatapycixclgdumefsbsblauidsrhoosudtva
lkfqihqlgtlaetspolplguducmsucaphogamckppodktlplmcsqydduidnos
blpapxgdudzponosbltdkaiftlplgsipdpubizuazscouembnmcumcofsmbf
prpcnqehr
```

4) (50 pts) Write a program in C, Python or Java that reads in information from standard input about several Playfair key, plaintext message pairs and prints out the corresponding encrypted ciphertext. Please use the padding character 'x', and if there's ever a double x, use the padding character q as the back up padding character. Output should be one message per line. Given below will be both the input format and output format.

Input Format

The first line of input will be a single positive integer, *n*, representing the number of messages to encrypt (test cases).

The test cases follow with information about them taking 2 lines each. The first line of each test case is the secret key to use for Playfair for that test case. This is guaranteed to be a string of lowercase letters. (Remember that duplicate letters get skipped and that i/j are together in the Playfair grid.) The second line of each test case will be the plaintext message to encrypt with the key given on the previous line.

Output Format

For each test case, output a single line with the corresponding cipher text. So that there is ONLY one correct answer, for the purposes of this program, always output ‘j’ (never ‘i’) and pad with the character ‘x’ as necessary. If you have to encrypt “xx”, please use the padding character ‘q’.

Sample Input

```
3
problems
shewenttothestore
temperature
shewenttothestore
cryptography
codingisquitefunparticularlyinthestateofmississippiletstestxxxal
soandqqq
```

Note: The last line printed above wraps around. Thus, the string “soandqqq” should be appended to the al on the previous line. This is accurate in the separately posted sample file.

Sample Output

```
agmvmkqyqbytmaqbpm
okueuwmvmlmfrnmltm
odekmakqlxkpfjwlyhycdpcugyncfqpbkmybrkadqeqzqkqzqkhphqmdbzrkzbpx
pxwhmlghlfxpxpxp
```

Note: Same issue with the third line of output shown above, it’s all in one line. The separately posted file playfair_sample.in is accurate.