

- **P8.8** *Letter frequencies.* If you encrypt a file using the cipher of [Exercise •• P8.7](#), it will have all of its letters jumbled up, and will look as if there is no hope of decrypting it without knowing the keyword. Guessing the keyword seems hopeless too. There are just too many possible keywords. However, someone who is trained in decryption will be able to break this cipher in no time at all. The average letter frequencies of English letters are well known. The most common letter is E, which occurs about 13 percent of the time. Here are the average frequencies of the letters.

A	8%	H	4%	O	7%	U	3%
B	<1%	I	7%	P	3%	V	<1%
C	3%	J	<1%	Q	<1%	W	2%
D	4%	K	<1%	R	8%	X	<1%
E	13%	L	4%	S	6%	Y	2%
F	3%	M	3%	T	9%	Z	<1%
G	2%	N	8%				

Write a program that reads an input file and displays the letter frequencies in that file. Such a tool will help a code breaker. If the most frequent letters in an encrypted file are H and K, then there is an excellent chance that they are the encryptions of E and T.

Show the result in a table such as the one above, and make sure the columns line up.

- **P8.10** *Playfair cipher.* Another way of thwarting a simple letter frequency analysis of an encrypted text is to encrypt *pairs* of letters together. A simple scheme to do this is the Playfair cipher. You pick a keyword and remove duplicate letters from it. Then you fill the keyword, and the remaining letters of the alphabet, into a 5×5 square. (Since there are only 25 squares, I and J are considered the same letter.)

Here is such an arrangement with the keyword PLAYFAIR.

```

P L A Y F
I R B C D
E G H K M
N O Q S T
U V W X Z

```

To encrypt a letter pair, say AM, look at the rectangle with corners A and M:

```

P L A Y F
I R B C D
E G H K M
N O Q S T
U V W X Z

```

The encoding of this pair is formed by looking at the other two corners of the rectangle, in this case, FH. If both letters happen to be in the same row or column, such as GO, simply swap the two letters. Decryption is done in the same way.

Write a program that encrypts or decrypts an input text according to this cipher.