University of Waterloo

Sun microsystems

Problem J4: A Simple Encryption Algorithm

One of the simplest ways of coding a message is to do a letter shift. For example if you shift the letters in the original message by 5 then A in your original message becomes F in the coded message. (B → G, C → H, …, T → Y, U → Z, V → A, …, Z → E). To decode the message, you simply need to shift back by the same number.

A slightly trickier encryption uses a keyword to determine the amount of the shift. Suppose you were using a keyword "ACT". To encode the message, you take the original message, remove everything but the alphabetic characters, and form the message into a block that has the same width as the keyword. Here is a sample message to encrypt:

BANANA & PEEL

The blocked version of the message is shown below with the keyword ACT as a header.

A	**C**	**T**
B	A	N
A	N	A
P	E	E
L		

Now, the message is encoded using a letter shift. However, this time it is not a uniform shift; it will depend upon the keyword letter at the top of the column. If the letter at the top of the column is an 'A', then the letters in that column are not shifted. If the letter is a 'B', then the letters in that column shift by 1, and so on. In the example, the letters in the third column will shift by 19 since the 'T' is the 20th letter of the alphabet.

The encoded message is:

A	**C**	**T**
B	C	G
A	P	T
P	G	X
L		

You will write a program that will accept a keyword and a string to be encoded. The keyword will never be more than 6 characters. The message will always be given in all upper case characters. The total message length will never be more than 60 characters.

Sample Input 1	**Sample Output 1**
ACT	BCGAPTPGXL
BANANA & PEEL	
Sample Input 2	**Sample Output 2**
TRICKY	BCWXONKFOTKKFZVI
I LOVE PROGRAMMING!	