4938 - Manual Cipher

North America - Southern California - 2010/2011

You are employed by a secret government agency that communicates with its field agents via encrypted messages only. The Agency is sending you to a location that does not have electricity, so you must send reports by scratching encrypted short messages onto tree bark and floating the bark down river for recovery by fellow agents. Five hours before departure, you consider it wise to provide a decryption program so that the Agency can decipher your important communications.

You will use a *numerically keyed aperiodic polyalphabetic cipher*. Such a scheme changes the encipherment alphabet after a specified number of letters, given in a numerical key. The numerical key describes how many characters to use in an encipherment alphabet before changing to a new alphabet. You will actually use a single alphabet, but rotate the substitution based upon the keyword. The decrypted (plain) alphabet consists of lowercase ASCII letters a-z and the space character. The encrypted (cipher) alphabet consists of uppercase ASCII letters A-Z and the space character.

Table 1 shows an encryption/decryption table based upon the codeword *BLUE* and numerical key *2314*. The plain-text alphabet is displayed across the top as column headers. The first column reading down spells out the codeword, BLUE. For each row, continue the cipher alphabet after the codeword character, cycling back to `A' after the space character. Use the numerical key to construct the last column of the table. The numerical key does not become part of the encrypted message; it merely dictates how many characters to use from an encipherment alphabet before changing to the next alphabet.

Your program is to decrypt messages that were encrypted using this process: Given the plain-text message "watson are you there", use the first row to substitute two characters `w' and `a' with `X' and `B'. Next, use the second row to substitute the three characters `t' `s' `o' with `D' `C' `Z'. Substitute one character, `n' with `G'. Substitute the next four characters ` ' (space) `a' `r' `e' with `D' `E' `V' `I'. Having exhausted the codeword and numerical keys (2 + 3 + 1 + 4 = 10 characters, change back to the first row, and substitute the two characters ` ' (space) `y' with `A' and `Z'. Continue using the character counts 2-3-1-4-2-3-1-4-2-... until the entire message is enciphered.

Decryption is the reverse of encryption. Given the cipher text "XBDCZGDEVIAZZEKMLIVI", start at the first row and substitute two characters `X' and `B' with `w' and `a'. Change to the next alphabet on the second row and substitute three characters `D' `C' `Z' with `t' `s' `o'. Continue as with encryption, using the character counts 2-3-1-4-2-3-1-4-2-... until the entire message is deciphered.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	sp	
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z		A	*2*
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z		A	B	C	D	E	F	G	H	I	J	K	*3*
U	V	W	X	Y	Z		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	*1*
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z		A	B	C	D	*4*

Table 1. Code word *BLUE* with a numerical key of *2314*. (`sp` indicates space)

Input

Input consists of two or more lines. The first line contains the code word, a colon, and the numerical key. The codeword is built from the characters A-Z only (no spaces). A codeword may be 2-10 characters long. For each letter in the code word, there will be a corresponding decimal digit in the numerical key. `0' (zero) will never occur in the numerical key. The remaining lines contain enciphered text, with each line being treated as

a separate message. Lines of enciphered text range between 1 and 79 characters. Input is terminated by end-of-file.

The plain-text alphabet is always a-z and space, and the cipher text alphabet is always A-Z and space.

Output

For each line of enciphered text, your program is to produce a line of deciphered plain-text. Each plain-text output line is to be the same length as the corresponding enciphered input line.

Sample Input

```
BLUE:2314
XBDCZGDEVIAZZEKMLIVI
NPCAEBXSIWAVYMPUVEFPFACPYXDRIXUJYR
CBBVKKYRRMOHKWZPDWIREAXZBYDXVIFT
```

Sample Output

```
watson are you there
mosquitoes unbearable send netting
bark running low send more trees
```

Southern California 2010-2011