

Problem 220: ADFGVX

Difficulty: Hard

Author: Brett Reynolds, Annapolis Junction, Maryland, United States

Originally Published: Code Quest 2023

Problem Background

In 1894, an Italian physicist named Guglielmo Marconi discovered a world-changing new technology - the ability to communicate wirelessly through the use of radio waves. Up to that point, all communication required some form of physical connection, either a messenger manually delivering a written message, or a telegraph operator transmitting signals over a wire using Morse Code. This had a tremendous impact on our society as well as many other areas.

Of interest to many countries was the military application of the radio; a unit equipped with a radio could remain in contact with their commanders at all times, and so could receive new orders and relay intelligence reports in real time. However, since anyone with an antenna could receive those same orders and reports - including the enemy - a secure encryption scheme became of paramount importance.

When World War I broke out just 20 years after Marconi's discovery, nations on both sides of the conflict grappled with this problem. At the time, most ciphers used either substitution (replacing letters or groups of letters with different letters/groups) or transposition (switching the order of letters or groups of letters without changing them); however, there were established methods of breaking ciphers that used either approach, and so these ciphers were insecure. Near the end of the conflict, Germany believed they'd found a solution to this problem: the ADFGVX cipher, which employed both substitution and transposition.

Problem Description

The ADFGVX cipher works in two steps: letters are substituted according to a grid, and then are transposed to further obfuscate the message. The key to the cipher consists of the layout of the substitution grid and a keyword which directs how the transposition should be performed. The end result is an encrypted message that uses only the letters A, D, F, G, V, and X. If you're wondering why the cipher uses those specific letters, it's because they're easily distinguishable from each other in Morse Code, reducing the risk that the message would be misunderstood and turned into gibberish.

To begin, a 6-by-6 grid is populated with the digits 0 through 9 and the 26 letters of the English alphabet, arranged in a random order. Each row and column of the grid is associated with one of the letters A, D, F, G, V, or X in sequence, as shown in the table on the next page:

	A	D	F	G	V	X
A	q	c	t	1	o	8
D	w	0	b	d	z	k
F	4	h	p	m	3	j
G	g	s	6	7	e	v
V	l	9	2	f	x	n
X	y	a	u	5	i	r

Next, each letter of the message is located within the grid and replaced with a pair of letters; the labels for that cell's row and column, respectively. For example, using the grid above, 'c' becomes 'AD' - the letter 'c' appears in row A and column D. "code quest 2022" would be encoded as "AD AV DG GV AA XF GV GD AF VF DD VF VF". While this looks like nonsense, it's still easy to break, and so the cipher adds a second step. A new grid is created now, with the top row filled in with the letters of a keyword. The rest of the grid is created by listing the individual letters in the semi-enciphered message from left to right and top to bottom:

M	A	R	T	I	N
A	D	A	V	D	G
G	V	A	A	X	F
G	V	G	D	A	F
V	F	D	D	V	F
V	F				

→

A	I	M	N	R	T
D	D	A	G	A	V
V	X	G	F	A	A
V	A	G	F	G	D
F	V	V	F	D	D
F		V			

The table on the left shows the populated transposition grid; the table on the right shows how the transposition is performed. Once the message is filled in completely, the columns are reordered to place the letters of the keyword in alphabetical order. The final encrypted message is then read from left to right, top to bottom. As a result, our original message "code quest 2022" is encrypted as:

DDAGAVXGFAAVAGFGDFWFDFFV

For this problem, your team will need to decrypt messages that have been encoded using the ADFGVX cipher. To decrypt a message, follow the encryption process in reverse. Good luck!

Sample Input

The first line of your program's input, **received from the standard input channel**, will contain a positive integer representing the number of test cases. Each test case will include eight lines of text:

- The first six lines will contain six characters each (lowercase letters and/or numbers), representing the layout of the substitution grid used to encode the message.

- The seventh line will contain a single word in uppercase letters, which is the keyword used to perform the transposition step of the cipher. This keyword will not contain any duplicate letters.
- The eighth line will contain a message consisting only of the characters A, D, F, G, V, and/or X, representing the encoded message.

```
3
qct1o8
w0bdzk
4hpm3j
gs67ev
192fxn
yau5ir
MARTIN
DDAGAVVXGFAAVAGFGDFVVFDDFV
1c62et
iljvm7
d8rgko
suabph
9y354z
fnxq0w
CODE
AFFDVGVDAFXXFFGGGVFGVDXDGAAXGDAXD
3kcdqg
5iub1f
92me6a
h017ry
xto84s
znjwvp
QUEST
GVADDXDDDVAVFVXGFFGADAFVXGVDVDVVGXDDGAVFGGFVXVG
```

Sample Output

For each test case, your program must print a single line containing the decrypted plaintext message in lowercase letters and numbers. Do not attempt to re-insert spaces or punctuation into the message.

```
codequest2022
cryptophyisfun
thisiscodequests10thyear
```