

Problem 162: Null Cipher

Difficulty: Easy

Author: Javier Jimenez, Marietta, Georgia, United States

Originally Published: Code Quest 2022

Problem Background

There are two primary methods to obscuring information you wish to keep hidden. Cryptography uses an algorithm or similar process to convert a message to another form, rendering it illegible. Steganography aims to simply hide a message so that a would-be eavesdropper doesn't realize a message actually exists in the first place. Steganography has taken a wide range of forms throughout history: messages written in invisible ink, patterns representing Morse Code knitted into sweaters, and messages shrunk to microscopic size and printed on transparent film have all been used throughout history. One of the simplest forms of steganography is known as the "null cipher."

Problem Description

The null cipher is effective because it appears to be a perfectly harmless message. The secret message - known as a ciphertext - is hidden within another message by adding in a large number of "null" values, either words or letters, which have nothing to do with the original message. Ideally, an eavesdropper would see the message and not realize there was a second message hidden inside, but the intended recipient would know to remove certain words or characters to restore the original message.

Lockheed Martin is working with the National Security Agency to test a slightly different form of null cipher. The NSA intends to embed a message within a string of random characters. Their hope is that an eavesdropper *will* suspect a hidden message, but will assume that the random nature of the message means that it's encrypted using a cipher, and will waste time attempting to break it. In reality, the message will simply be scattered throughout the text string. Any character that is part of the actual message will immediately follow an English vowel; that is, one of the letters a, e, i, o, or u. When those characters occur in the actual message, they will follow a different vowel; the character after them is *not* part of the message. For example, the string below can be read as "hello world":

fk^aan^elⁱgue^yilⁱfh^al^efkⁱjnh^eds^oak^ujfh^endsⁱfi^uap^ourⁱh^enf^edj^ugb^al^efkⁱjs^hed^ef^unsⁱf

Given some sample strings generated by the NSA, design a program that can extract the original messages.

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 a single line of text, containing lowercase letters.

```
3
fksahnlgueyilfhnaIfkjnhdssaokjfhnDsfiwaourhnfdjgbalfkjshedfnsf
mkjmnacioudhrieeqwthyiugueresjfgwatfhwghfnhgnffn
elruoqywicwnjksakvfbsgyohuehngghiefhggadfgsfSfs
```

Sample Output

For each test case, your program must print a single line containing the plaintext message extracted from the input string.

```
helloworld
codequest
lockheed
```