CLAVES SEGURAS GRADO 11

Un password seguro es algo delicado. Los usuarios prefieren passwords que sean fáciles de recordar (como “amigo”), pero este password puede ser inseguro. Algunos lugares usan un generador randómico de passwords (como “xvtpzyo”), pero los usuarios toman demasiado tiempo recordándolos y algunas veces lo escriben en una nota pegada en su computador.

Una solución potencial es generar password “pronunciables” que sean relativamente seguros pero fáciles de recordar.

FnordCom está desarrollando un generador de passwords. Su trabajo en el departamento de control de calidad es probar el generador y asegurarse de que los passwords sean aceptables.

Para ser aceptable, el password debe satisfacer estas tres reglas:

1. Debe contener al menos una vocal.

2. No debe tener tres vocales consecutivas o tres consonantes consecutivas.

3. No debe tener dos ocurrencias consecutivas de la misma letra, excepto por ‘ee’ o ‘oo’.

(Para el propósito de este problema, las vocales son 'a', 'e', 'i', 'o', y 'u'; todas las demás letras son consonantes.)

Note que Estas reglas no son perfectas; habrán muchas palabras comunes/pronunciables que no son aceptables.

La entrada consiste en una o más potenciales passwords, uno por línea, seguidas por una línea conteniendo una palabra 'end' que señala el fin de la entrada. Cada password tiene como mínimo una y como máximo veinte letras de largo y está formado por solo letras en minúscula. Por cada password, despliegue si es o no aceptable, usando el formato mostrado en el ejemplo de salida.

Example

Input

a

tv

ptoui

bontres

zoggax

wiinq

eep

houctuh

end

Output

<a> is acceptable.

<tv> is not acceptable.

<ptoui> is not acceptable.

<bontres> is not acceptable.

<zoggax> is not acceptable.

<wiinq> is not acceptable.

<eep> is acceptable.

<houctuh> is acceptable.