Phishing

En los últimos años, el phishing se ha convertido en uno de los principales vectores de infección para los ciberataques. Estamos intentando detectar qué mails tienen phishing en base a unas cuantas palabras clave.

Dada una secuencia de palabras peligrosas, podemos clasificar como phishing una cadena de texto siempre que contenga al menos un 50% de estas palabras.

Entrada

La entrada comenzará con un número N que indicará el número de palabras que se catalogan como peligrosas dentro de un mail. A continuación, vendrán N líneas con N palabras peligrosas separadas por espacios. Después vendrá un número M que indica el número de palabras que contiene el mail. Finalmente, vendrán M líneas con las M palabras que componen el mail. Se garantiza que, en caso de contenerlas, el mail sólo incluirá las palabras peligrosas una vez y en el orden en que vienen en la entrada.

Salida

Por cada caso de prueba, se imprimirá “PHISING DETECTADO” si el 50% de las palabras del mail o se corresponden con palabras maliciosas. Por el contrario, se imprimirá “CORREO LEGITIMO” si esta situación no se da.

Ejemplo de entrada	**Ejemplo de salida**
3 contraseña sacar dinero 6 Necesito tu contraseña para sacar dinero	PHISHING DETECTADO
Ejemplo de entrada	**Ejemplo de salida**
3 contraseña sacar dinero 10 He perdido mi contraseña y ahora no puedo sacar dinero	CORREO LEGITIMO

Límites

- $0 \leq N \leq 20$
- $0 \leq M \leq 100$