Exercise 1094795585: Flag Verification Problem

Background In Capture The Flag (CTF) competitions, a "flag" is a secret string or piece of data that participants must discover to prove they have solved a particular challenge. The flag acts as evidence that the competitor has successfully completed the task, whether it involves exploiting a vulnerability, analyzing a binary, solving a cryptographic puzzle, or investigating digital artifacts. Typically, flags are formatted in a recognizable way, such as `CTF{example_flag}` or similar, and this format is usually specified in the challenge description.

Flags can be either static, meaning the same flag is available to all teams and embedded directly within the challenge, or dynamic, where each team receives a unique flag generated for their specific instance of the challenge. The process of finding a flag varies depending on the type of challenge. For example, in web security challenges, participants might need to exploit a website to reveal the flag, while in reverse engineering, they might analyze a program's code or behavior to extract it. Forensics challenges may require recovering hidden data from files or memory, and cryptography challenges involve breaking or analyzing cryptographic schemes to uncover the flag.

Once a participant finds a flag, they submit it to the CTF platform, which checks its validity and awards points accordingly. Ultimately, the primary objective in CTF competitions is to find and submit as many flags as possible, demonstrating skill and knowledge across various areas of cybersecurity.

Statement of the problem The author of this challenge accidentally lost the flag to this challenge. However, unlike in *Flag Warehouse*[1], where the flag is lost in a pile of randomness, the author of this challenge accidentally dropped the flag into an industrial grade food waste processor. As a result, the flag is hashed together with all the revolting food waste, which, according to cryptography, is irreversible. But, being the computer scientist that you are, who can write $O(n)$ solutions to the *2sum* problem, you are confident that can *identify* the flag, even if you cannot reverse the process.

Given some hex-encoded SHA256 hash values, determine whether the value belongs to the real flag.

Input The first line contains the integer n ($1 \leq n \leq 10000$), the number of lines in the test case. Each line of the following n lines contains exactly one hex-encoded SHA256 hash.

Output If the hash is the hash of the flag of this challenge, output "**YES**". Otherwise, output "**NO**"

Sample Input If the flag is `cuhk25ctf{minpcc_is_very_secure}`, then the input:

```
3
29199fd444cb4a731c5de120fd22a9ae1eac03964efc343d3817697f11a6b300
5b19468faec4dbf2a602177b825e4d47bb371fad74d75c23672429aeacaef8f4
29199fd444cb4a731c5de120fd22a9ae1eac03964efc343d3817697f11a6b300
```

Sample Output Should output:

```
YES
NO
YES
```

Hint You are reminded that the flag format for this challenge is `cuhk25ctf{[0-9a-zA-Z_]+}`.[2]

[1] See CUHK CTF 2024
[2] only if that helps lol