```
char* init_buf = 0x804e220;
int* buf = ebp - 0x98;
buf[0] = *(int*)(init_buf);
buf[1] = *(int*)(init_buf + 0x4);
buf[2] = *(int*)(init_buf + 0x8);
(char*)(buf)[0xc] = init_buf[0xc];
```
↓
```
int idx = 0;        // &idx = ebp - 0x4
char str[0x80];     // str = ebp - 0x84 (input key)
int v1;             // v1 = ebp - 0x88
char* str1 = buf;   // str1 = ebp - 0x98
int v2;             // &v2 = ebp - 0x9c
```
↓

str[idx] != 0?

- true → `(str[idx] >= 'a') && (str[idx] <= 'z')?`
  - true →
    ```
    v1 = &str[idx];
    *((char*)v1) = str[idx] - 'a' + 'A';
    ```
    → `++idx;` → (back to str[idx] != 0?)
  - false → `++idx;` → (back to str[idx] != 0?)
- false → `idx = 0;`
  ↓
  str1[idx] != 0?
  - true →
    ```
    v1 = str[idx];
    v1 = 0xc0de * v1;
    v2 = v1;
    ```
    ↓
    v2 == str1[idx]?
    - false → `idx != 0xc?`
      - false → **YES!**
      - true → **Nope.**
    - true → `++idx;` → (back to str1[idx] != 0?)
  - false → **Nope.**
```
```