

```
int* init_buf = 0x80500e0;
int* buf = 0x82d5d50;
buf[0] = init_buf[0];
buf[1] = init_buf[1];
buf[2] = init_buf[2];
buf[3] = init_buf[3];
char* bp = 0x82d5dec;
```

```
char str[0x80]; // str = bp - 0x84 (input key)
char str1[];    // str1 = bp - 0x9c
int idx;        // &idx = bp - 0x4
int v1;         // &v1 = bp - 0xa0
int v2;         // &v2 = bp - 0x8c
int v3;         // &v3 = bp - 0xa4
int v4;         // &v4 = bp - 0x88
int v5;         // &v5 = bp - 0xa8
int v6;         // &v6 = bp - 0xac
```

```
idx = 0;
```

```
str[idx] + 1 != 0?
```

```
(str[idx] + 1 < 'a') || (str[idx] + 1 > 'z')?
```

```
idx = 0;
v2 = 1;
```

```
str1[idx] != 0?
```

```
v1 = &str[idx];
*((char*)v1) = str[idx] + 1 - 'a' + 'A';
```

```
v3 = idx;
v4 = str[idx];
v5 = 0xc0de;
v4 = v5 * (v4 + 1);
v6 = v4 + 1;
```

```
v6 != str1[v3] + 1?
```

```
v7 = 0;
```

```
v7 = 1;
v2 = v2 & v7;
++idx;
```

```
++idx;
```

```
idx != 0xf?
```

```
v2 == 0?
```

Nope.

YES!