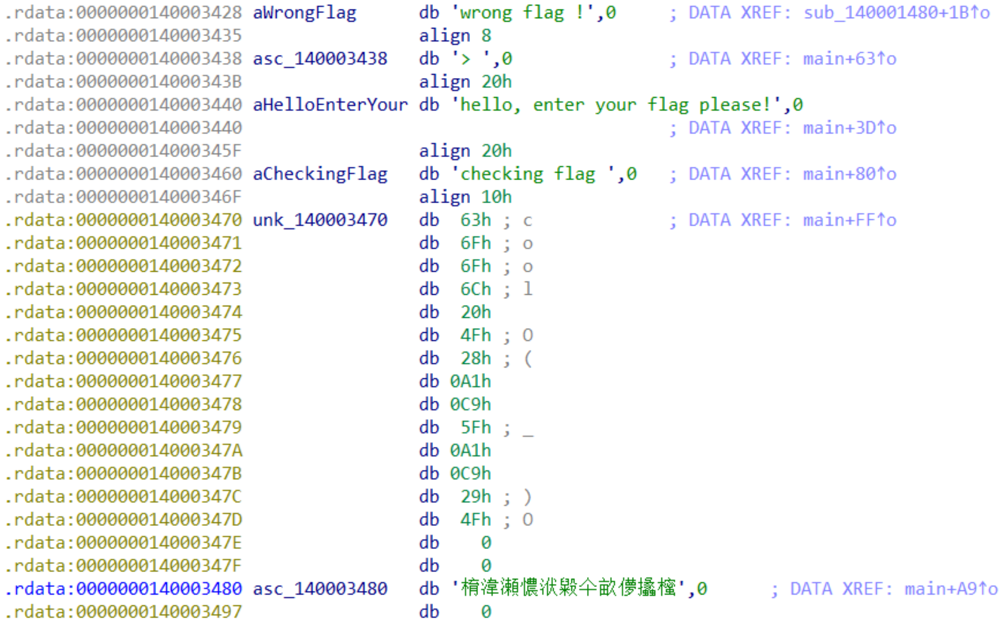
helloRe

用ida打开

先找找输入输出发现



```
.rdata:0000000140003428 aWrongFlag      db 'wrong flag !',0     ; DATA XREF: sub_140001480+1B↑o
.rdata:0000000140003435                 align 8
.rdata:0000000140003438 asc_140003438   db '> ',0               ; DATA XREF: main+63↑o
.rdata:000000014000343B                 align 20h
.rdata:0000000140003440 aHelloEnterYour db 'hello, enter your flag please!',0
.rdata:0000000140003440                                         ; DATA XREF: main+3D↑o
.rdata:000000014000345F                 align 20h
.rdata:0000000140003460 aCheckingFlag   db 'checking flag ',0   ; DATA XREF: main+80↑o
.rdata:000000014000346F                 align 10h
.rdata:0000000140003470 unk_140003470   db  63h ; c             ; DATA XREF: main+FF↑o
.rdata:0000000140003471                 db  6Fh ; o
.rdata:0000000140003472                 db  6Fh ; o
.rdata:0000000140003473                 db  6Ch ; l
.rdata:0000000140003474                 db  20h
.rdata:0000000140003475                 db  4Fh ; O
.rdata:0000000140003476                 db  28h ; (
.rdata:0000000140003477                 db 0A1h
.rdata:0000000140003478                 db 0C9h
.rdata:0000000140003479                 db  5Fh ; _
.rdata:000000014000347A                 db 0A1h
.rdata:000000014000347B                 db 0C9h
.rdata:000000014000347C                 db  29h ; )
.rdata:000000014000347D                 db  4Fh ; O
.rdata:000000014000347E                 db    0
.rdata:000000014000347F                 db    0
.rdata:0000000140003480 asc_140003480   db '棈湋瀬憹洑毇仐畝儚擑檧',0      ; DATA XREF: main+A9↑o
.rdata:0000000140003497                 db    0
```

看到这个这串乱码十分可疑（“棈湋瀬憹洑毇仐畝儚擑檧”）

改成utf-8格式得到

97h 99h 9Ch 91h 9Eh 81h 91h 9Dh 9Bh 9Ah 9Ah 0ABh 81h 97h 0AEh 80h 83h 8Fh 94h 89h 99h 97h 0 0

然后看代码发现对这串数字进行异或解密即可

写一个程序解密

```
#include <stdio.h>
int main()
{
    int tag = 0xff;
    unsigned char ida_chars[] =
    {
    151, 153, 156, 145, 158, 129, 145, 157, 155, 154,
    154, 171, 129, 151, 174, 128, 131, 143, 148, 137,
    153, 151, 0, 0
    };
    for (int i = 0; i < 22; i++) {
        printf("%c", ida_chars[i] ^ (tag--));
    }
    return 0;
}
```

输出即为flag