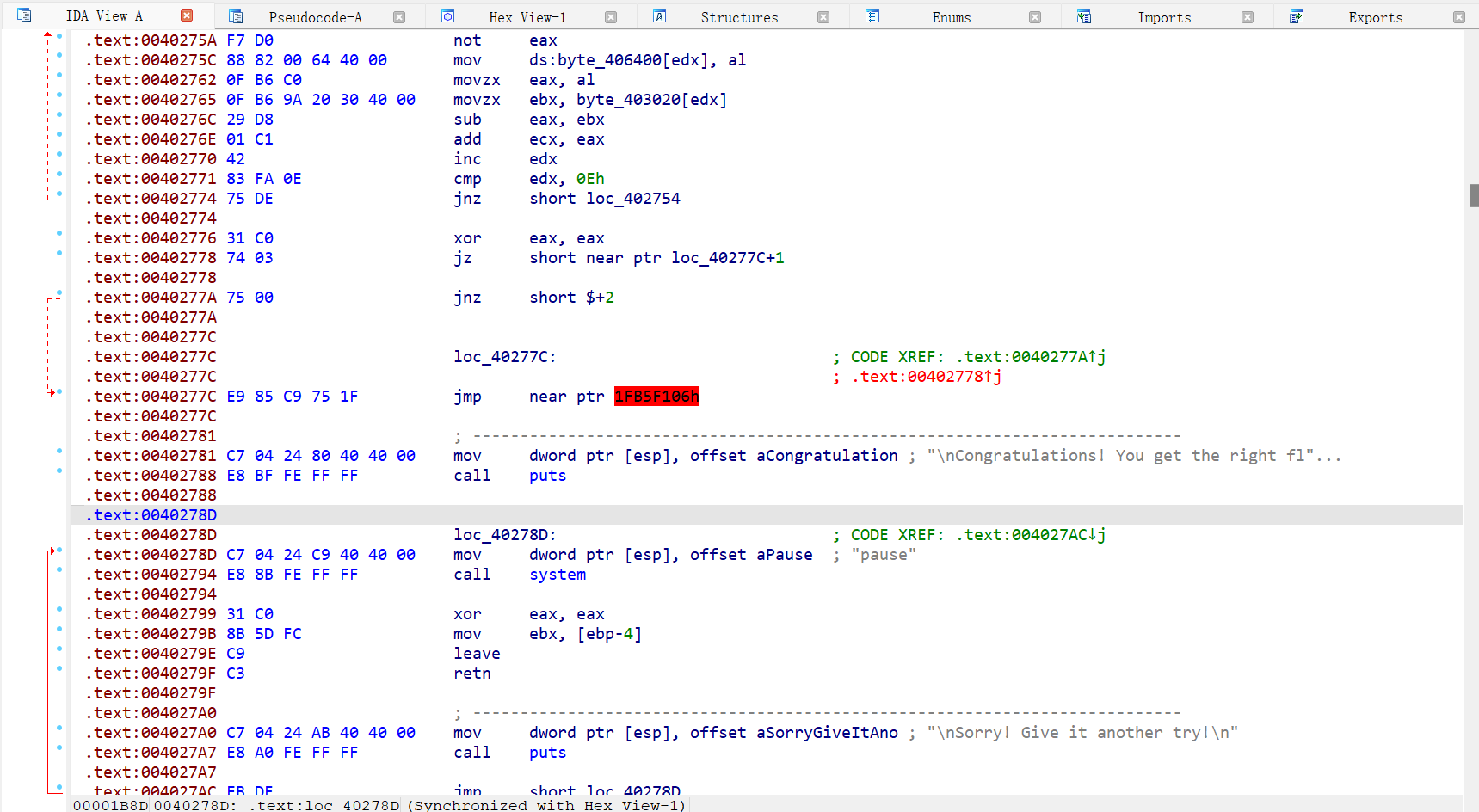
Homework-3 Report

姓名：项 枫 学号：2022211570

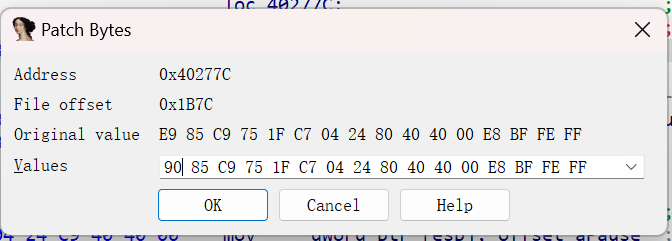
**一、解题过程**

1、花指令解决

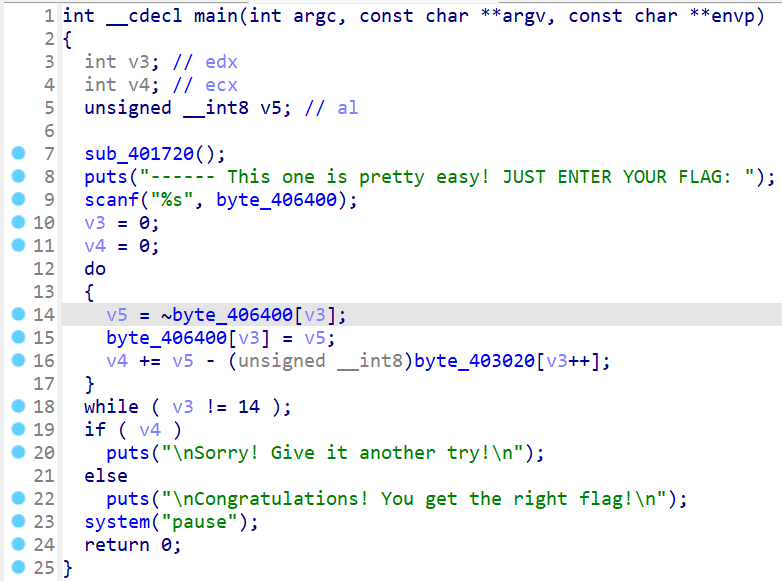
（1）存在jmp花指令



（2）将E9改成90



（3）F5反编译



2、main函数分析

（1）12—17行：将输入字符串先逐字符取反，再与byte\_403020处字符串逐个字符进行相减，相减结果进行相加存入v4。

（2）19—22行：只有v4为0时，才输出"\nCongratulations! You get the right flag!\n"。

综上，循环14次，可知字符串长度为14；flag为byte\_403020处字符串逐字符取反。

2、解flag程序

（1）程序代码（C++）如下：

#include<bits/stdc++.h>

int main(){

char flag[]={0xBD,0x9A,0x9E,0x8B,0xD5,0xCF,0x92,

0x96,0x9C,0x8D,0x90,0x91,0xD5,0xDE};

int i;

for(i=0;i<strlen(flag);i++){

flag[i]=~flag[i];

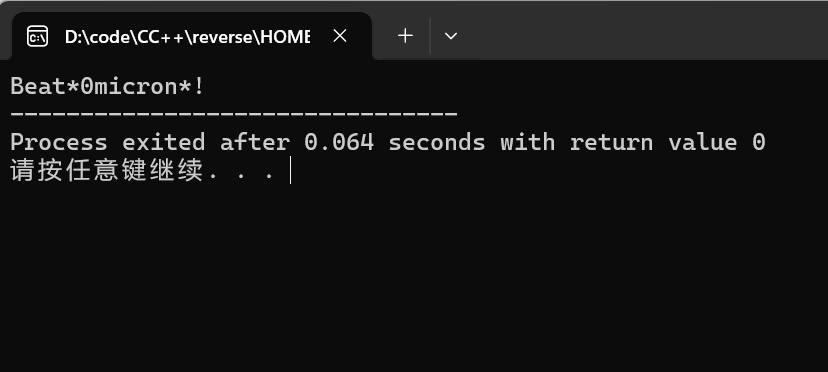
}

printf("%s",flag);

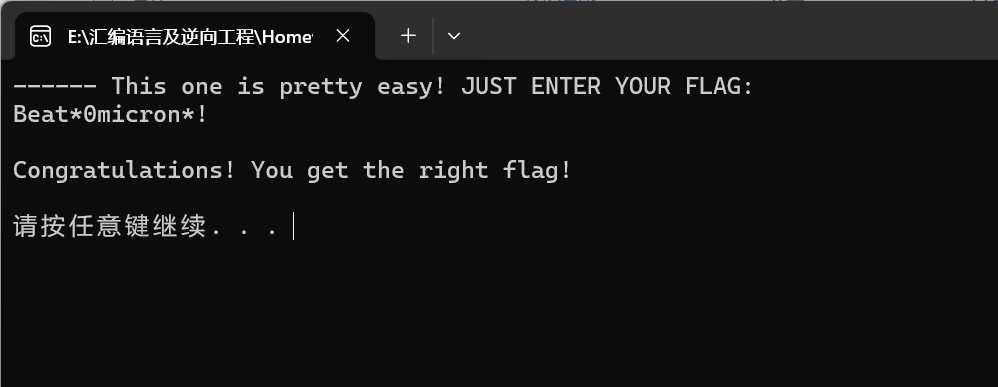
return 0;

}

（2）程序运行结果



3、flag成功通过



**二、收获和感受**

通过本次作业，初步了解了花指令及其逆向的操作。

最后，感谢潘老师课上辛勤的教学。