### 北京邮电大学——期末线上机试答题报告

|  |  |  |
| --- | --- | --- |
|  |  |  |
| 机 试 总 成 绩  (满分 100`) |  | |

|  |  |
| --- | --- |
| **学院** | 网络空间安全学院 |
| **专业** | 信息安全 |
| **班级** | 2022211801 |
| **姓名** | **项枫** |
| **学号** | 2022211570 |
| **座位号** | 10 |
| **考核科目** | 《汇编语言与逆向工程》 |
| **考核方式** | 线上机试、开卷 |

**2024年06月22日（上午） 10:00—12:00**

**（10:00—12:00期间，应试电脑需全程断网）**

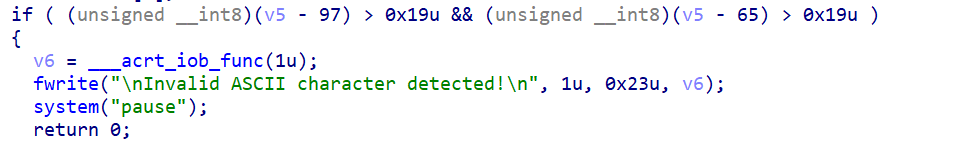
1. CPP\_1 (本题20`)

1、函数分析：

进入main:



由此可知flag长度为5

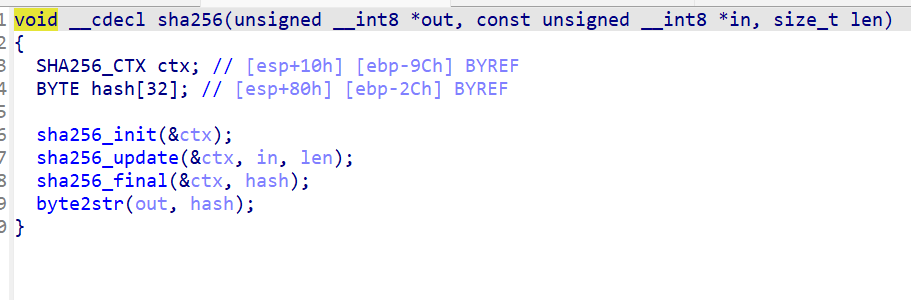


ASCII码范围在65~90，97~122之间

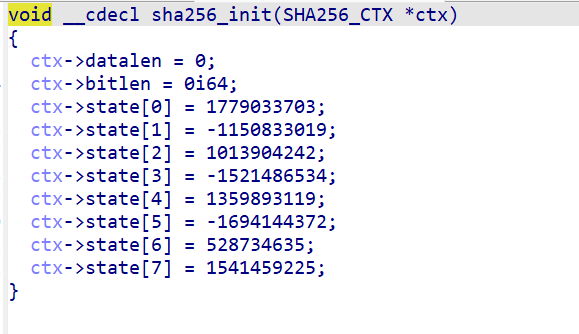


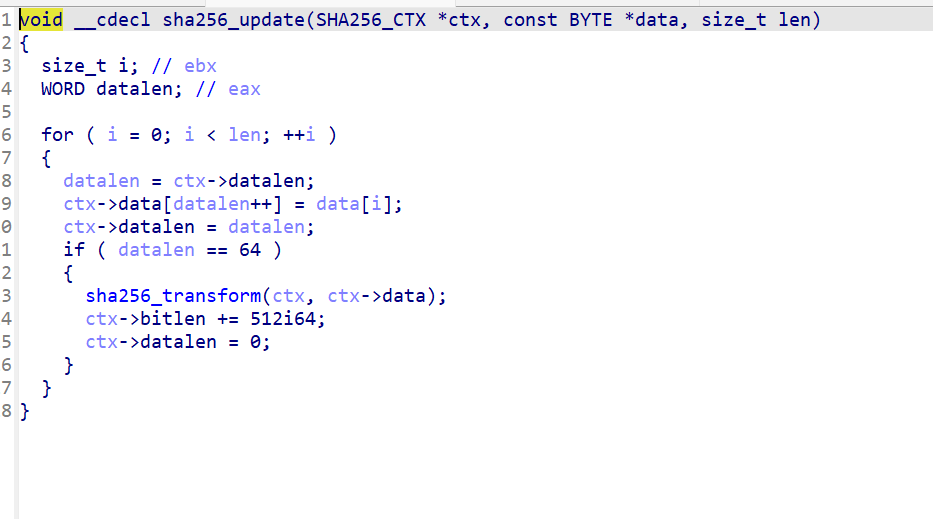
取前4个字符进入sha256函数进行运算

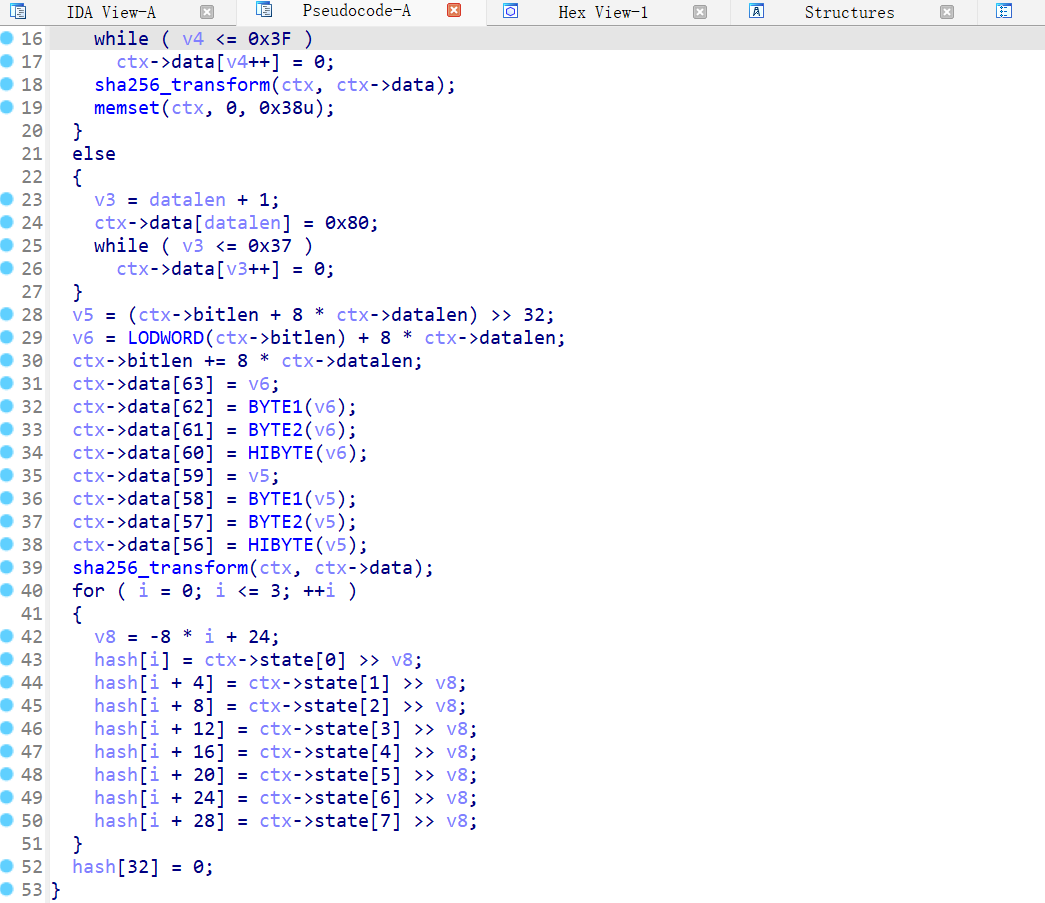
双击进入sha256()函数

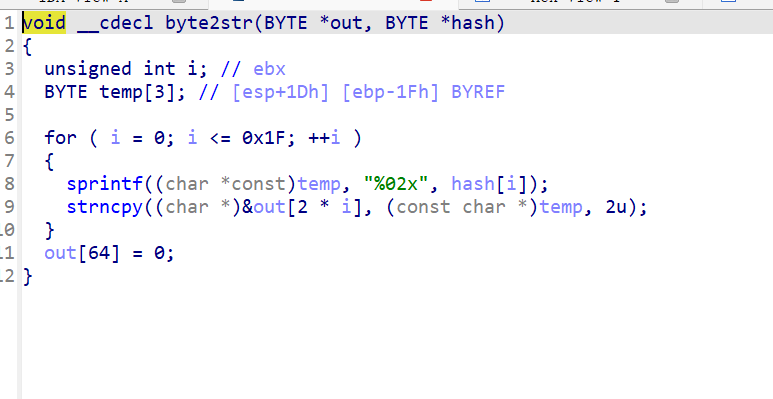


可看到sha256\_init()，sha256\_update()，sha256\_final()，byte2str()几个函数，逐个进入



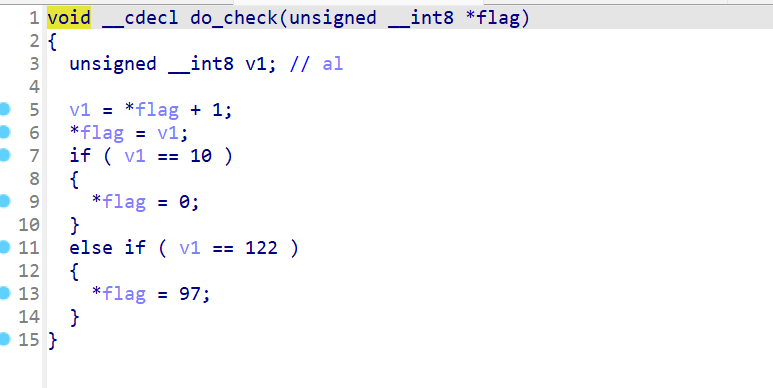




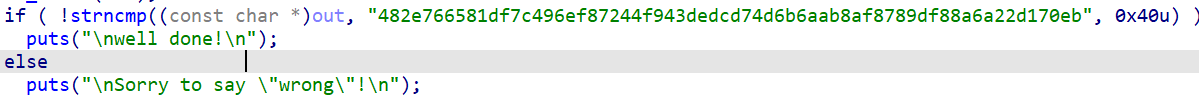


综上，可判断为sha256算法

进入do\_check()函数：



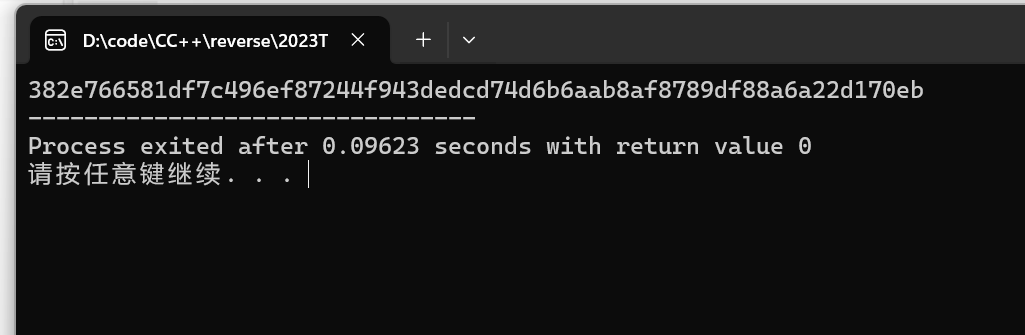
该函数为，将sha256的结果进行+1；



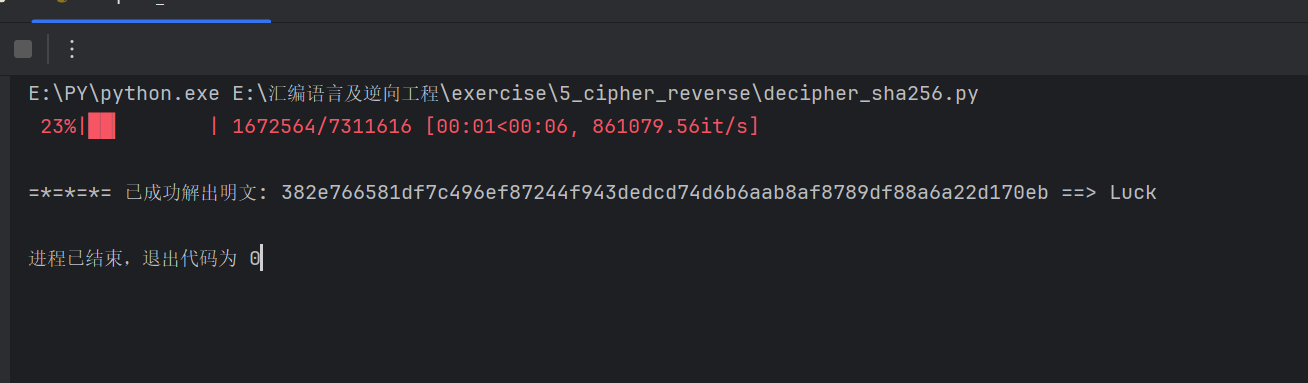
将经过以上运算后的结果，与字符串“482e766581df7c496ef87244f943dedcd74d6b6aab8af8789df88a6a22d170eb”进行比对，一致则正确。

2、解flag：

先将字符串“482e766581df7c496ef87244f943dedcd74d6b6aab8af8789df88a6a22d170eb”进行减1操作，得到字符串为“382e766581df7c496ef87244f943dedcd74d6b6aab8af8789df88a6a22d170eb”；



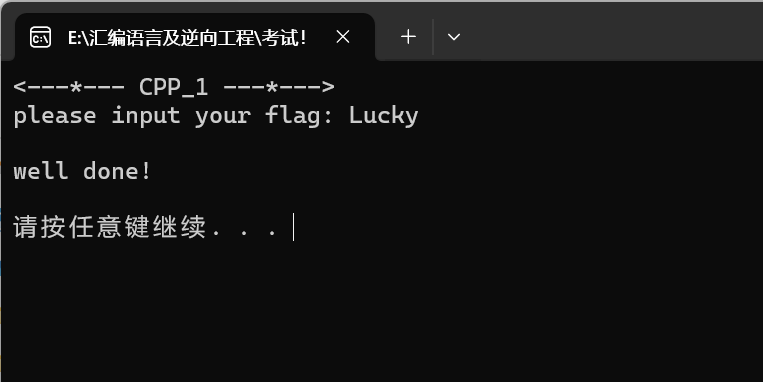
然后进行sha256爆破：



结果为Luck

Flag为：Lucky

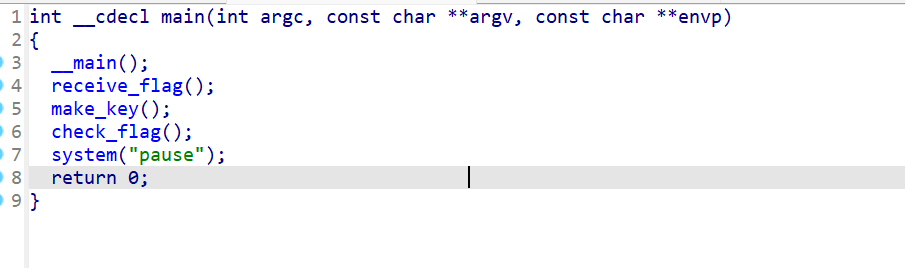
Flag通过：



1. CPP\_2 (本题20`)

1、函数分析：

进入main



进入receive\_flag()



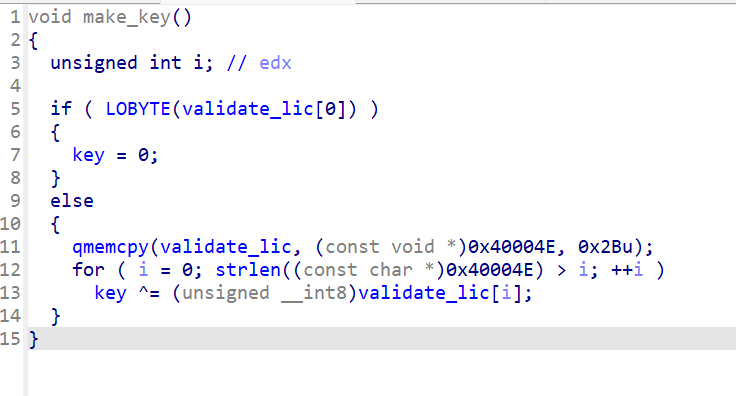
读入字符串

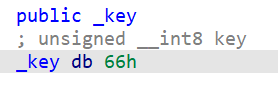




判断字符串长度是否为flag\_len即0FH即16

进入make\_key()



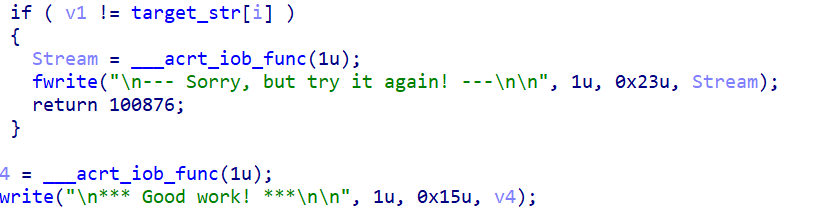


Key初始为0x66

进入check\_flag()



将key与字符进行异或



将异或后结果与target\_str[]进行比对，一致则正确

2、解flag

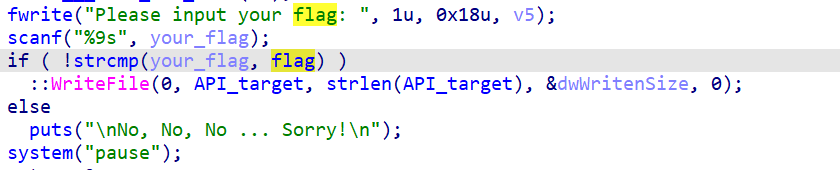
将target\_str[]与key进行异或，即可解出flag。

flag为：

1. CPP\_3 (本题20`)

1、函数分析：

进入main:



将输入字符串与flag进行比对

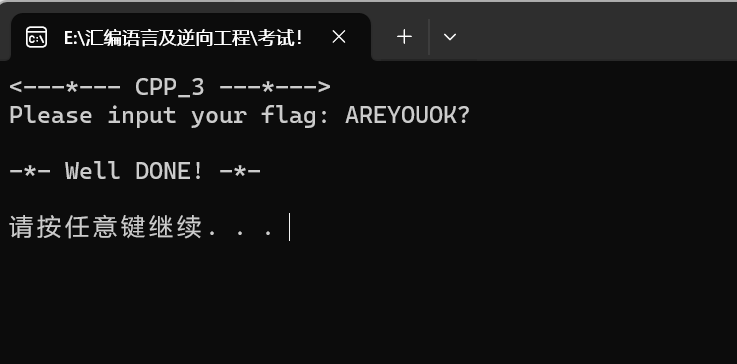
2、解flag:

双击flag:

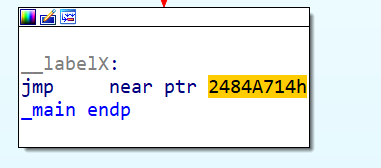


flag为：AREYOUOK?

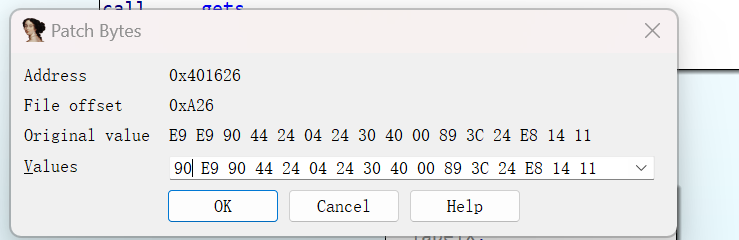
Flag通过：

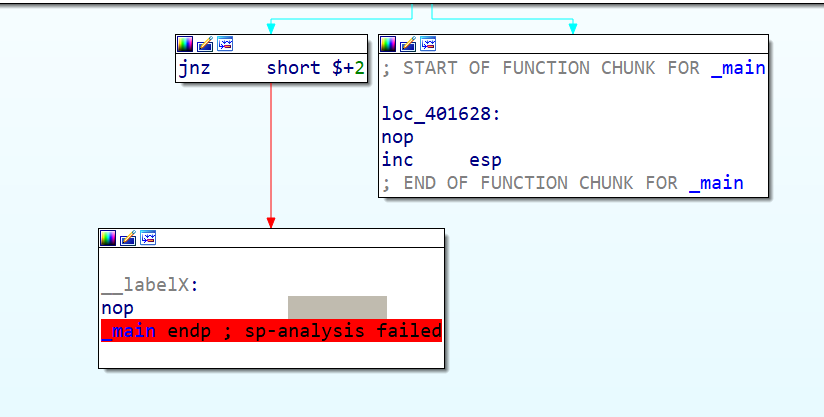


1. CPP\_4 (本题20`)



存在花指令，改成90

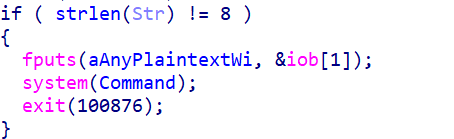




1. CPP\_5 (本题20`)

1、函数分析：

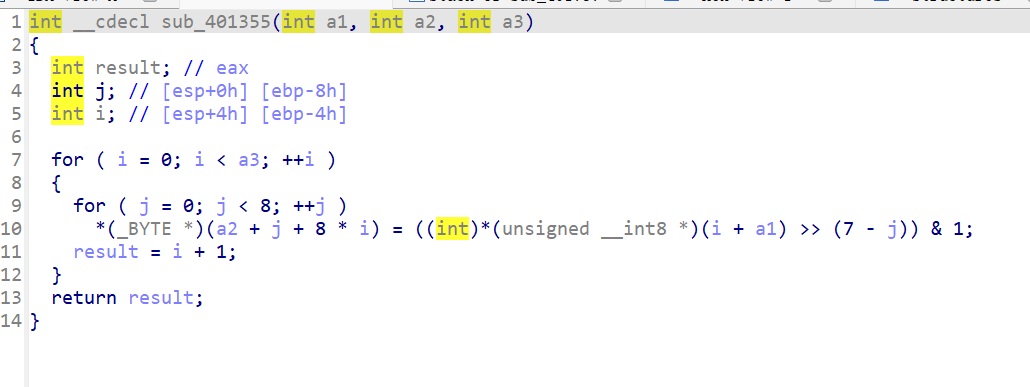
进入main:

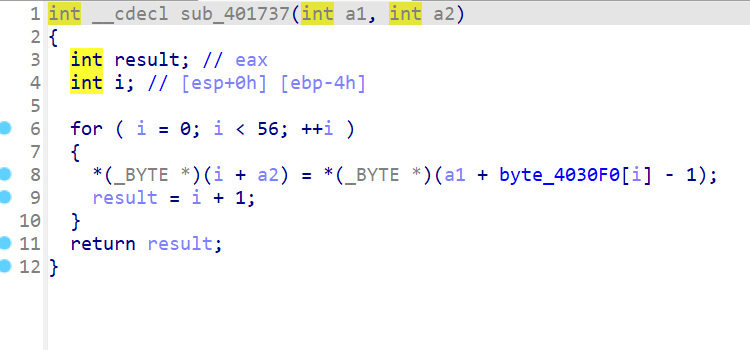


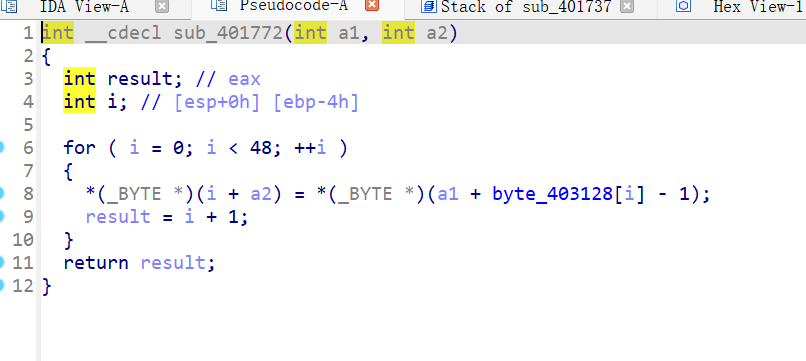
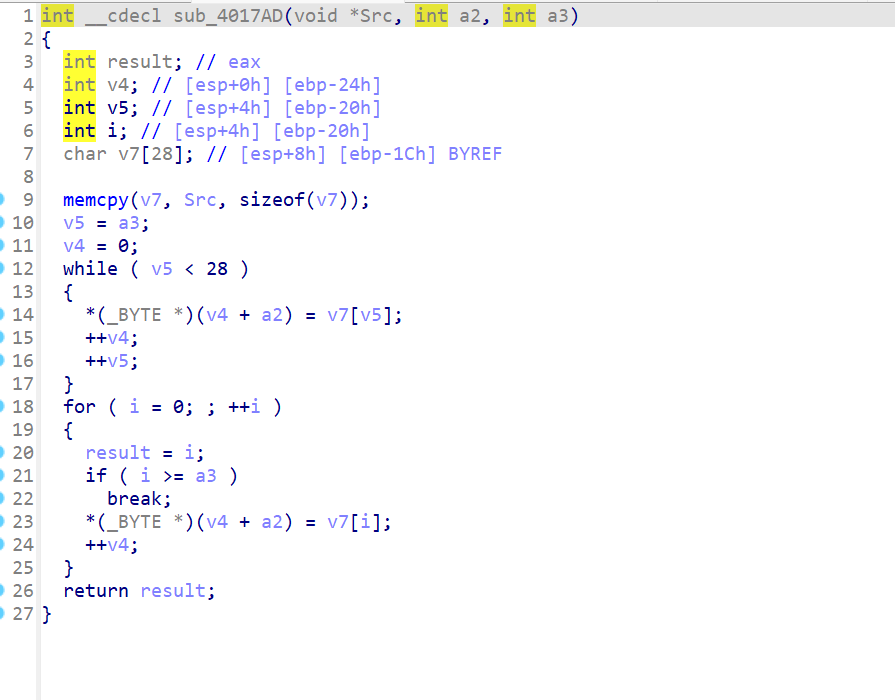
判断字符串长度是否为8，由此可知，flag长度为8

沿着sub\_40100A()进入sub\_401835()

逐步进入sub\_40101E、sub\_401046、sub\_401014、sub\_40100F







可确定该函数为DES算法的密钥编排

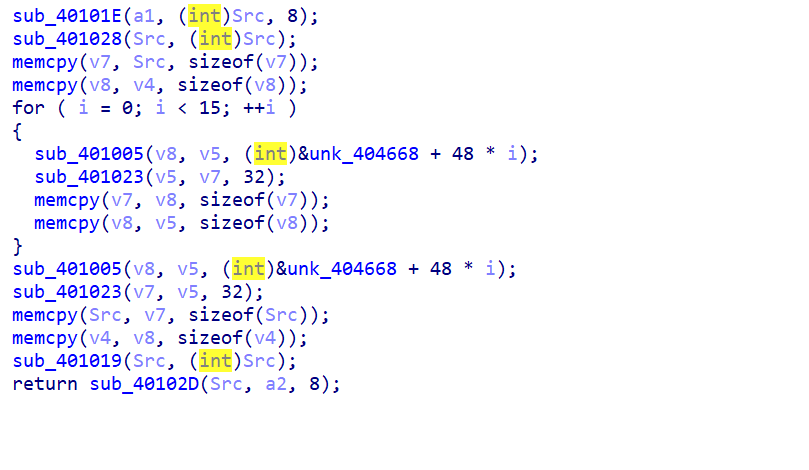


aDesEn1c中存放着密钥，双击进入

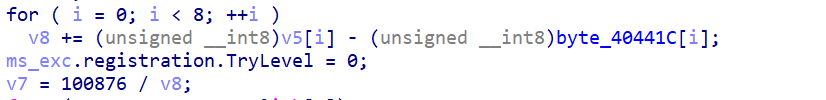


密钥为“DES\_EN1C”

沿着sub\_401032进入sub\_4010B0



可确定为该函数为DES算法的16轮迭代过程



将加密后的字符串，与byte\_40441C处字符串进行逐字符相减

2、解flag:

综上，可知为DES算法，密钥为“DES\_EN1C”，密文为DB 23 D9 EA D0 7A 27 CE，

Flag为：partplan



Flag通过：

