### 北京邮电大学——期末线上机试答题报告

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

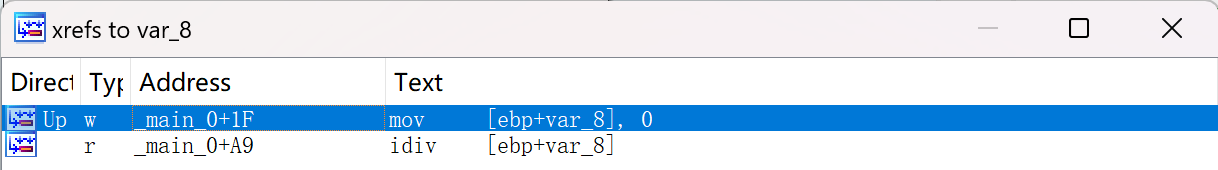
|  |  |
| --- | --- |
| **学院** | 网络空间安全学院 |
| **专业** | 信息安全 |
| **班级** |  |
| **姓名** |  |
| **学号** |  |
| **座位号** |  |
| **考核科目** | 汇编语言与逆向工程 |
| **考核方式** | 线上机试、开卷 |

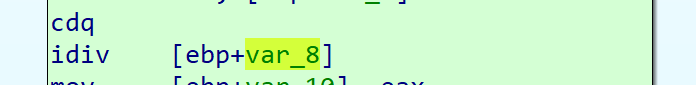
**2023年06月21日（上午） 10:00—12:00**

**（09:55—11:55，应试电脑需全程断网）**

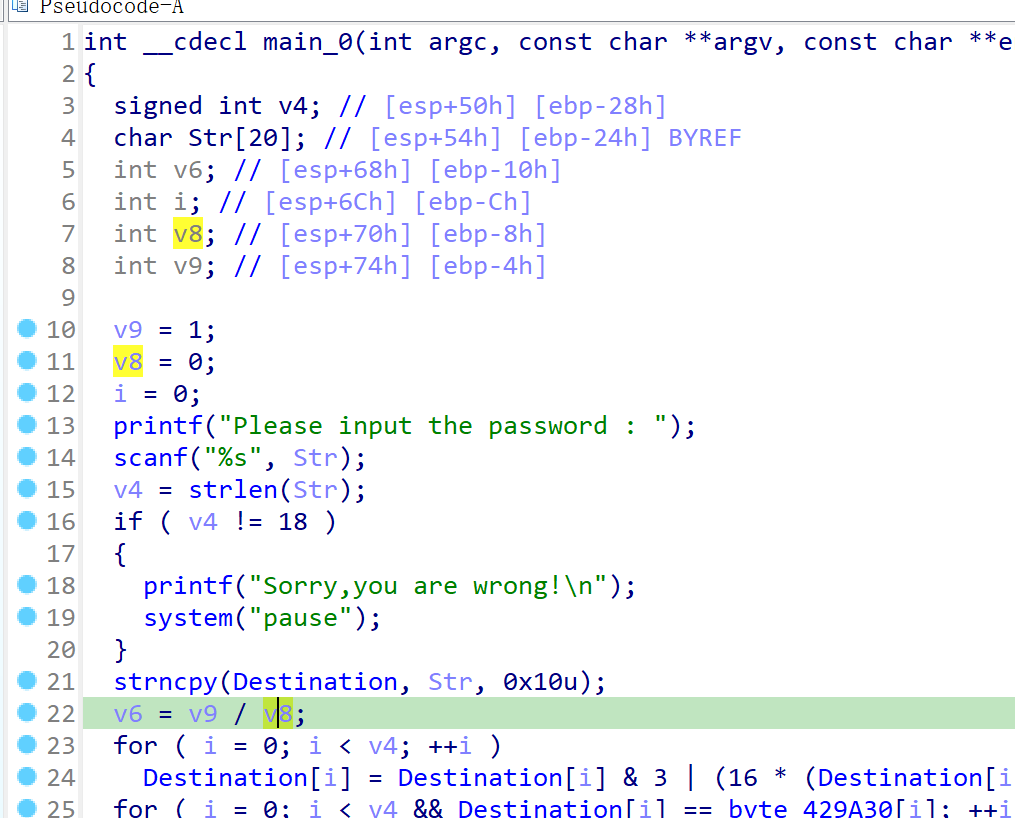
1. 题目1 (本题20`)

除零错误：



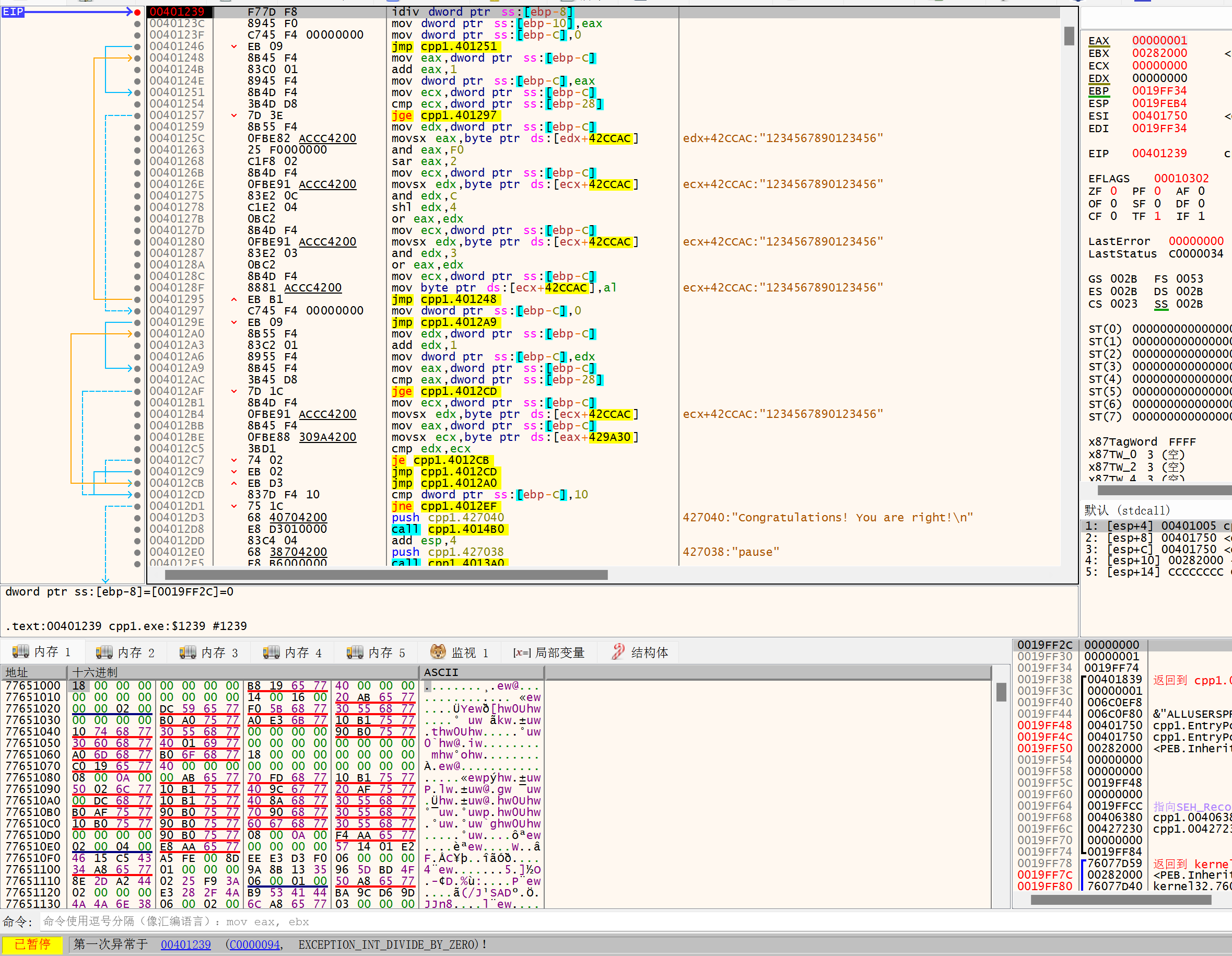


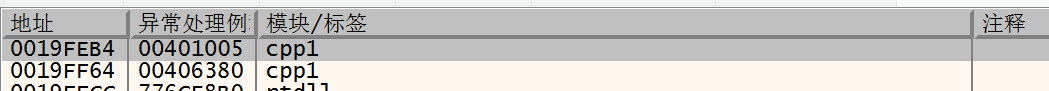
可看出在除0错误前将输入的前16位传给了destination：

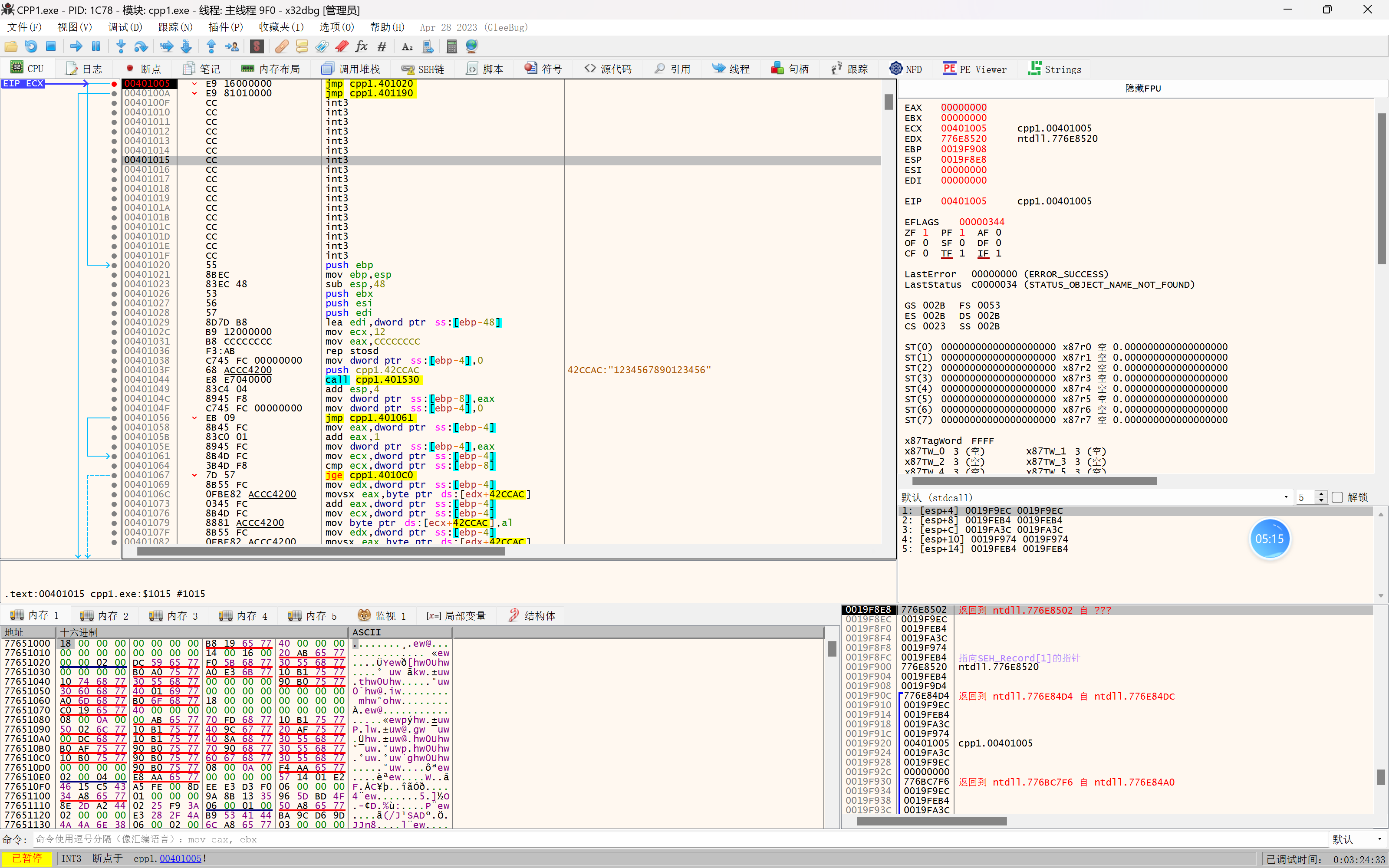


异常处理：

找到异常处理的函数地址：

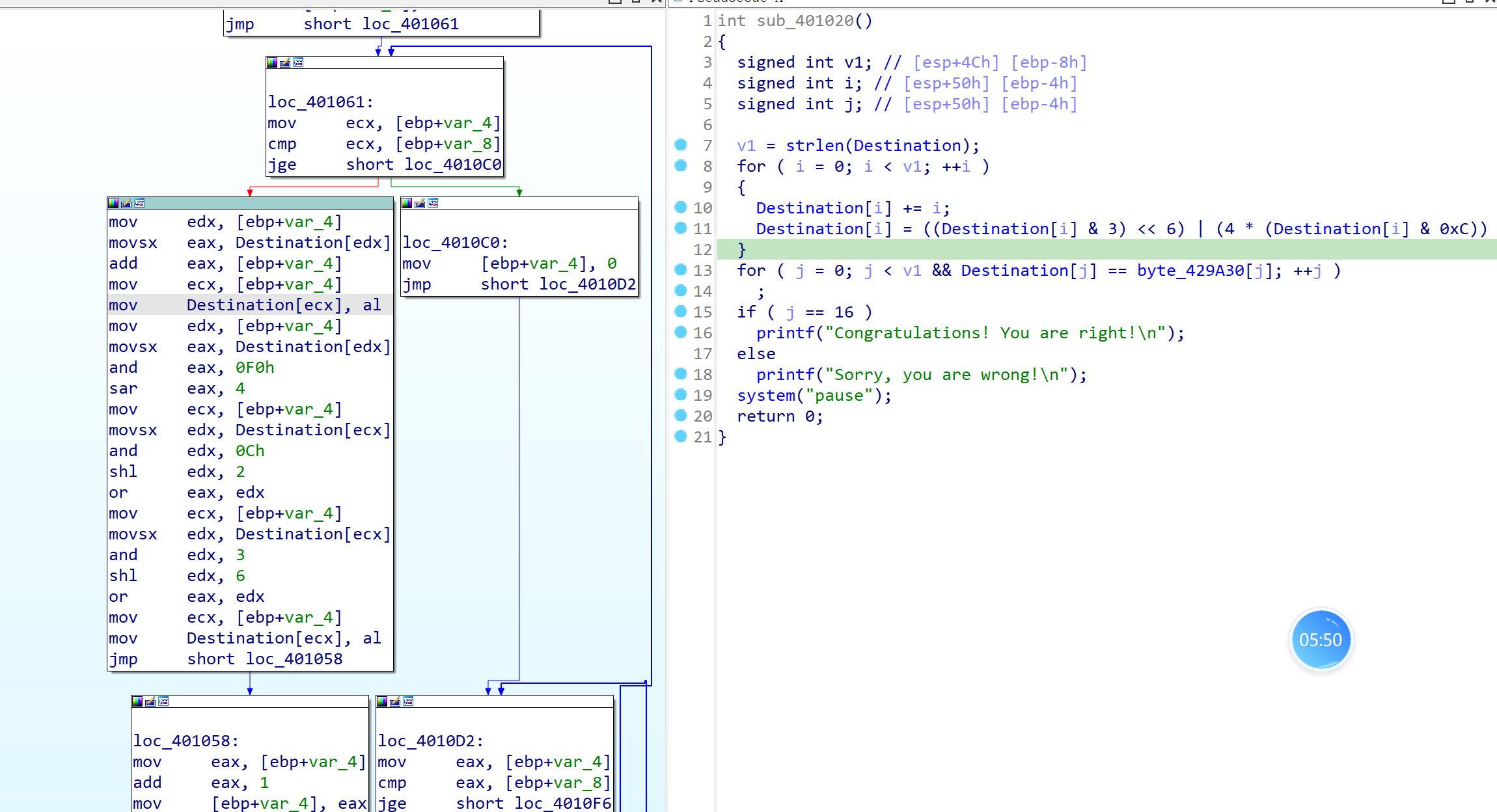




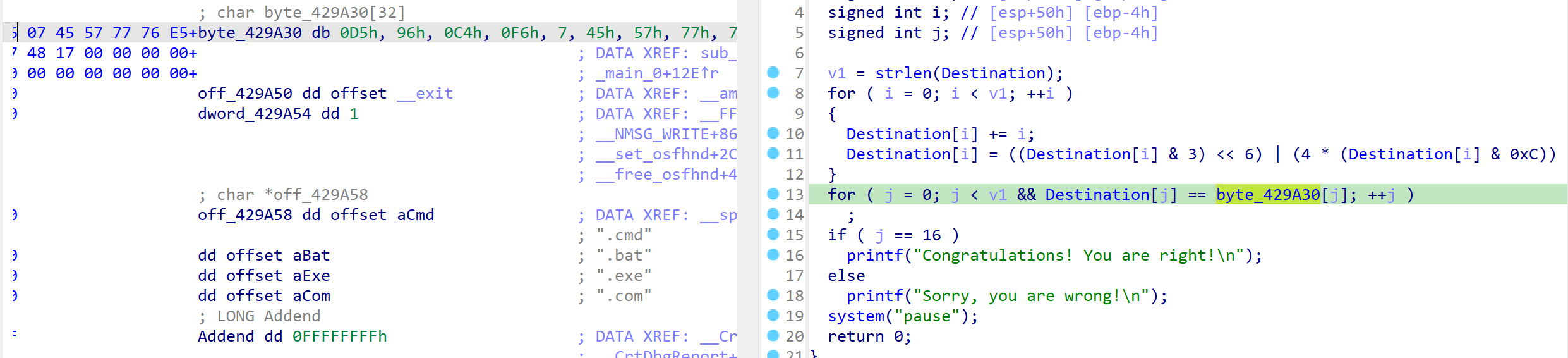


转为分析异常处理函数：

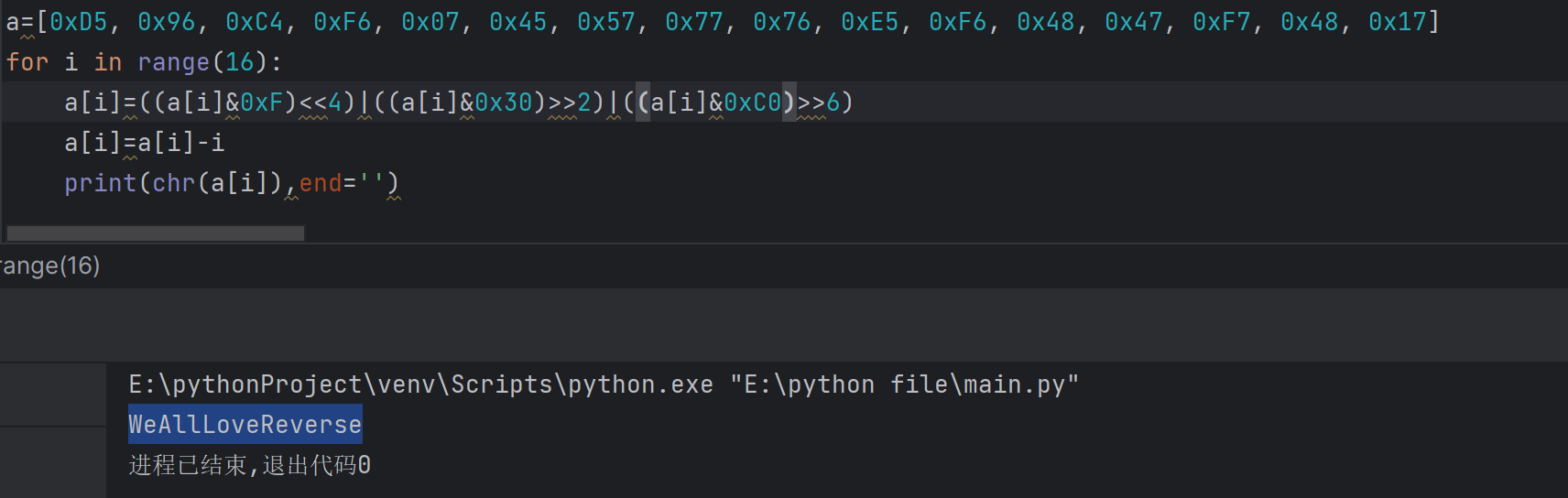
既输入处理后的前16位输入要和密钥相同：



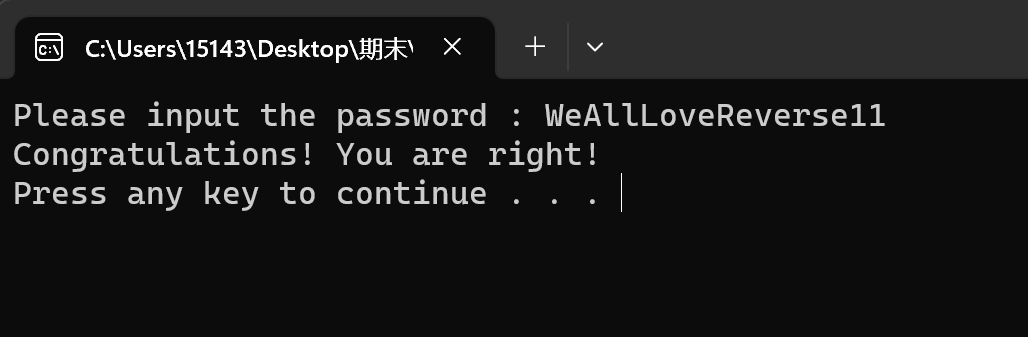
分析得出为一个简单的字节内位置变化，找到密文：



编制程序解出密钥为：

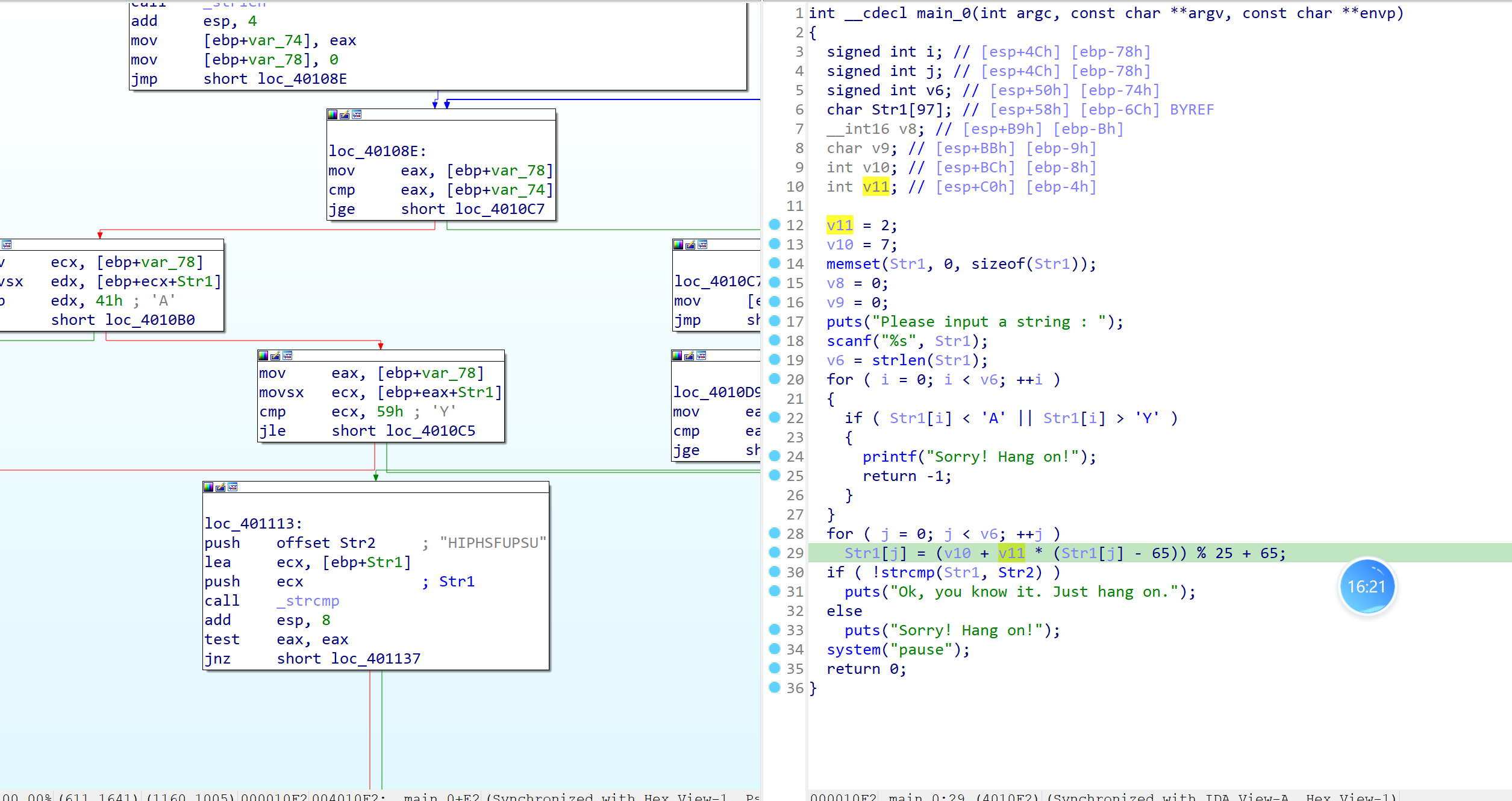


增加两位使其长度为18即可，则可得密钥为WeAllLoveReverse\*\*，由于没有输入判断，\*可为任意可输入字符：

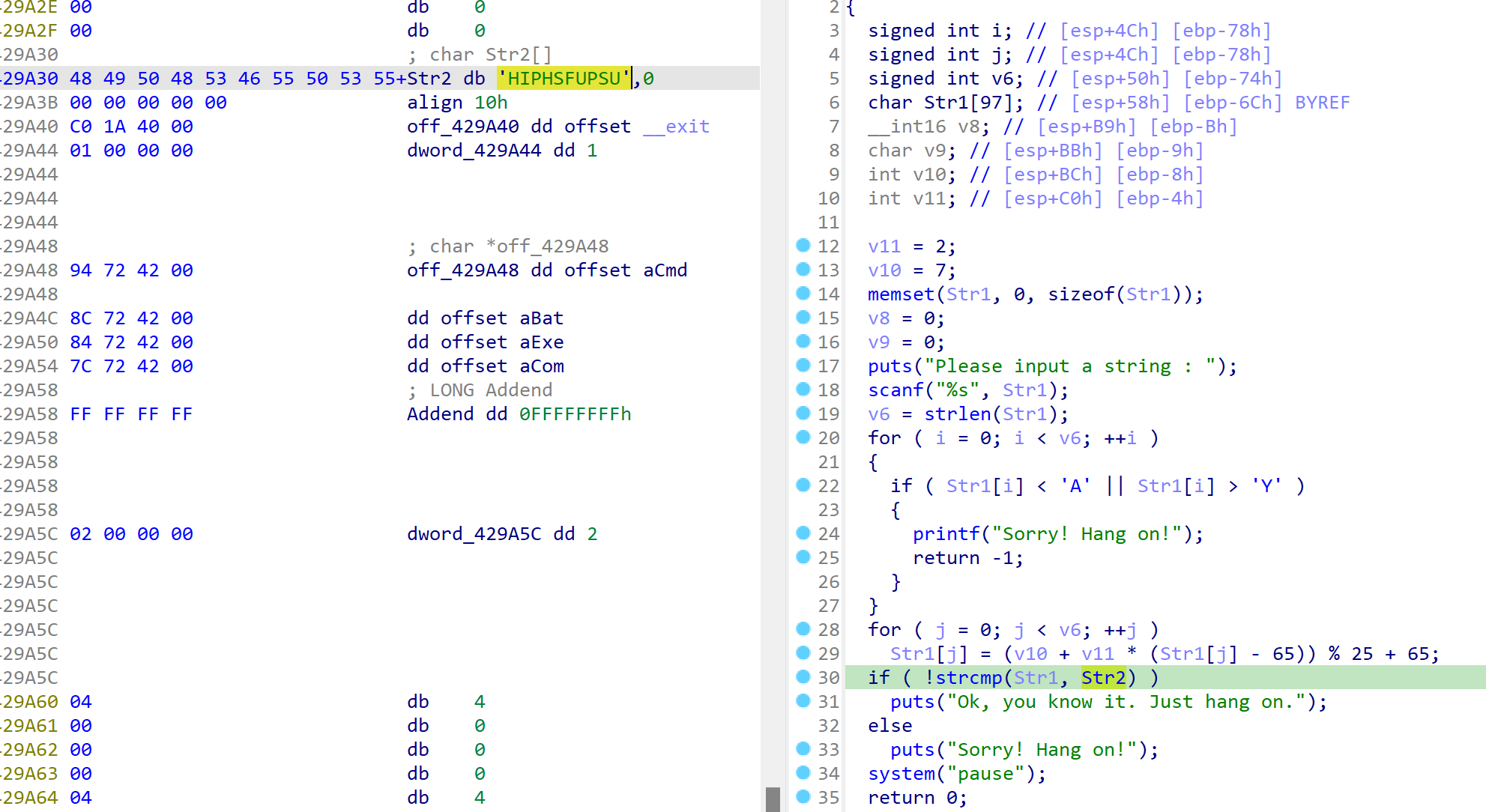


1. 题目2 (本题20`)

第二题为一个仿射密码，密钥分别是2和7，而且不是取模26而是取模25，而且有输入判断，必须是大写字母



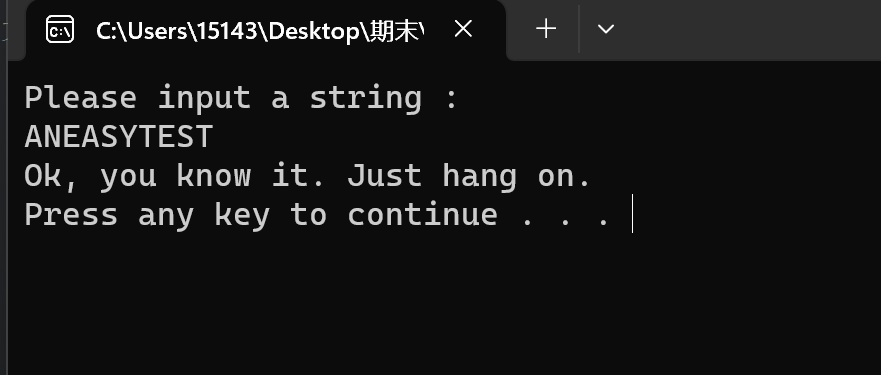
找出仿射后的密码：



编写脚本，解出密钥：

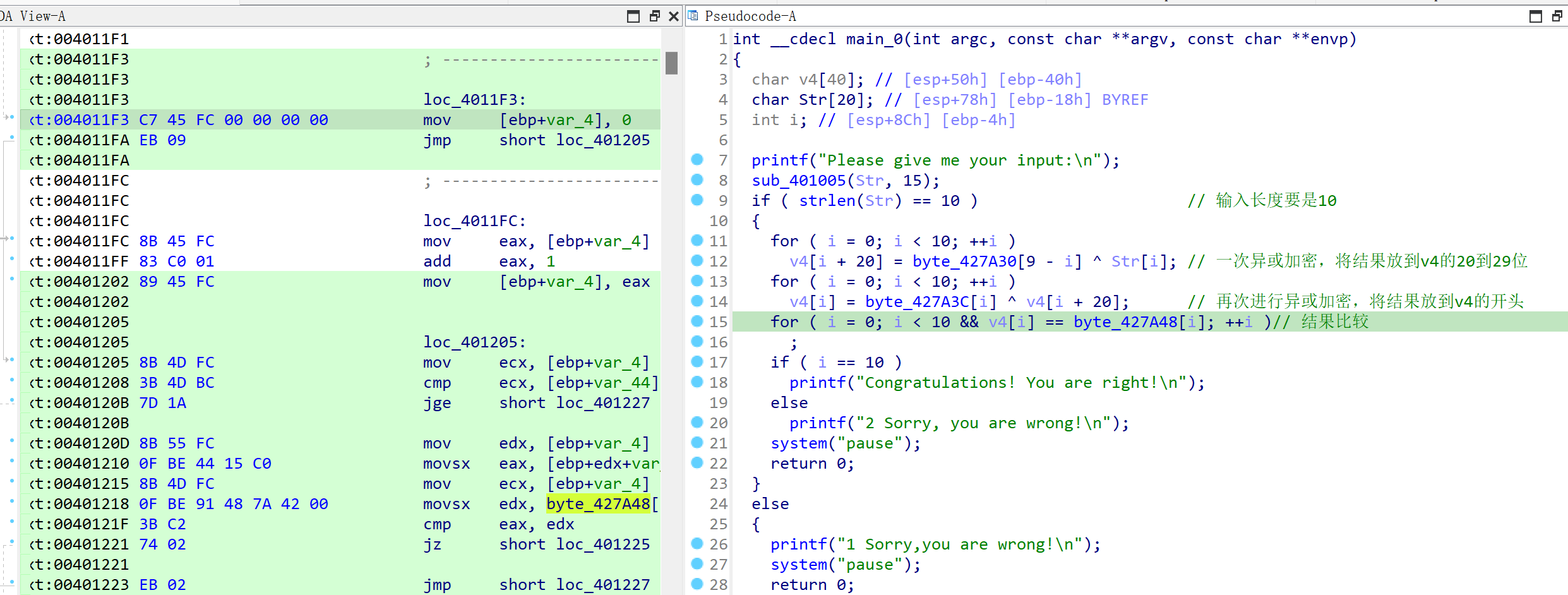


得密钥为ANEASYTEST

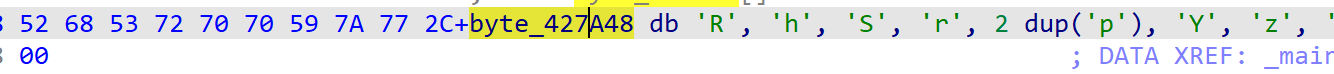


1. 题目3 (本题20`)

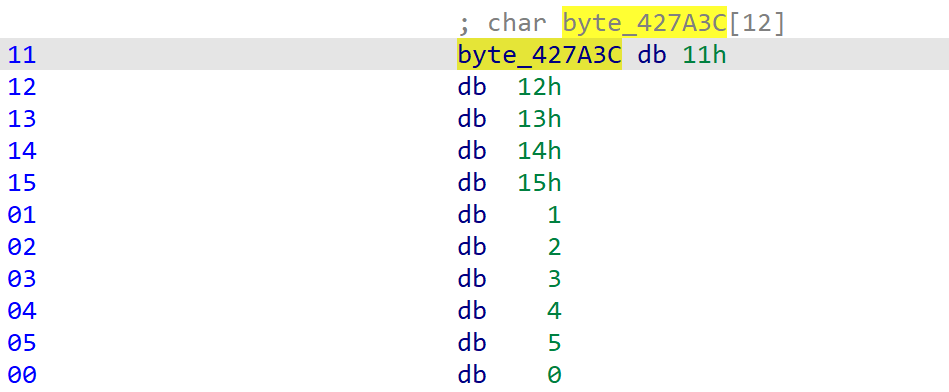
如图注释，第三题就是将长度为10的输入进行两次异或加密后和密钥进行比较：



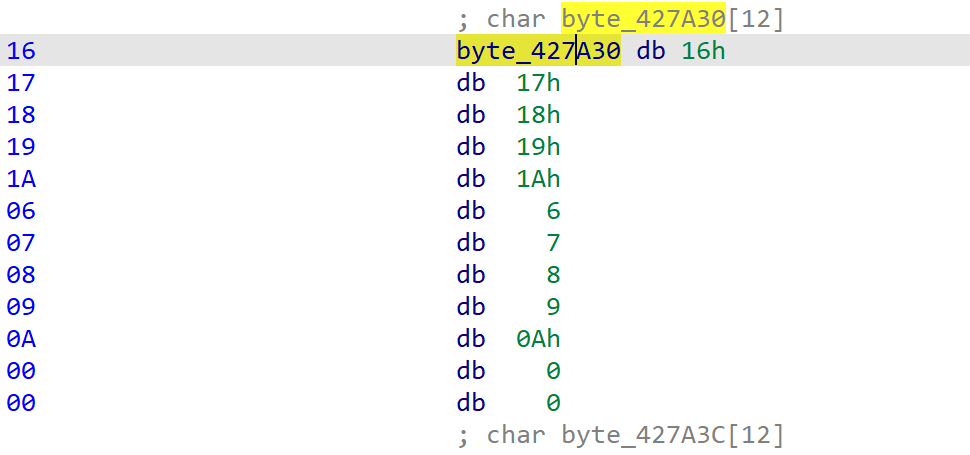
加密后的密文：



二次异或：



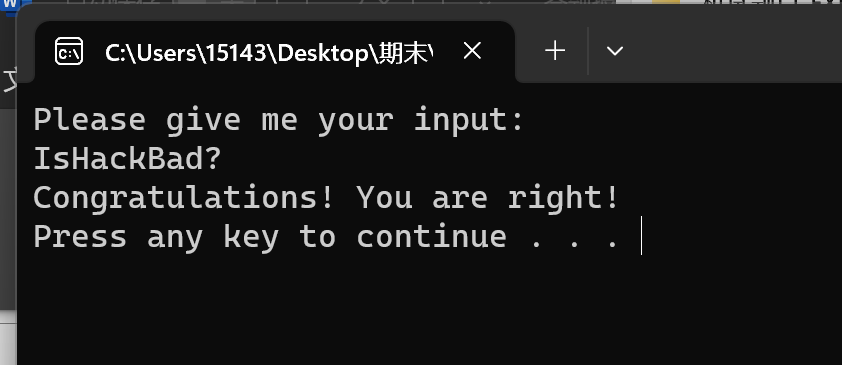
一次异或（顺序还得反过来，因为异或的9-i）：



编写脚本进行解密：



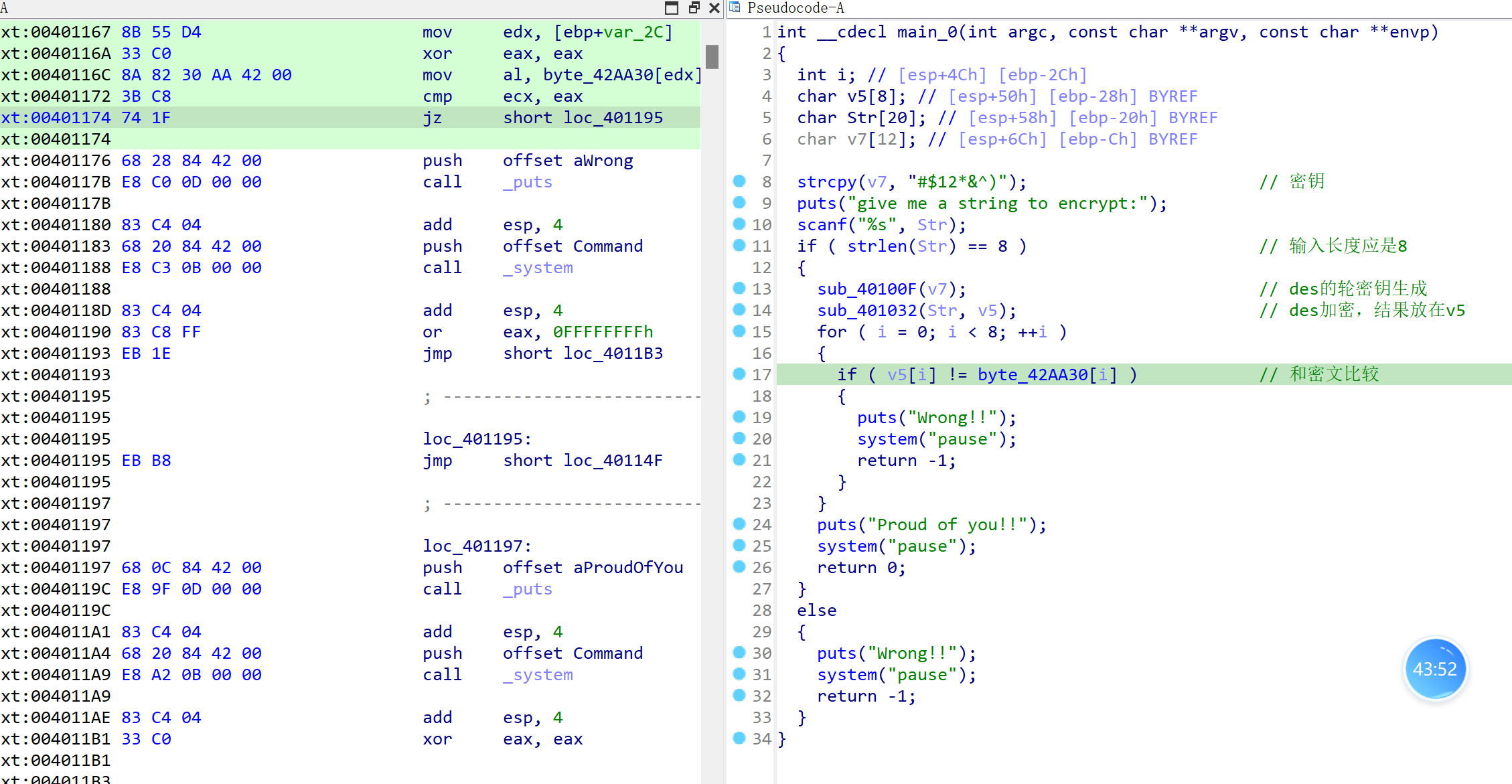
得密钥为IsHackBad?



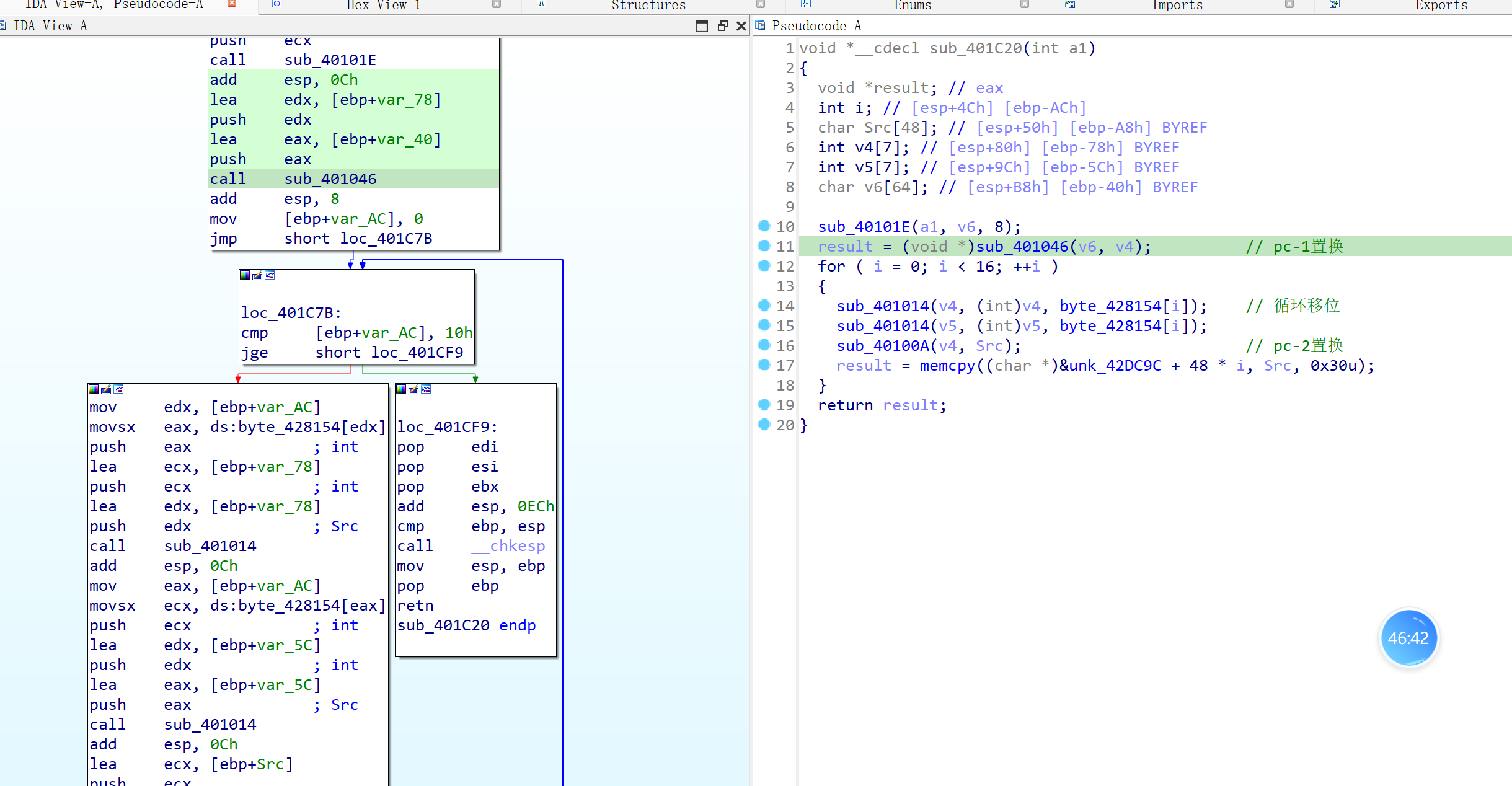
1. 题目4 (本题20`)

分析得出该题为DES加密

如图所示，函数整体结构：

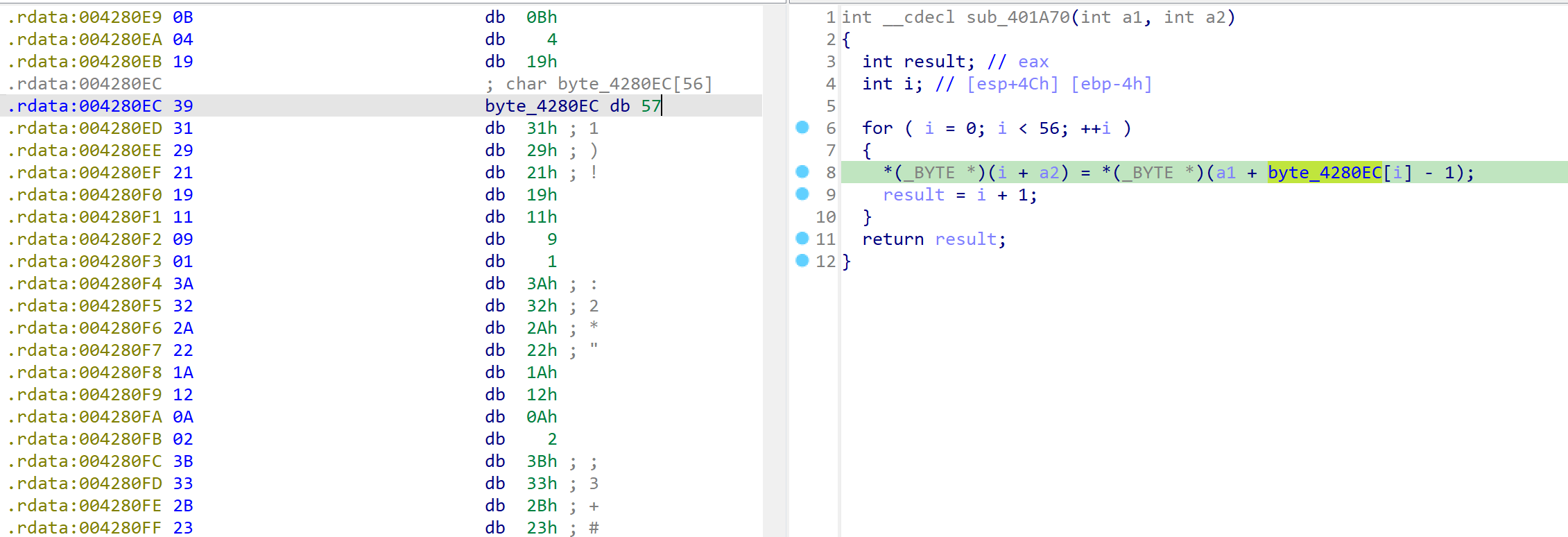


首先分析轮密钥生成函数，其整体结构如下：

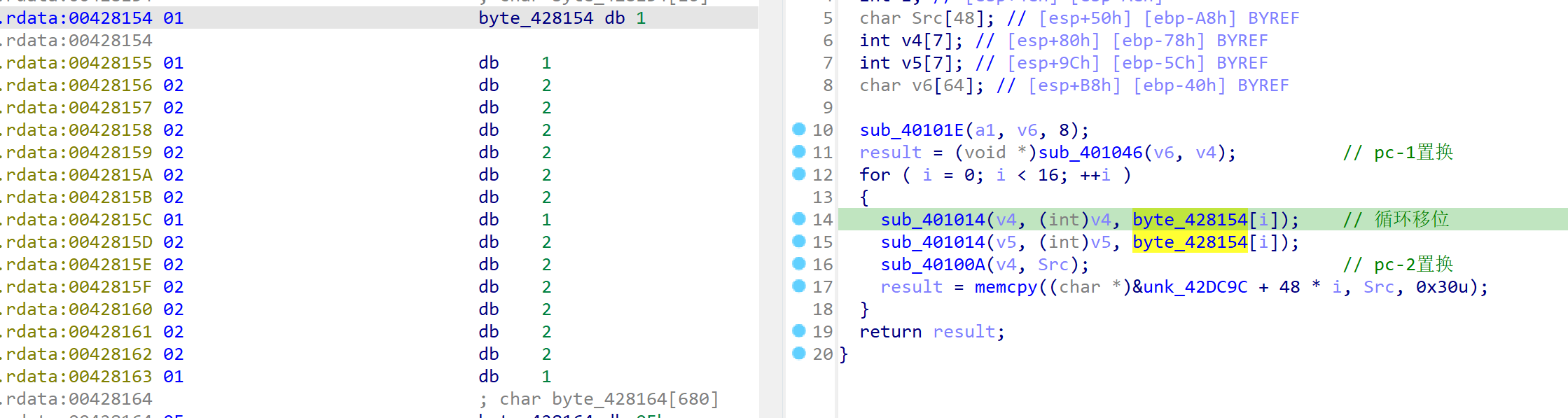


具体证据如：

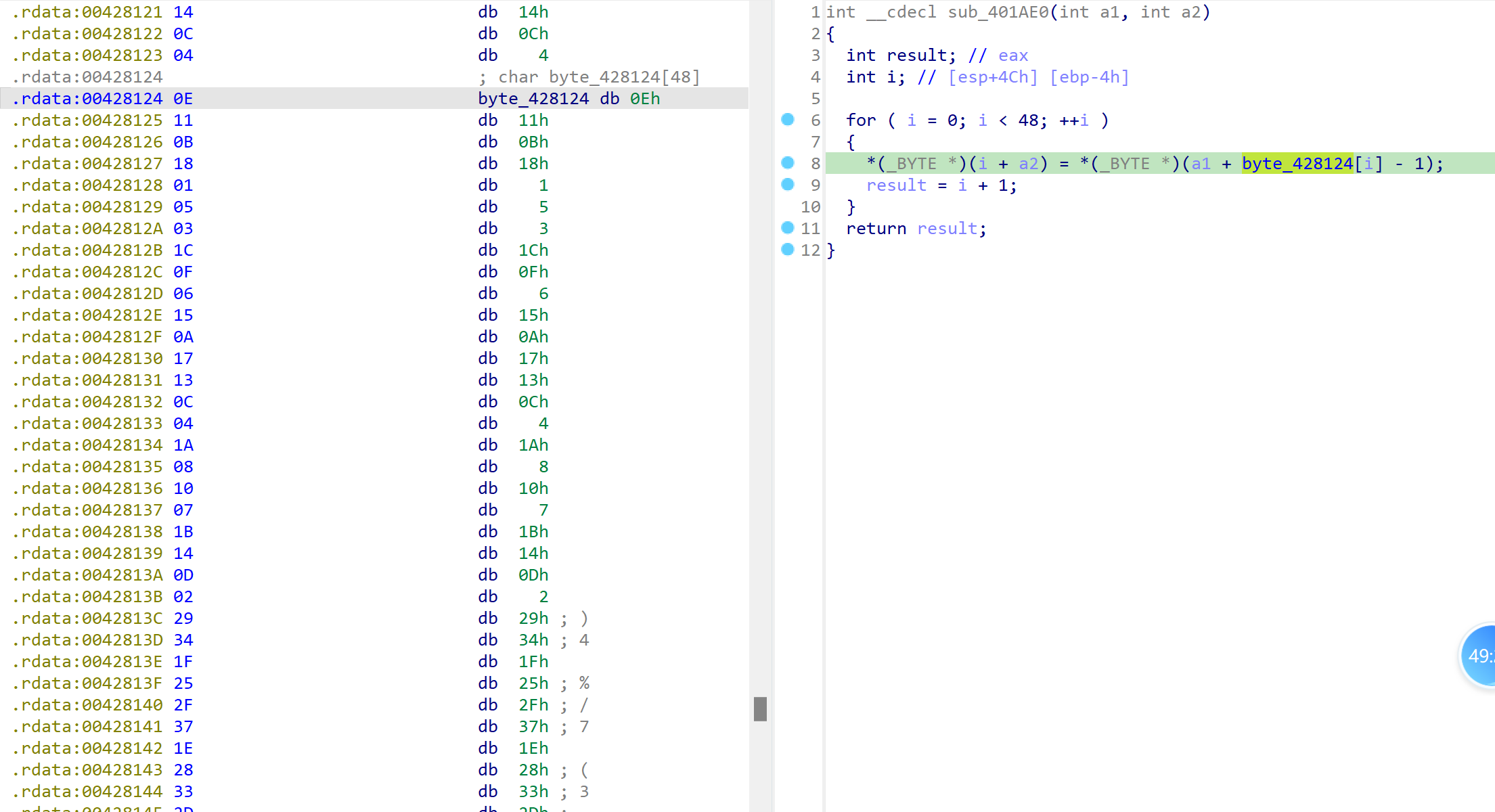
Pc-1置换函数中的pc-1盒：



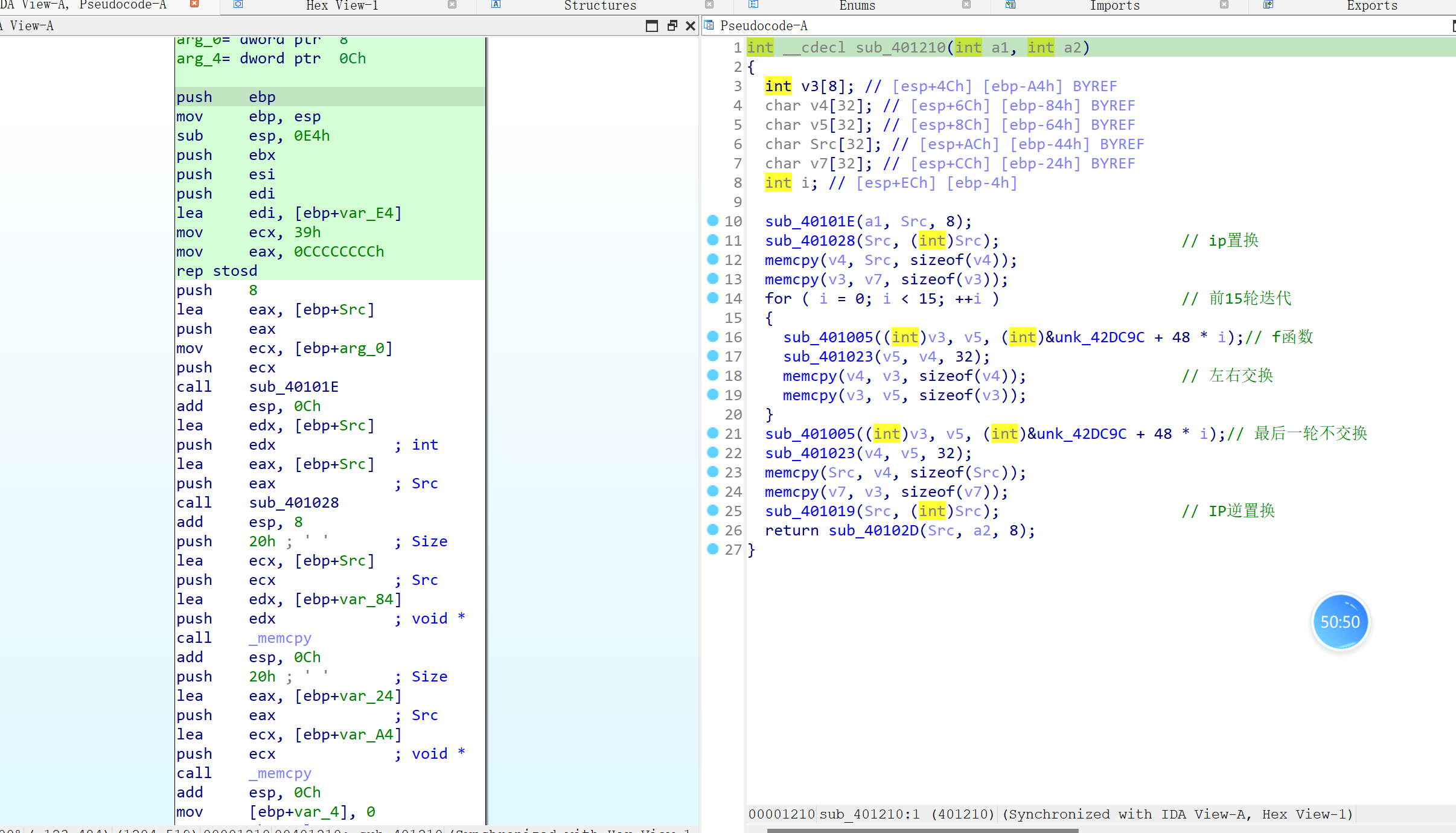
循环移位中记录每次循环移位位数的数组：



Pc-2置换中的pc-2盒:

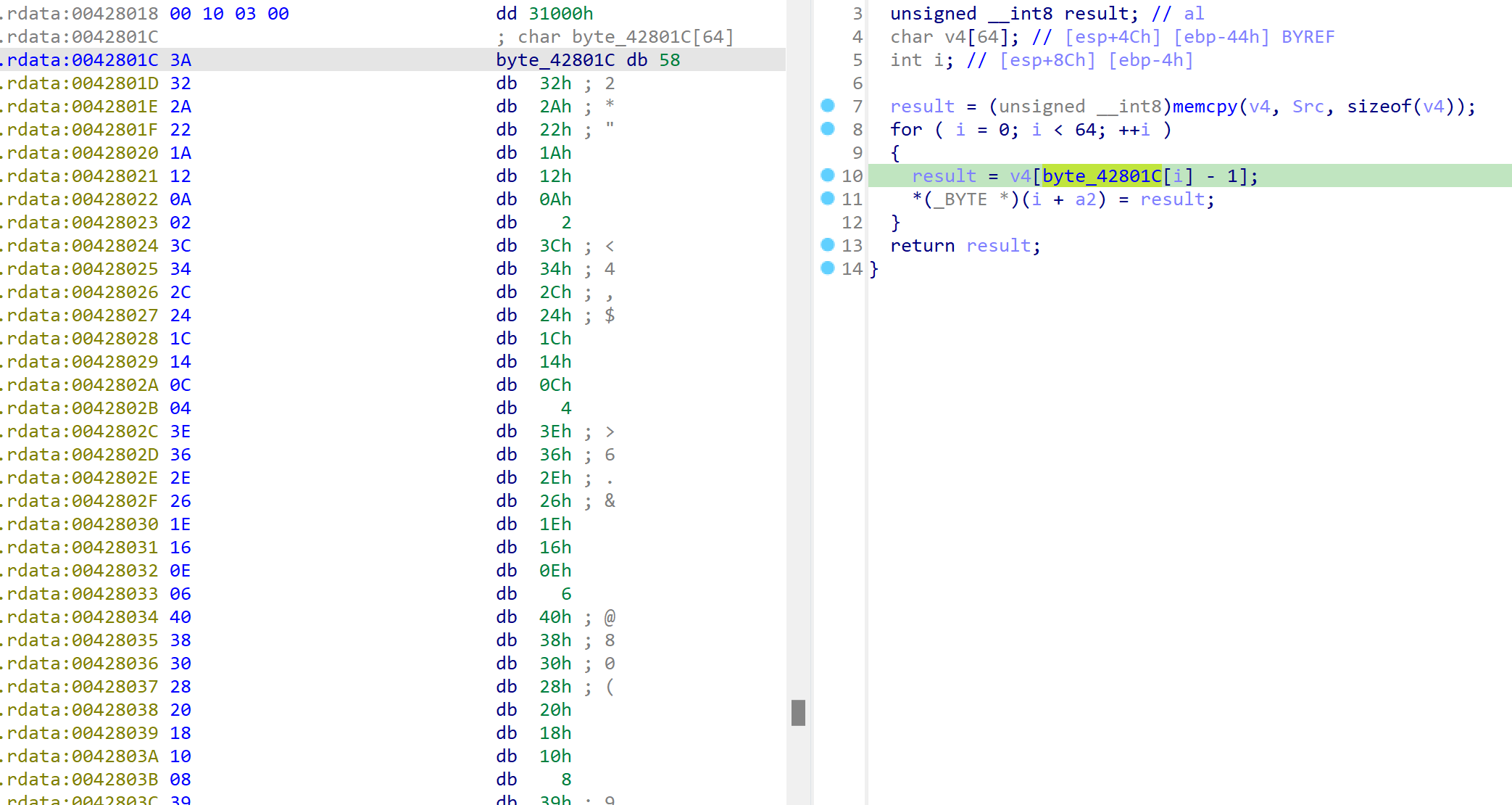


然后分析des加密函数，其整体结构如下：

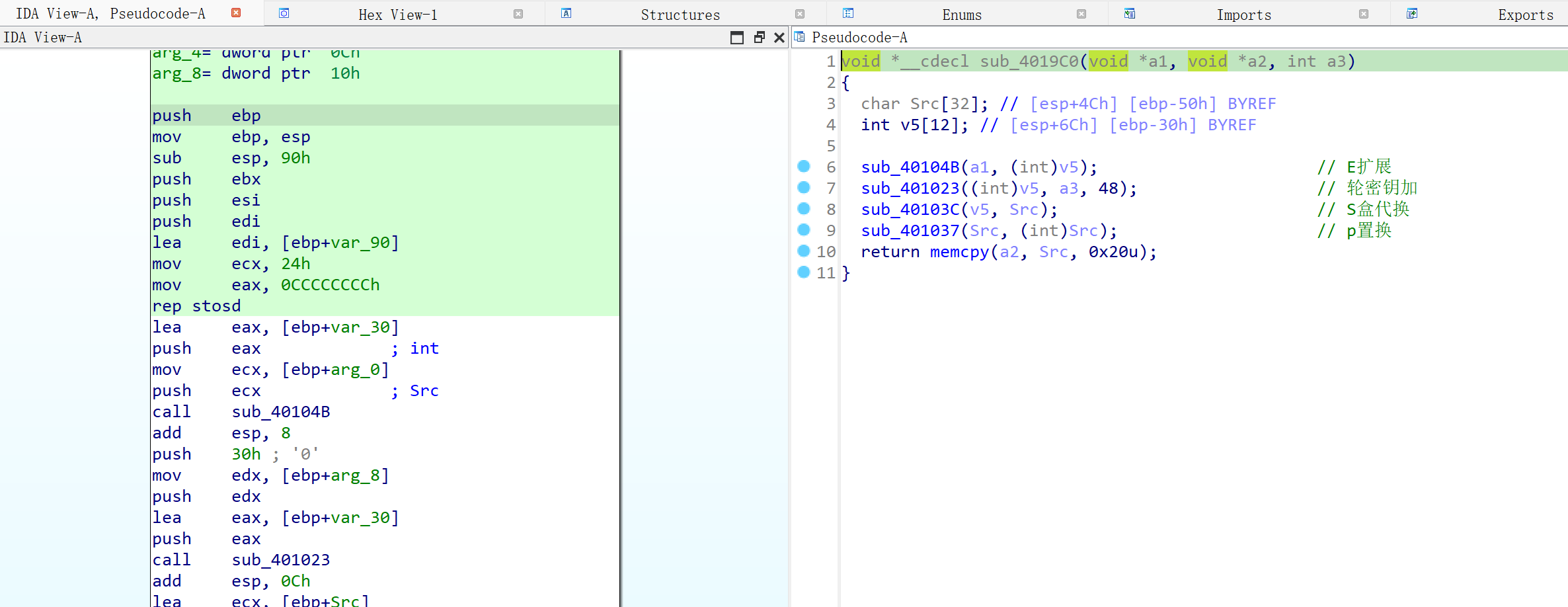


证据有：

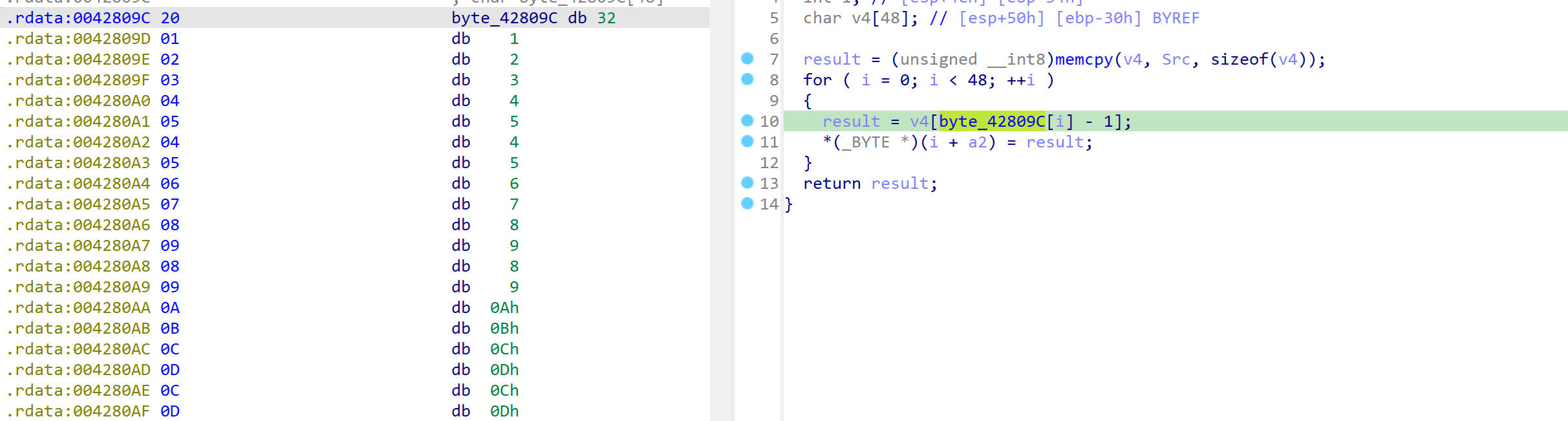
IP置换的ip盒



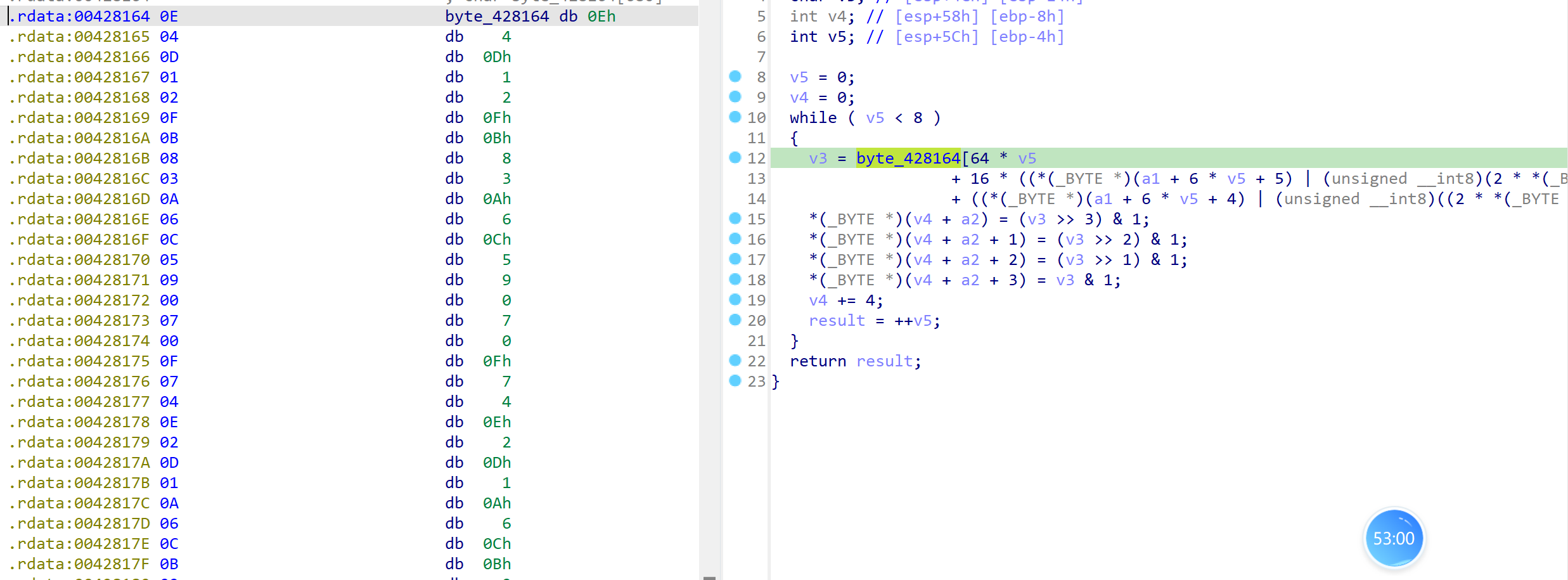
F函数中的4步：



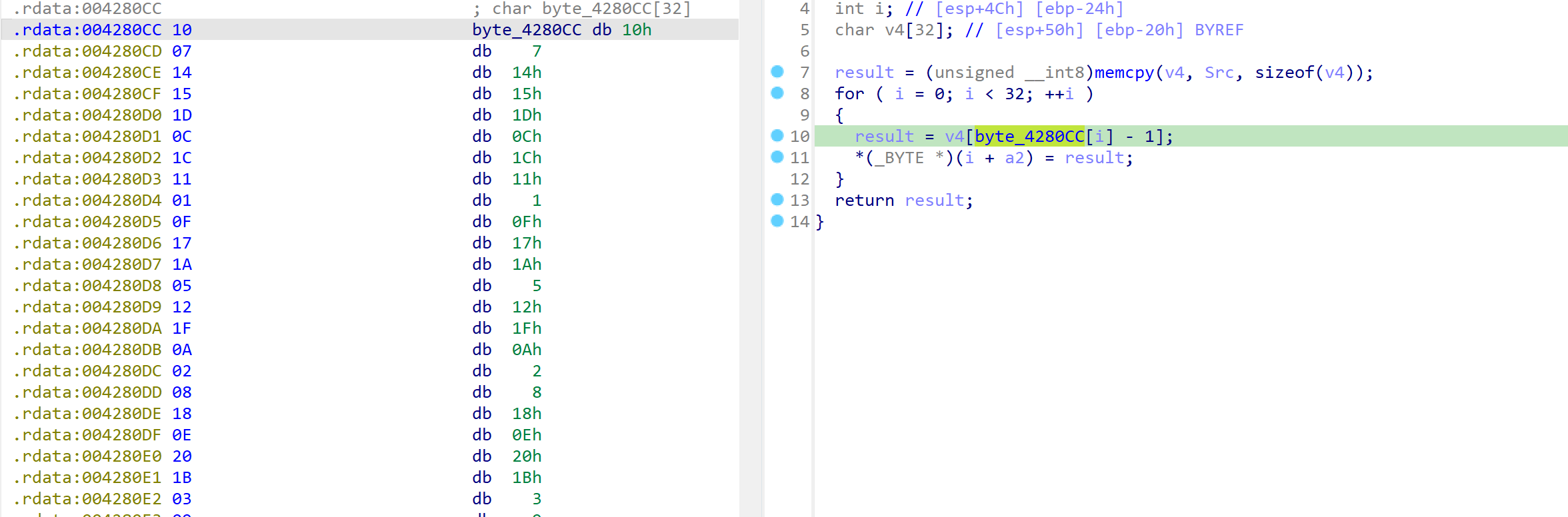
E扩展中的E盒：



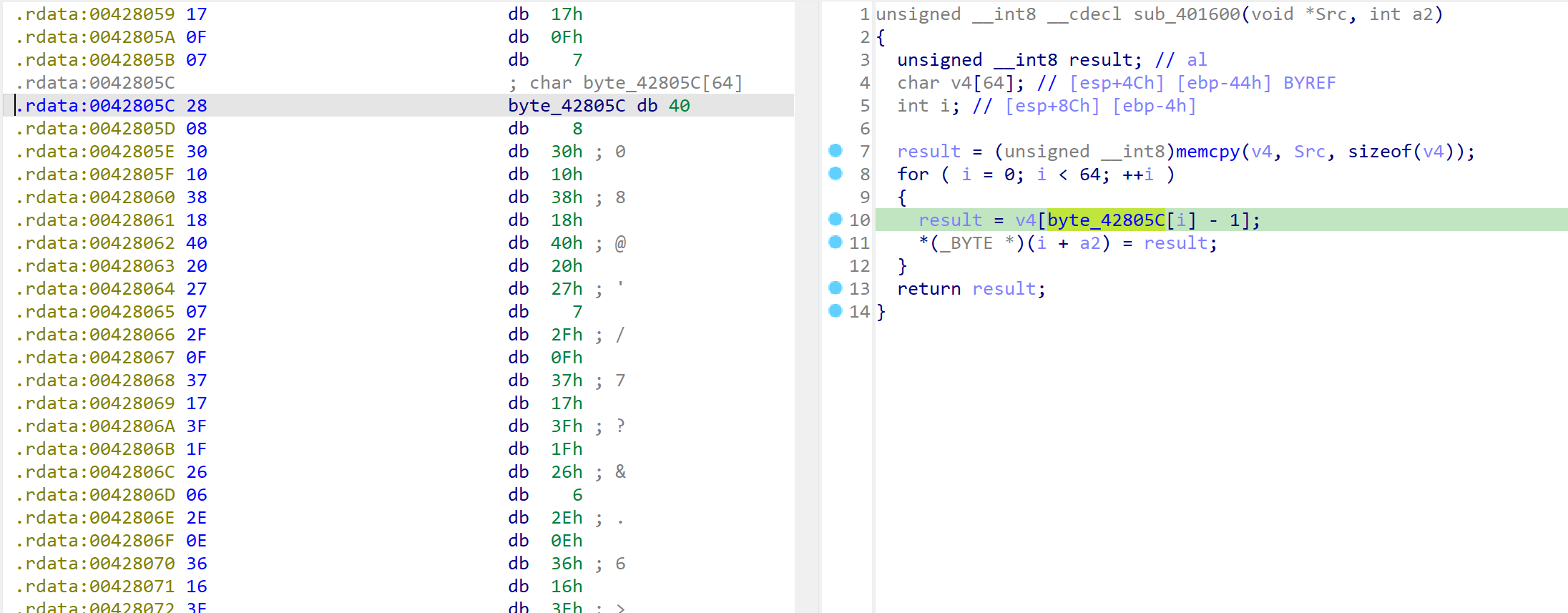
S代换中的S盒：



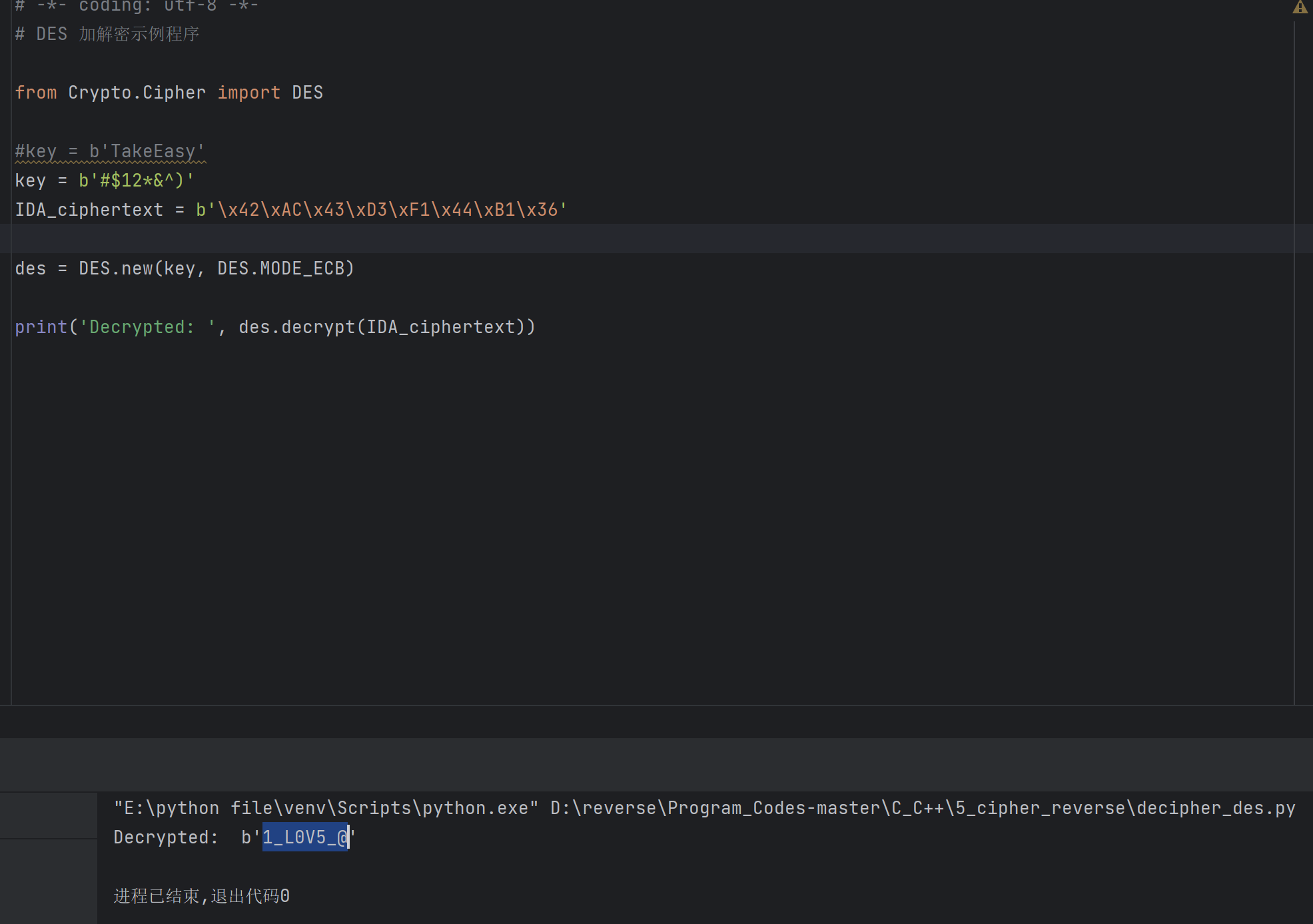
P代换中的p盒：



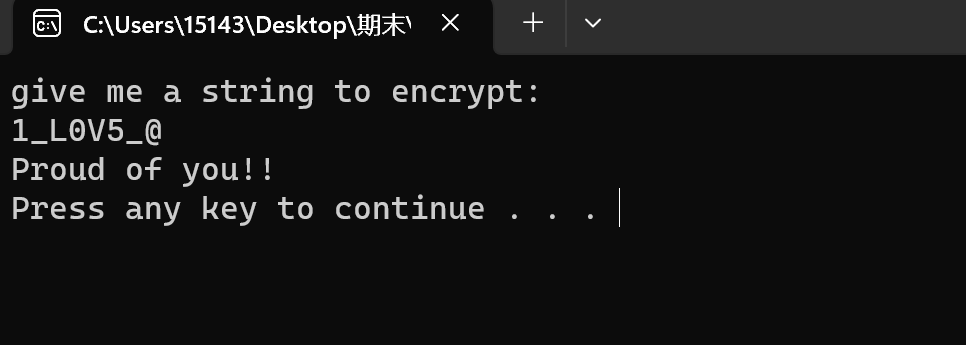
以及最后IP逆置换中的逆IP盒：



分析完毕，输入脚本进行解密：

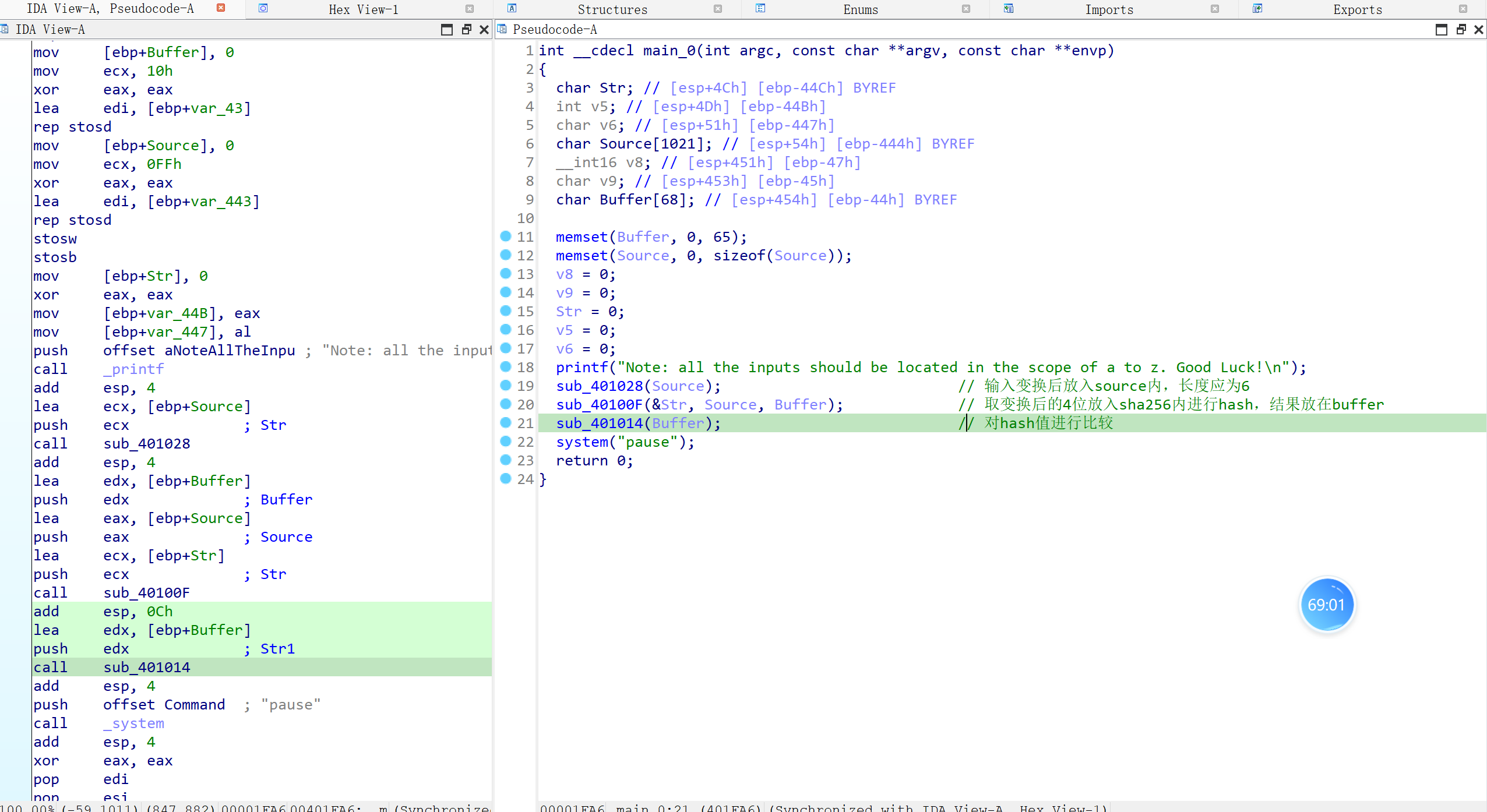


得密钥为：1\_L0V5\_@



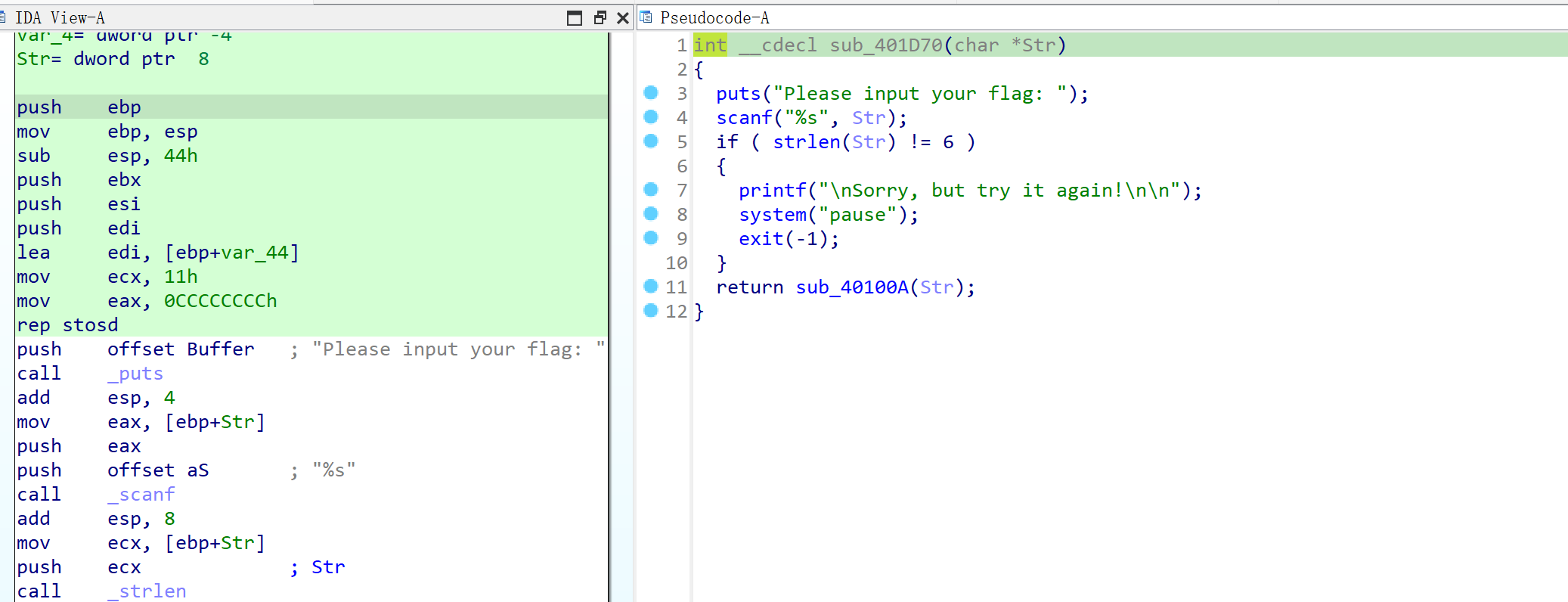
1. 题目5 (本题20`)

首先观察程序主体结构：



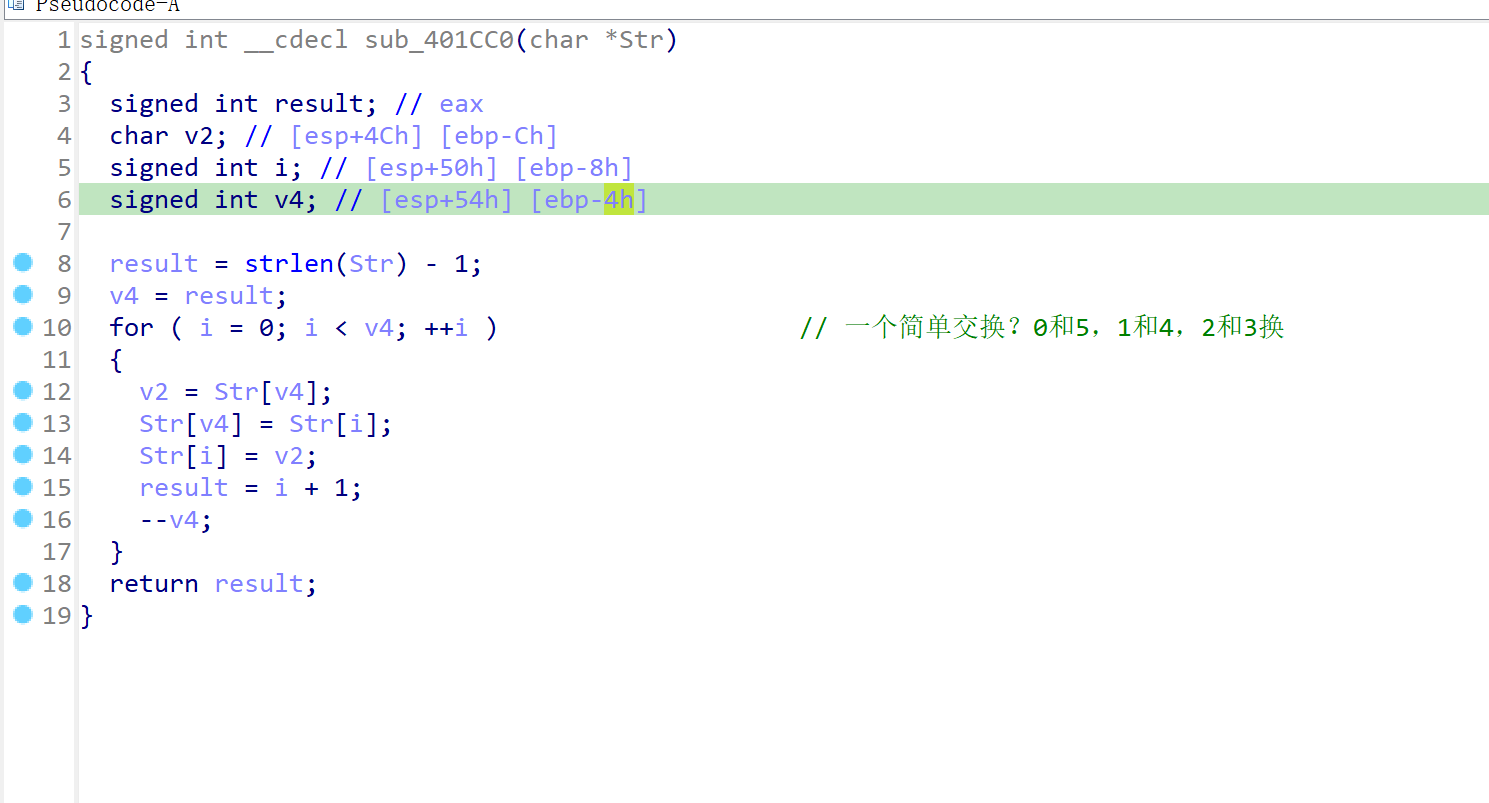
进入第一个函数内：

发现其将输入放在了str中，输入必须为6位，并返回了一个带str的函数：



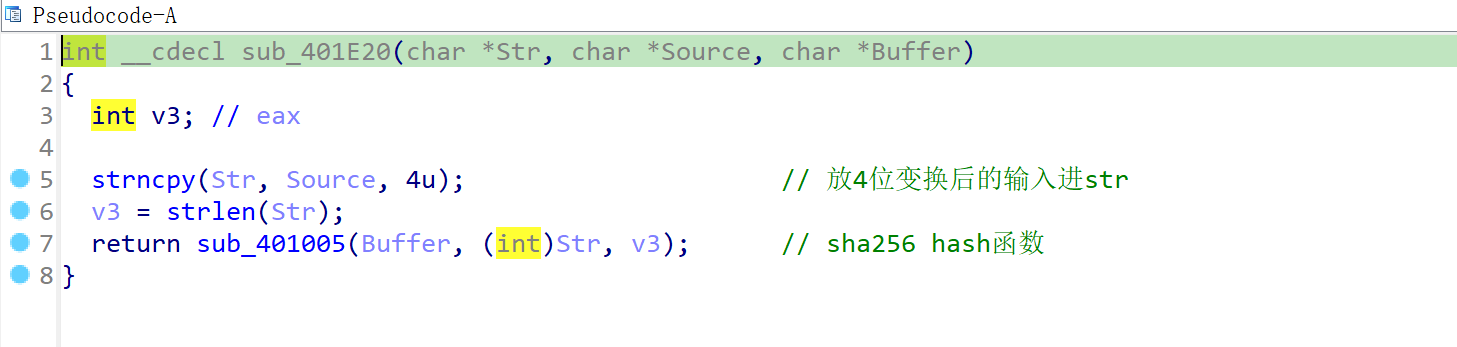
查看其返回的函数：

发现其就是一个简单的交换，将输入的第0位和第5位，第1位和第4位，第2位和第三位交换：



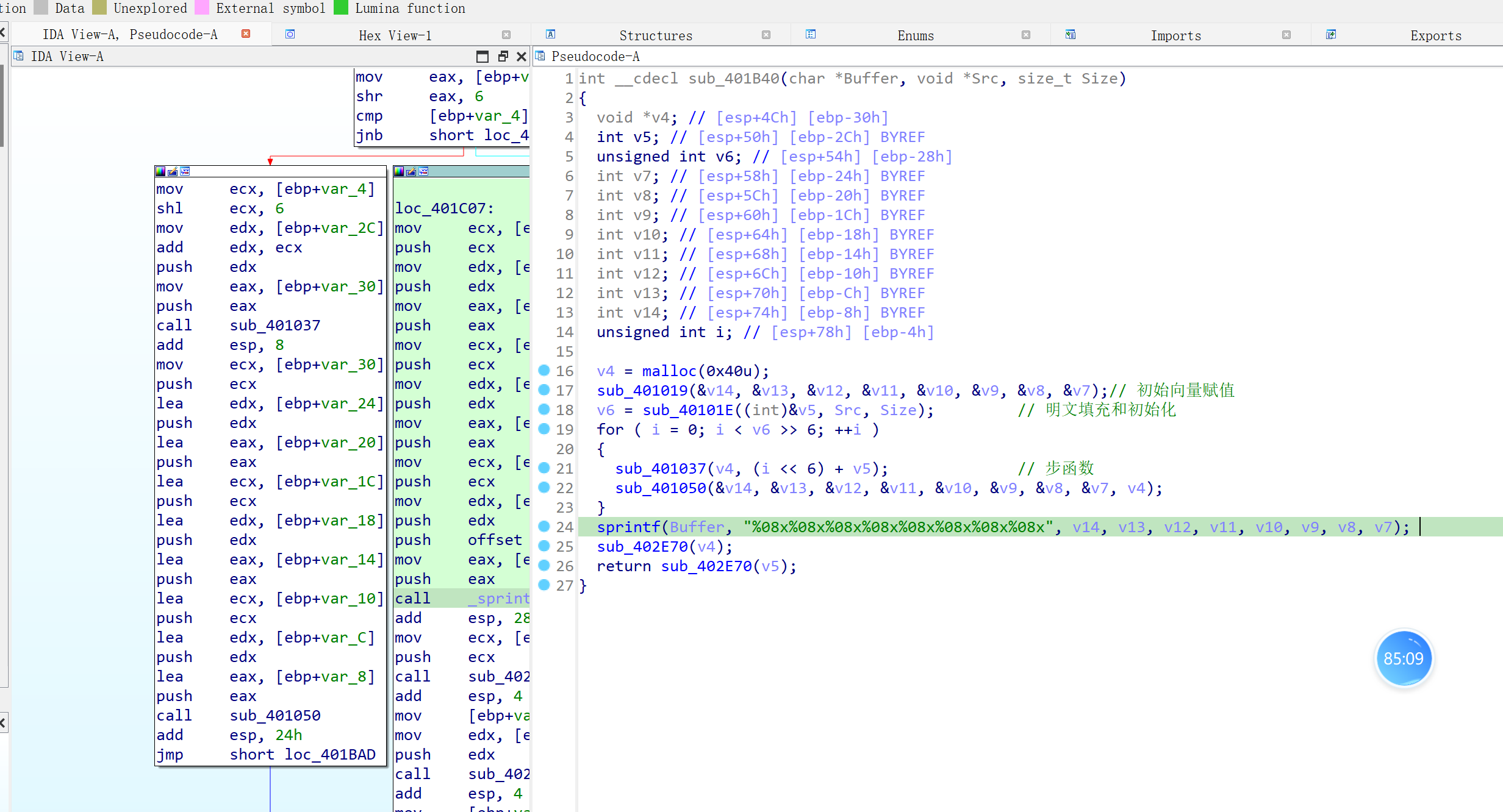
其最终结果就是在最外层返回的Source中是已经被交换过位置的输入

查看第二个主要函数：



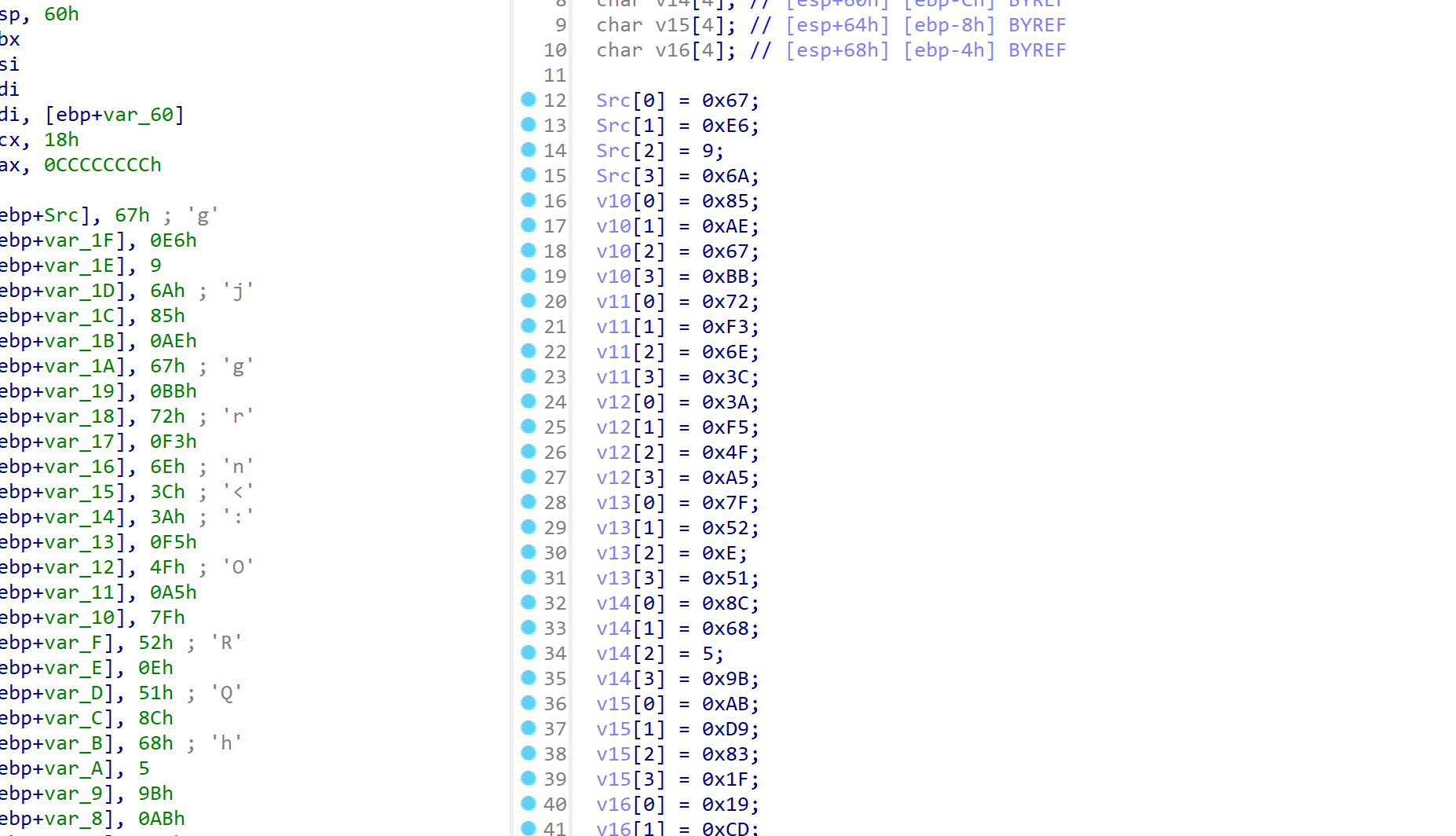
其将变换后输入的前4位放进了str

并将其传入一个函数内，经后续分析可知其为sha-256 hash函数：

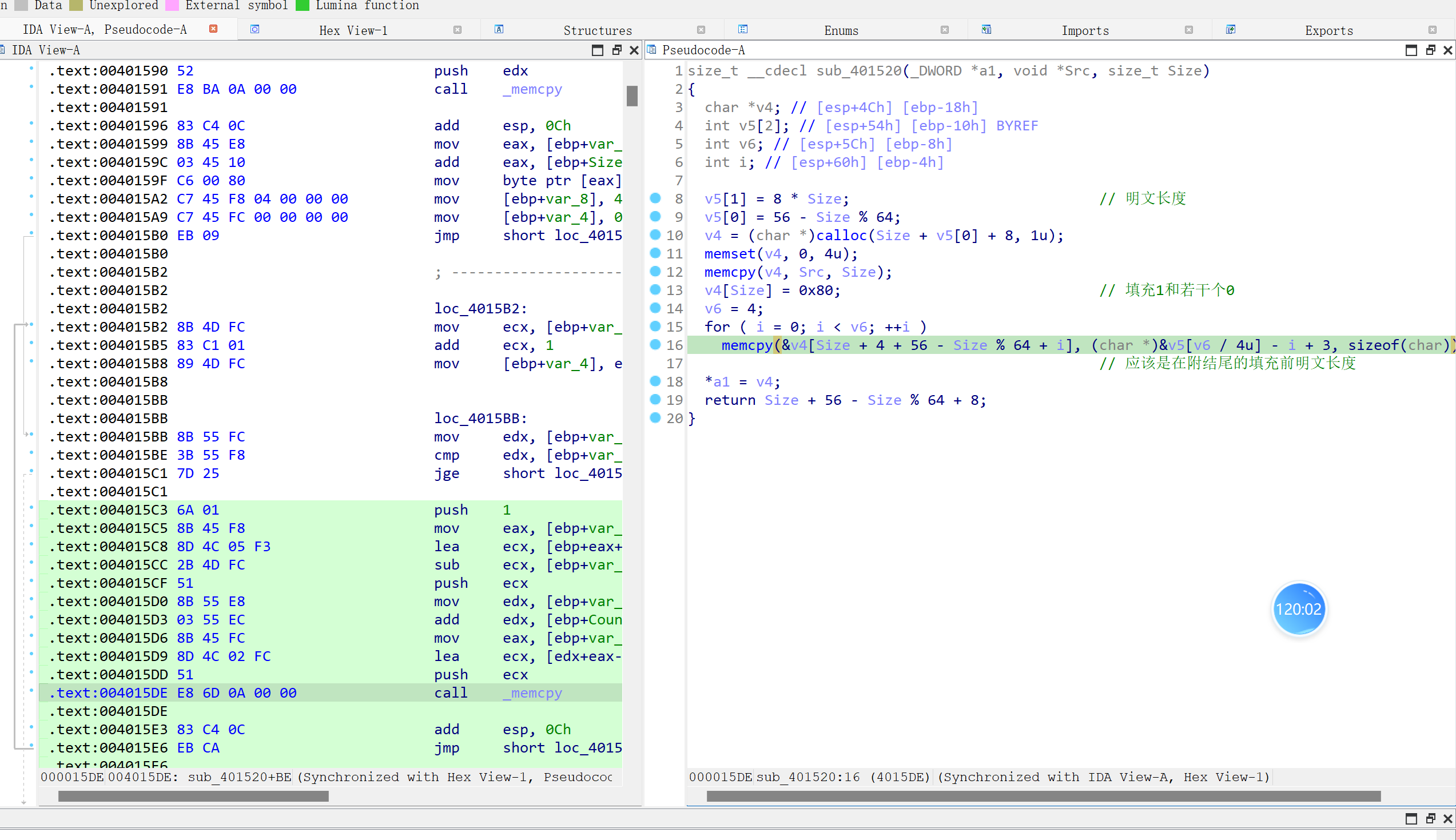


分析初始向量赋值：

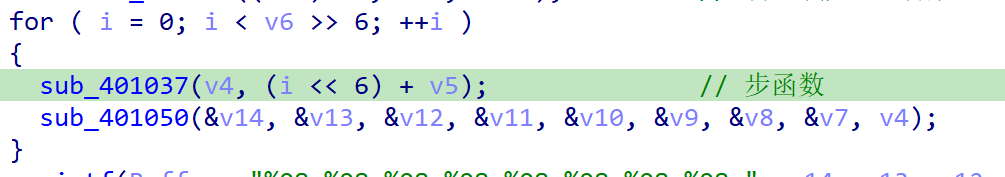
发现其为sha256初始向量：



分析明文填充和初始化函数：

其具体各部分的功能如下：  


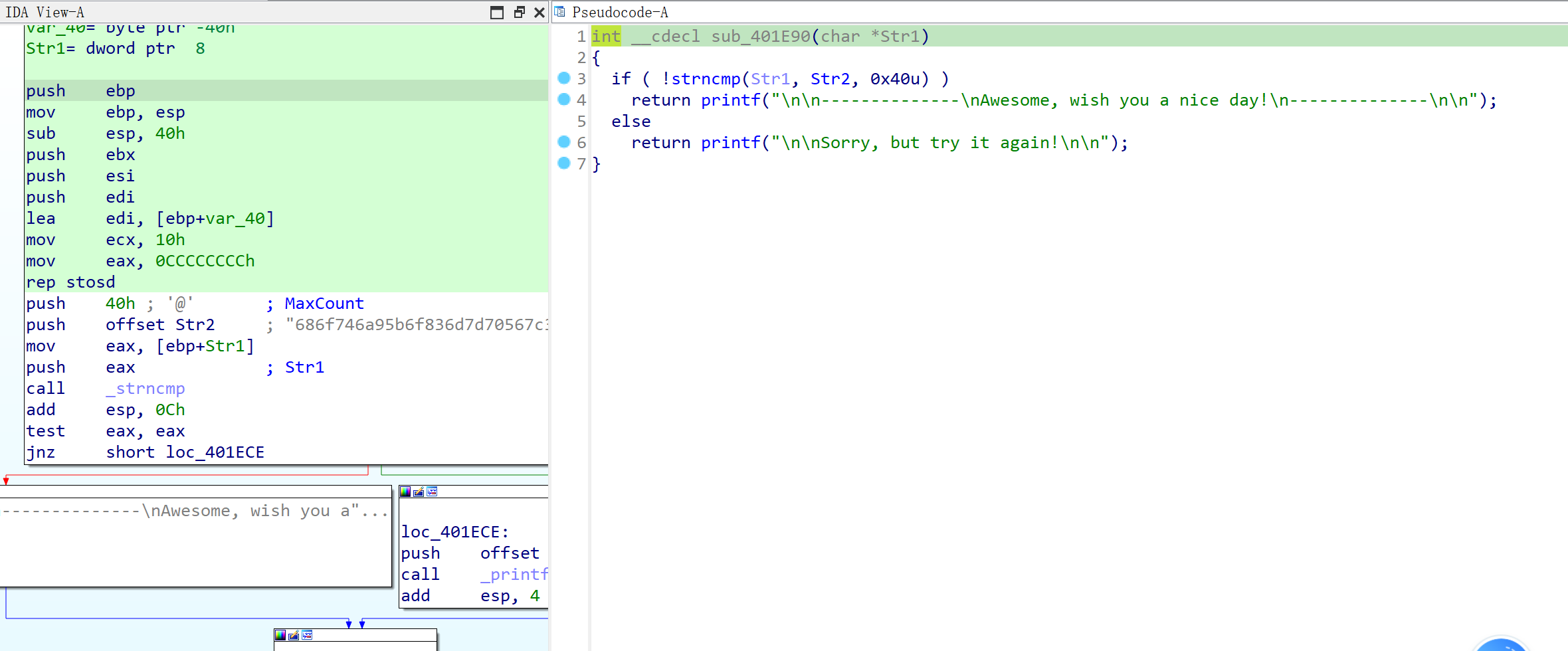
下面便是sha256的512分组明文块数\*64步步函数，不再分析



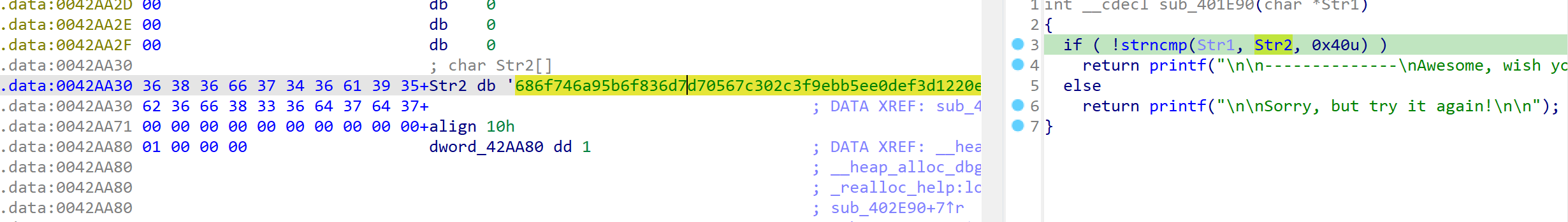
因而可确认第二个主要函数为sha256函数

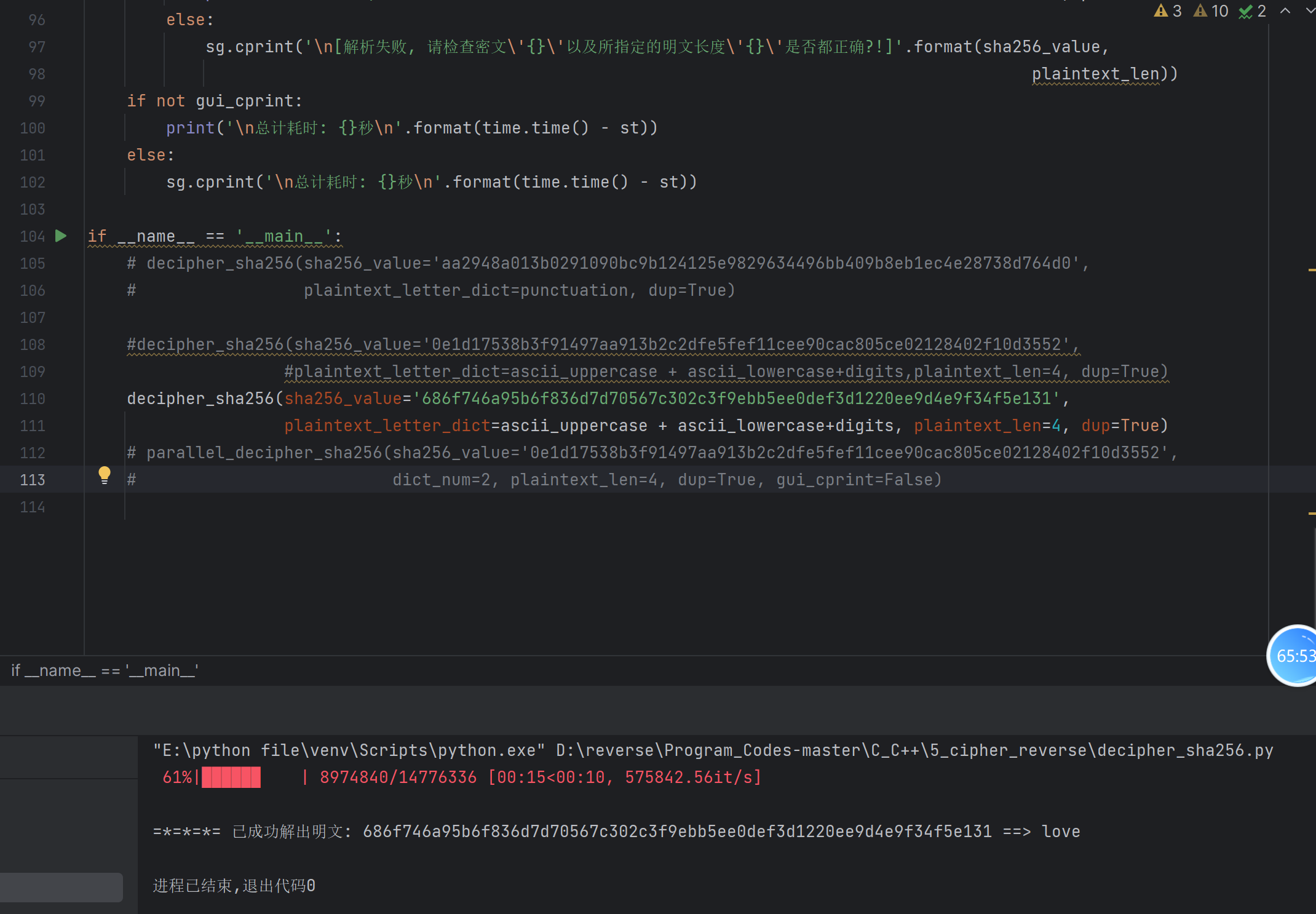
现查看第三个主要函数：

既对hash值进行比较：



找到目标hash值，放入脚本进行碰撞：





得结果为love，又因明文已经经过交换

其交换后顺序应为原来得第5，4，3，2，1，0位，故原文的5，4，3，2位分别为love，则可还原出密钥应为\*\*evol,其中\*可以为任意可输入字符（虽说提示应该输入的都应该是小写字母，但实际上没有输入判断）：

