## 知识点

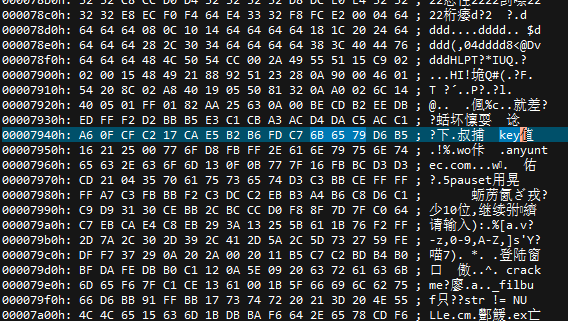
根据参数和返回值判断简单函数，eax和ecx寄存器，有条件转移与标志寄存器，使用UPX程序脱UPX壳。

## 题目

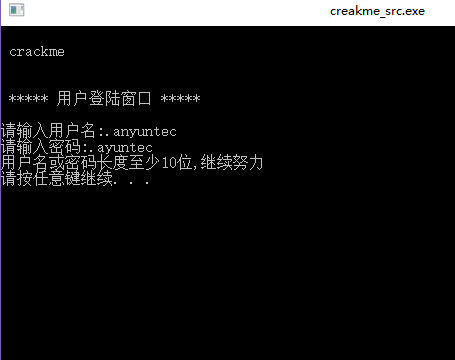


## 方法1（直接查看16进制代码）

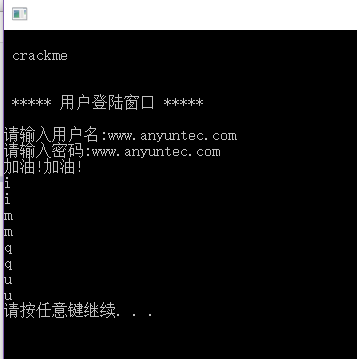
1. 使用UltraEdit查看exe的16进制数据，搜索关键词“key”；

****

1. 注意到key附近有.anyuntec.com字样，尝试输入，失败……

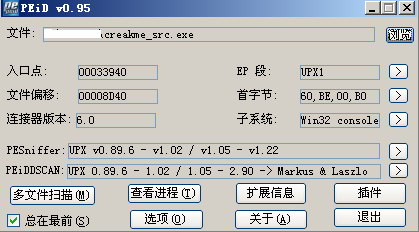


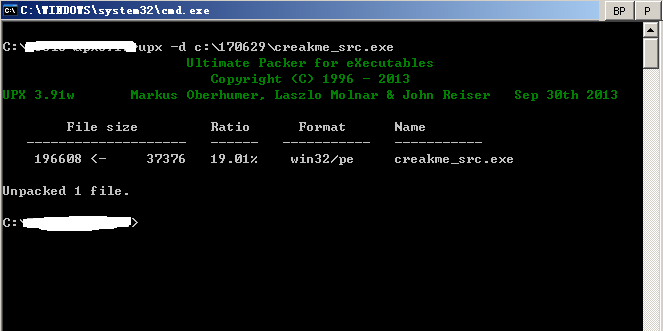
1. 猜测用户名和密码为www.anyuntec.com，尝试输入，得到字符串iimmqquu，成功

****

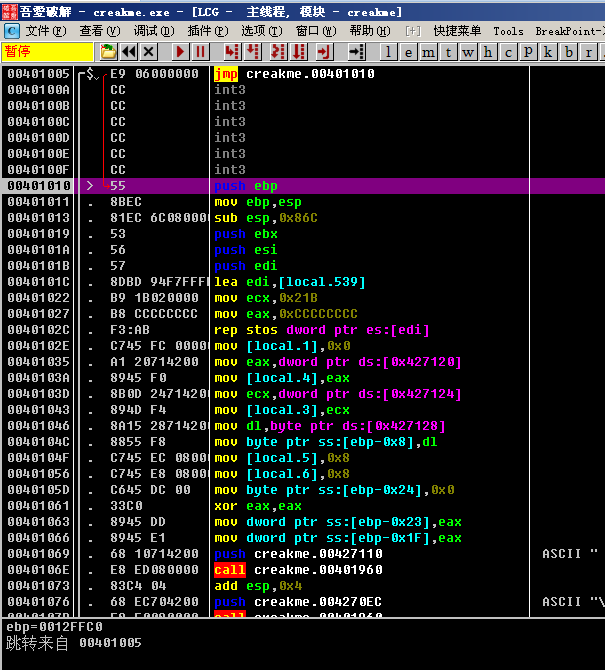
## 方法2（OllyDbg动态调试）

1. 首先查壳，该程序加了UPX压缩壳，直接使用UPX软件脱壳；





1. 使用OllyDbg加载脱壳后的程序，调试运行；

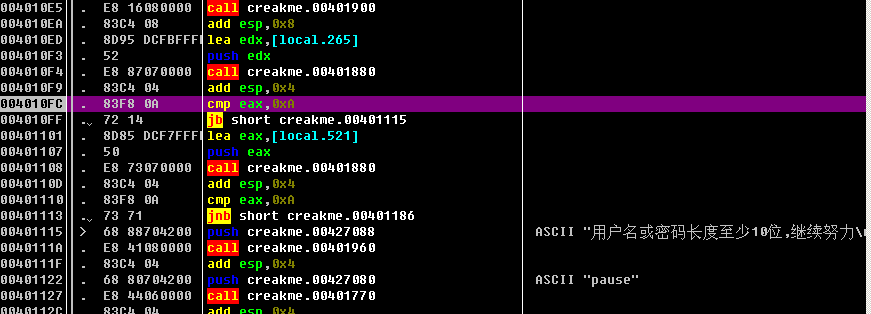


（main函数入口地址0x401010）

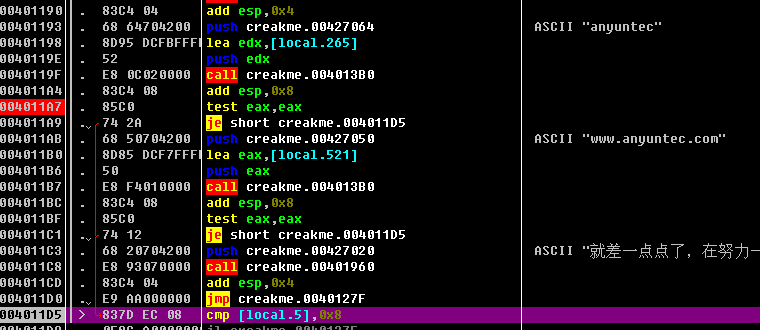


（调用printf()打印提示信息，调用scanf()获取输入）

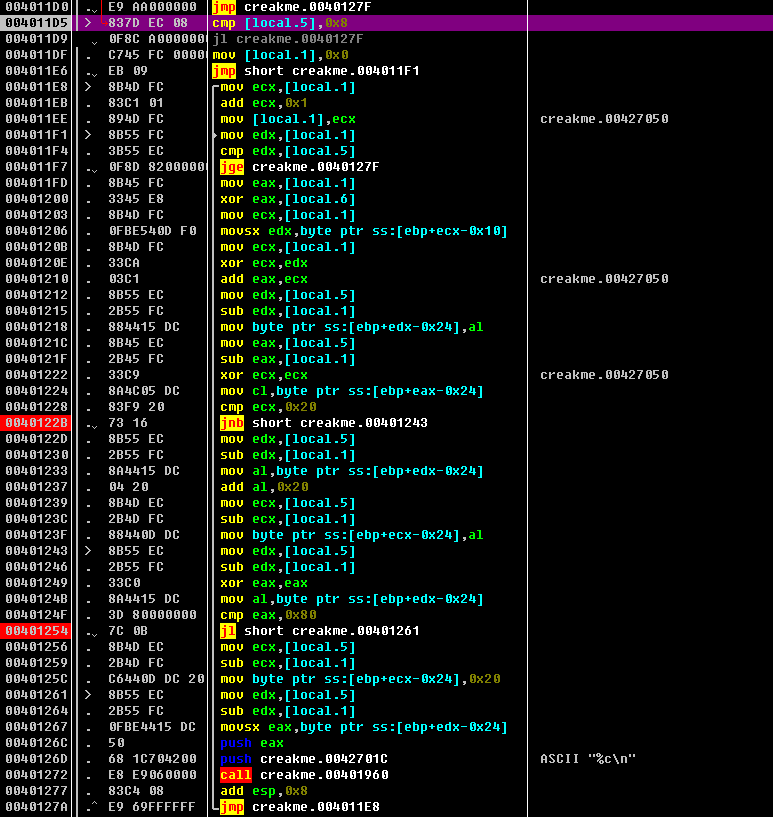
1. 经分析可知，软件首先进行用户名和密码的长度验证（若用户名或密码少于10个字符则报错退出）和字符串匹配验证（尝试将用户名与anyuntec匹配、密码与www.anyuntec.com匹配），跳过这两个跳转即可来到爆key的循环，共循环8次，每次打印一个字符。



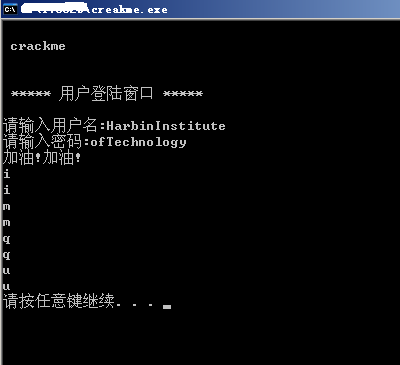
（调用strlen()计算用户名长度，与0xA比较大小，若小于则报错退出，否则继续计算密码大小并与0xA比较大小，若小于则同样报错退出）



（首先检查用户名是否为”anyuntec”，由于存在10个字符的长度限制，故按照程序逻辑，该条件永远不成立，若成立则直接跳转到爆key循环；接着检查密码是否为”www.anyuntec.com”，若成立则顺序执行爆key循环，否则报错退出）



（循环8次，爆key）



KEY{iimmqquu}