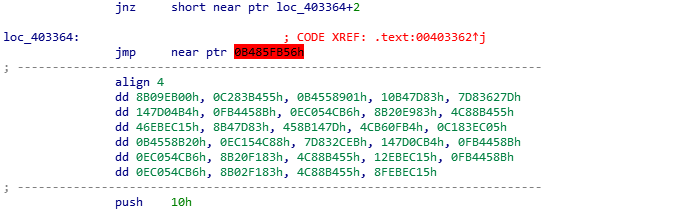
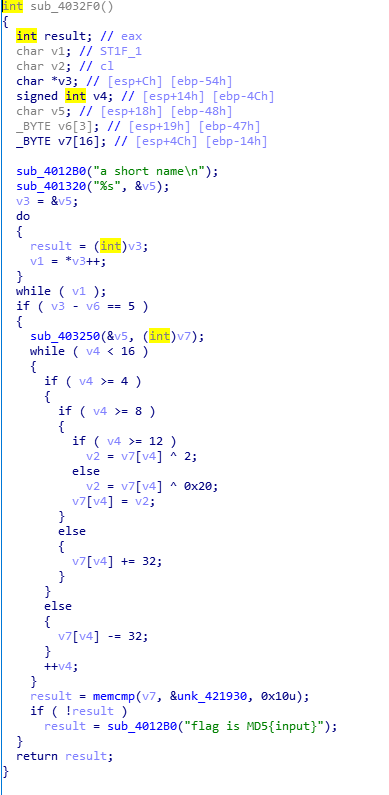
Easy\_rere

一个普通输入验证题，IDA打开后有发现反调试，还有花指令





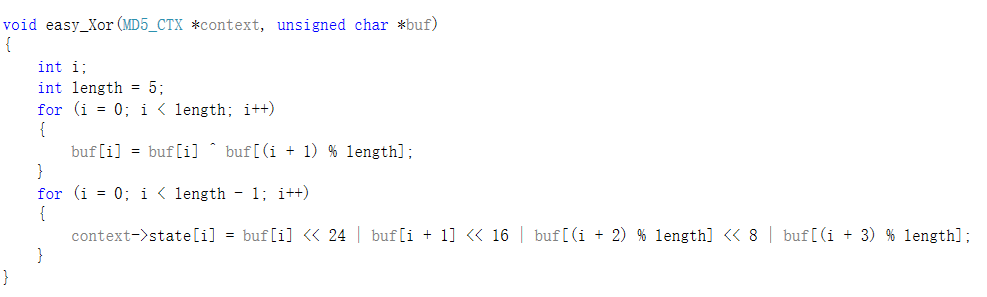
这些patch一下就可以正常调试，和反编译了。



大致意思就是输入5字节字符串经过sub\_403250处理然后长度就变为16了，做了一大堆亦或操作和最后unk\_421930字符串作比较。

不看sub\_403250函数是比较简单的。

而sub\_403250是一个魔改的md5，findcrypt发现不了的原因其实是把md5常量改成与输入相关的变量



因此这题只能爆破处理。爆破的字典还要设置一下如果都是[0x20,0x7e]的可见字符要爆破将近半个小时。根据提示short name，其实可以知道输入的是英文名，只需将英文大小写作为字典就可以。

