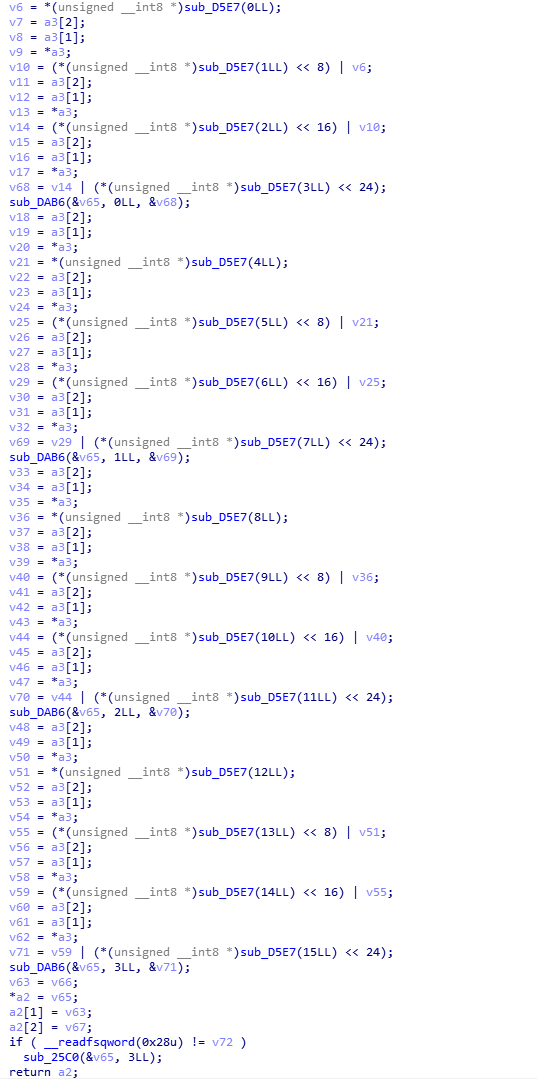
secret\_jpg

一个图片加密题，动态编译去符号表，破坏plt表结构。

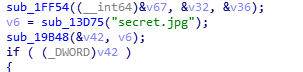
提供了一个经过加密后不能打开的图片。

执行程序会出现“whereisthekey：“要求输入一串字符串，这里对输入长度没有限制。

然后再sub\_1FF54函数会将输入分成4个双字小端存储起来，这里体现了你输入长度为16位。

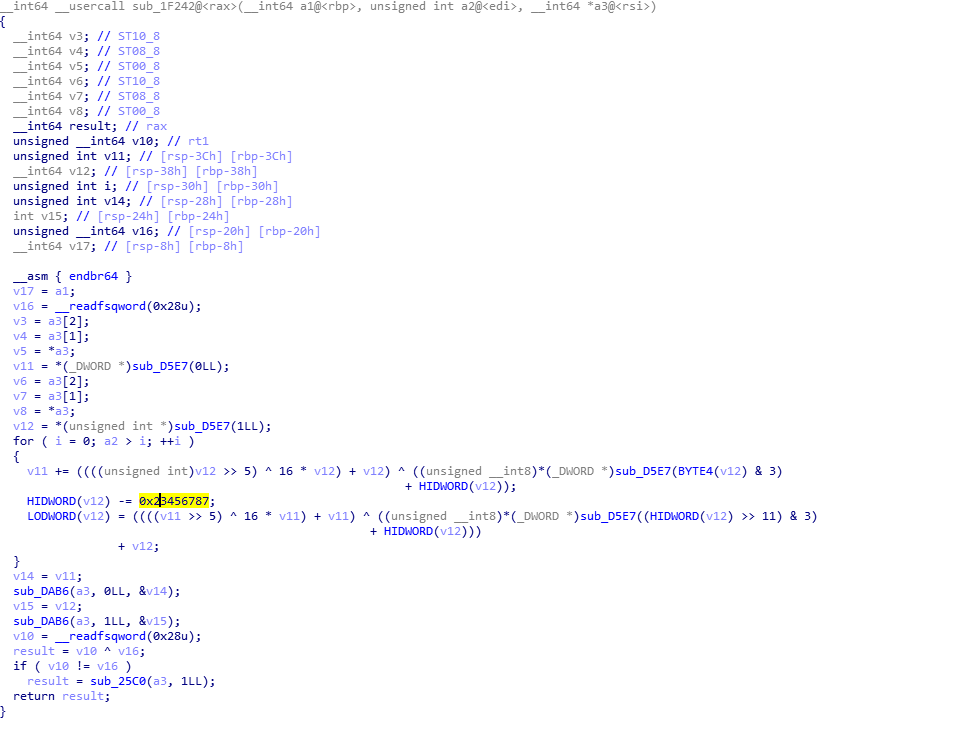


回到主函数会发现

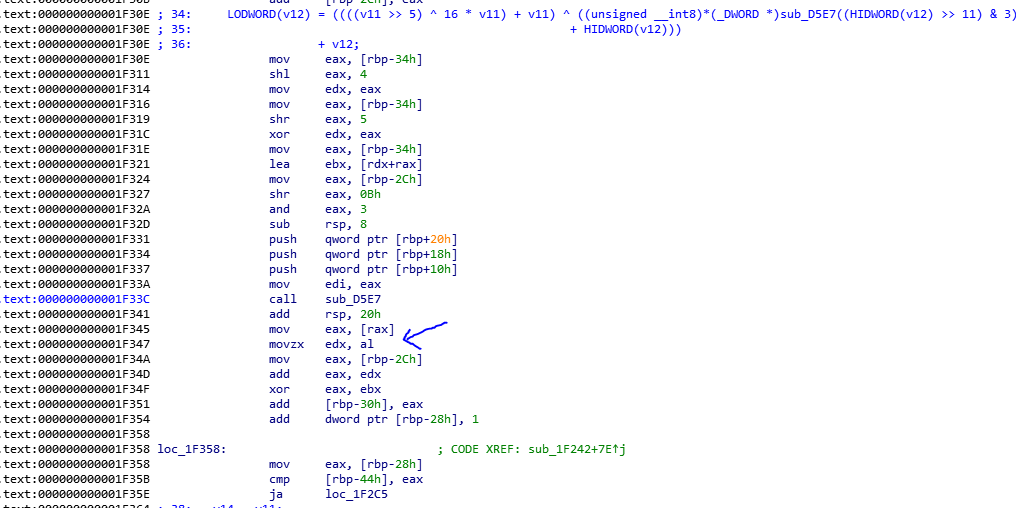


这里其实是检查目录下是否存在secret.jpg也就是需要加密的文件。

真正加密的入口是sub\_1F242



这里用到了魔改的Tea，delta为0x23456787，密钥就是输入的16长度的字符串。加密的内容是从secret.jpg依次读取的两位双字长内容。此时流程已经大概清楚了，就是输入作为Tea密钥把secret.jpg加密随后输出output.jpg。但如果是这样就需要根据jpg的格式要求爆破密钥，但密钥长达16字节，基本上爆破不出来。但仔细分析Tea魔改不只是delta，其实没次加密的过程中只用到了密钥的低字节。



所以只需爆破4字节长度的密钥，其他输入都与加密流程无关。

得到4字节长度关键密钥后解密output.jpg

