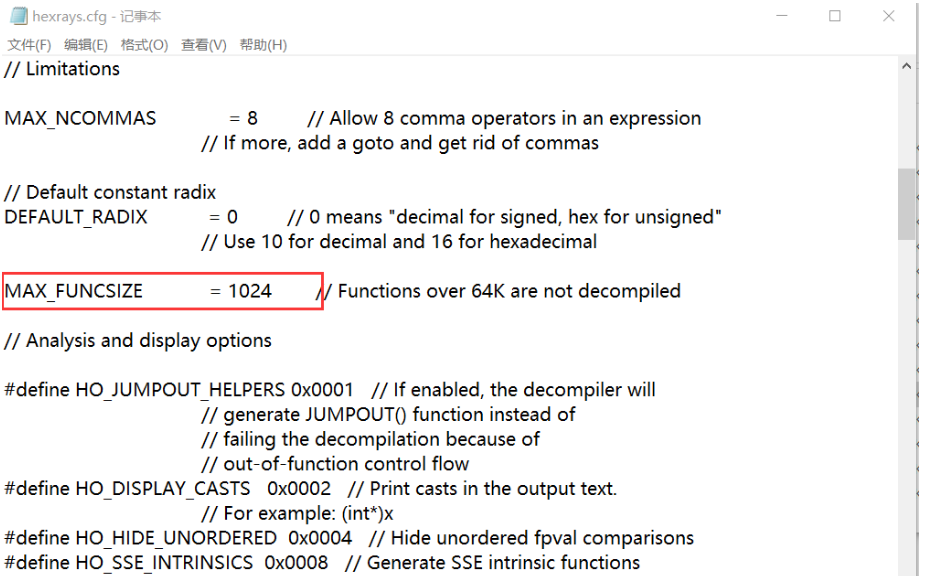
下载附件后查壳发现无壳直接拖进ida64查看main()函数

函数的结构非常简单。重点就在于sub\_83A()这个函数

这个函数很大直接f5是会报错的，要将ida /ctg目录下的hexrays.cfg文件中的MAX\_FUNCSIZE=64 改为 MAX\_FUNCSIZE=1024



再按f5等待一段时间后出伪c代码。

此函数有非常多繁琐但不复杂的计算，可以交给符号执行angr，具体见脚本

可以发现程序会返回错误的位数，可以使用爆破法，具体见脚本