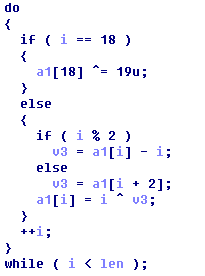
## EasyHook

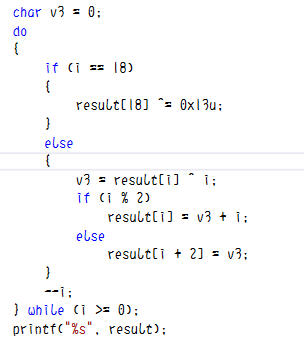
EasyHook异常友好，无花无壳无反调试。直接IDA查看main函数可以看到程序在0x401220处进行inline hook，将WriteFile转至0x401080处。

在0x401080处将调用0x401000检查buffer中传入的flag并恢复hook。

flag检查函数如图所示，可以看出flag的奇数位和偶数位分别执行不同的变换，然后和目标结果比对



相应写出倒推函数



得到flag{Ho0k\_w1th\_Fun}

不过题目有一个小缺陷，第一个字符无论是什么都会正常通过验证:)