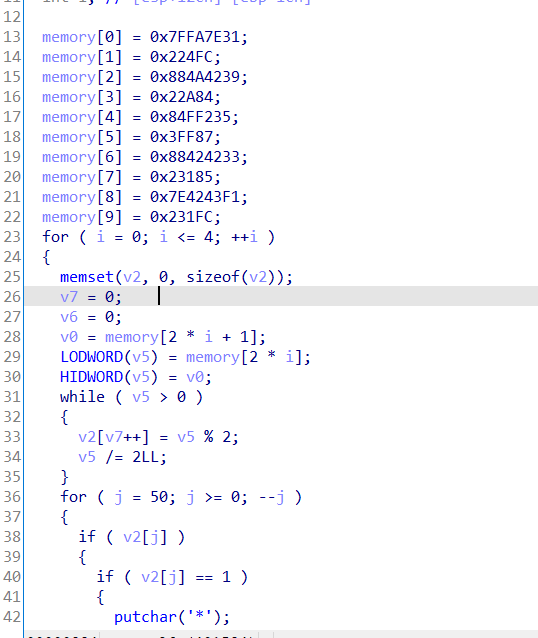


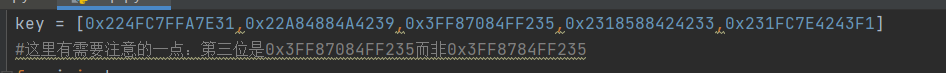
1. 找函数

我自己在做题的时候就没有找到\_ques函数，其实是有技巧的，这里有两个技巧可以找到此函数，1.找可以输出字符的函数putchar，puts等逐个交叉引用可以发现此函数，2.在函数列表里,在main函数前面有一个函数,ques没有执行(程序都是从main函数往下执行的)，即可以查看main函数上下的自定义函数。

1. 改eip就不说了，这里说一下高低位逐位比较的逆向分析



这里很容易看出memory数组的值分别赋值给v5高低位，其实没想到的是是逐位比较，下次看到%2和/2的组合应该想想是不是逐位比较，另外如果根据此编写脚本输出flag的话有一个点



原因是memory是给高低位赋值而非直接拼接，其他4个数字是因为地位恰好占满32位，而第三个数字占不满故需要补0才能进行后续打印，我自己写脚本打印的时候的结果一开始总是不对的原因就在这里。