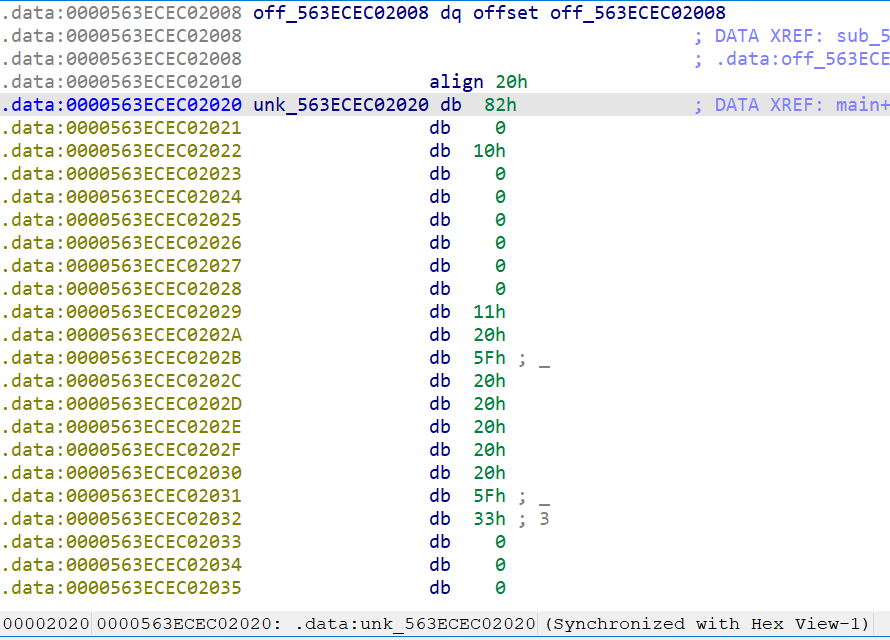
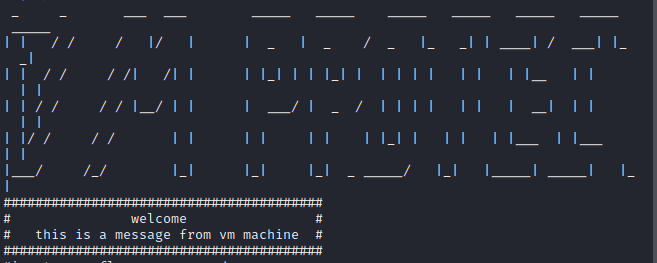
虚拟机逆向，ida打开可以看到



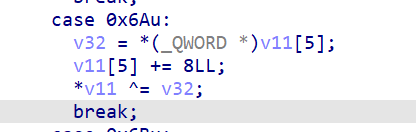
unk\_563ECEC02020处为字节码

然后需要弄清楚每个字节码的含义，分析switch中各个case的作用和含义，并进行动态调试，发现程序前面大部分的内容都没用，其实是在输出界面的内容。



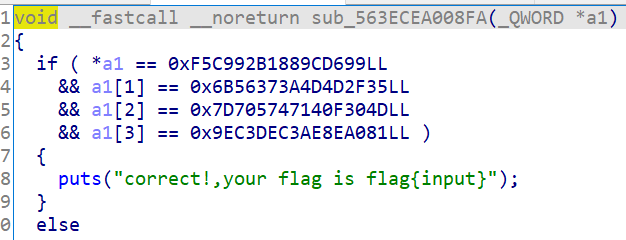
而真正的加密其实就是一个异或操作

而switch中的异或操作在此处



所以扣出字节码0x6a之后的8字节的数字，

分别为0xAABADBEEFBADBEED，0x1234567812345678，0x1111223366666612，0xADADEFABCDEFEDDE



直接写脚本与最后的结果做异或

result = [0xF5C992B1889CD699, 0x6B56373A4D4D2F35, 0x7D705747140F304D, 0x9EC3DEC3AE8EA081]

x = [0xAABADBEEFBADBEED, 0x1234567812345678, 0x1111223366666612, 0xADADEFABCDEFEDDE]

flag = ""

for i in range(4):

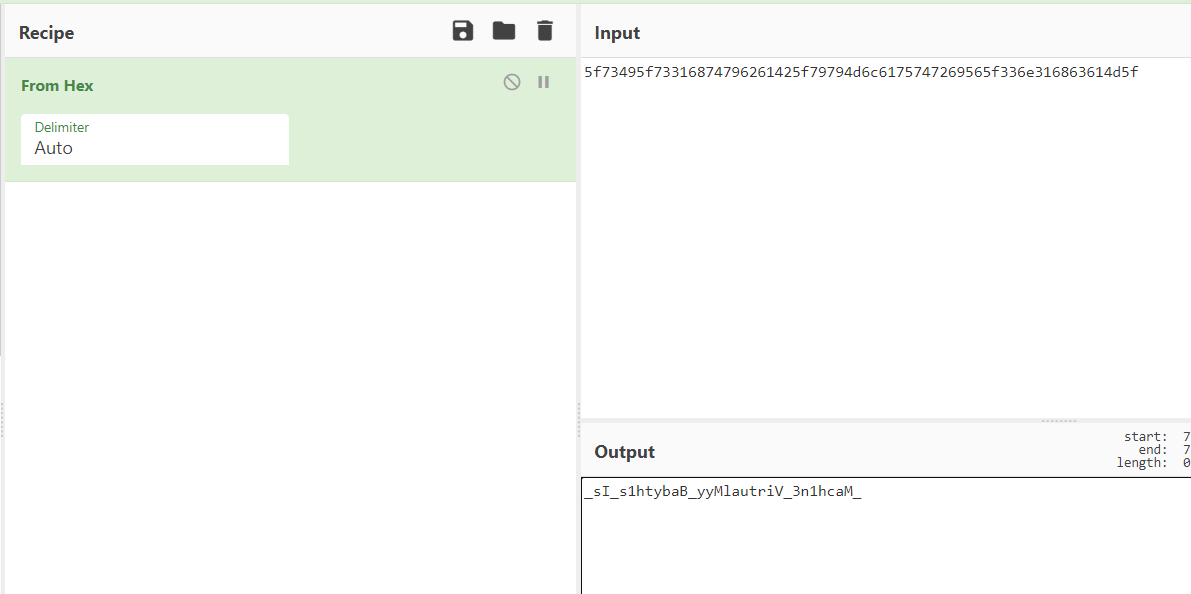
    flag += str(hex(result[i]^x[i]))[2:]

print(flag)

得到结果

5f73495f73316874796261425f79794d6c6175747269565f336e316863614d5f

然后16进制转字符串



得到的结果\_sI\_s1htybaB\_yyMlautriV\_3n1hcaM\_

按照每8位 置换一下顺序 得到

th1s\_Is\_Myy\_Baby\_Virtual\_Mach1n3