2021-2022学年春季学期《汇编语言与逆向工程》

期末试卷标准答案及评分标准

###### 第一题CPP1.exe

1. 识别到main函数中调用的核心加密函数sub\_40100A。(2分)
2. 沿sub\_40100A->sub\_4013D0->sub\_401014->sub\_401190可以进入到RC4的sbox初始化函数中。从这个函数的行为特征能够判断出加密算法为RC4，例如存在初始密钥为{0xfc,0xfb,0x3b,0x0d,0x73,0x6e}；生成值为0-255的S；循环256次复制密钥到临时向量T中；循环256次用T对S进行置换。（5个点10分）
3. 加密后的flag存储在byte\_42C700处。flag的前12字节使用RC4加密，flag后7字节使用异或加密，密钥存储在byte\_42C600处。（5分）
4. 解密得到的flag为NetworkClassNotGood。（3分）

###### 第二题CPP2.exe

1. 输入的flag要求长度大于等于5，且ascii码在大于等于65小于等于122。识别到main函数中调用的核心加密函数sub\_401005。（2分）
2. 识别出哈希算法为SHA256，理由是：存在SHA256的初始特征值{0x67,0xe6,0x09,0x6a}等；sub\_401500对输入数据填充至512的整数倍；sub\_401760是SHA256进行逻辑运算的过程。（5个点10分）
3. Main函数中对哈希值的每字节进行了加1操作。加密后的flag哈希值存储在0x0428184处，将其每字节减1还原出flag的哈希值。（5分）
4. 爆破得到原始明文为Seeyou。（3分）

###### 第三题CPP3.exe

1. 输入的flag长度要求为8位，加密逻辑就在main函数中。(2分)
2. 分析加密逻辑为将输入的每字节的最高位与最低位进行交换，然后与0x0429A38处的密钥进行异或加密。flag的加密结果存储在0x00429A30处。（10分）
3. 解密方式为重新与密钥异或一遍，并将每字节的最高位与最低位交换。（5分）
4. 得到flag为：TAKEeasy。（3分）

###### 第四题CPP4.exe

1. 0x4010FB处存在jmp花指令，将机器码0xE9改为0x90来进行修复。(5分)
2. 加密逻辑就在main函数中，byte\_429A30处存储了加密后的flag。（2分）
3. 加密方式为逐字节取反，因此解密只需要对byte\_429A30处的数据取反即可拿到flag。（10分）
4. 得到flag为：Beat\*0micron\*!（3分）

###### 第五题CPP5.exe

1. 识别到main函数中主要调用的功能函数为sub\_401023，往里走一直到sub\_401470。该函数对输入进行了检查，要求输入的第10，13，17，20，22字节为’-’。(2分)
2. 在sub\_401470中发现程序注册的SHE模块stru\_427078，根据其中的loc\_401530可知发生异常时会调用sub\_401014。(5分)
3. 在0x0401509处的除法会引发除0异常，进入异常处理逻辑。（3分）
4. 沿sub\_401014进入sub\_4012E0。其逻辑为对输入中的大小写字母进行参数a=3,b=7的仿射加密，而且加密过程中会将字母按字母表顺序映射为0~25再还原成字母。（6分）
5. flag加密结果存储在dword\_429A44处。对其中的字母进行仿射密码的解密操作。（2分）
6. 得到flag为flag{T1an-71-4a0-9e-a-!}。（2分）