20 98

第一题：

在 0x40117D 处存在 jmp 花指令，修补为 nop 后重新打开即可反编译 main_0 函数。

sub_401005(a, b) 等价于 Read(buffer, size)

输入长度为 15 的串，与 byte_427A30 倒序异或后，逐位与 byte_427A40 比较，相同则获取 flag.

即：for (i=0; i<15; i++)

flag[i] ^ byte_427A30[14-i] ^ = byte_427A40[i]

故 flag[i] = byte_427A30[14-i] ^ byte_427A40[i]

20

flag: MoreThenFriends

第二题：

在伪代码第 18 行出现除零异常，因此~~本~~猜测重要部分必定在异常处理函数中。

观察汇编代码，在 0x4011B6 - 0x4011C7 处为~~注册~~ SEH 链表操作，其中插入的函数为 sub_401005.

所以 sub_401005 函数应该有重要内容。

（一共 4 个函数，2 个 main，sub_401005 之指向 sub_401020，所以直接猜也知道异常处理在 sub_401020）。

进入 sub_401005，指向 sub_401020.

进入 sub_401020，经典位运算。

a[i] = 4*(a[i]&3) | ((a[i]&0xC)>>2) | a[i]&0xF0.

取后2位 左移2位；取3、4位 右移2位；取高4位 不动。

即这个操作是交换 a[i] 的低 1、2 bit 和 3、4 bit 位置，交换后与 byte_429A30 比较。

因此，交换 byte_429A30 低 12、34 bit 即得到 flag.

~~而~~得到 flag = "SecurityIsPuzzle"，但输入要求长度 18.（后面只取前 16 字节）故输入时 输入 flag 后随便打两个字母即可。

20

第三题：

输入一串长度≥5的小写字母串，取前4位进行某种加密后，得到一串16进制串，推测加密应该是hash函数，又摘要长度为128bit，即排除SHA2，可能为SHA-1或MD5

在sub_401420函数中，是对4个量进行初始化，分别值为 0x67452301，0xefcdab89，
0x98badcfe，0x10325476。

符合md5要求。

sub_401500返回3 size+0x38-size%0x40+8，

其实是填充后明文的长度，对齐单位为512bit，在加密函数中的循环轮数为长度÷64byte，完全符合md5加密。

因为明文就4字节，直接爆破即可。

爆出明文：love。

输入长度要求≥5，就在flag后随便补一个小写字母即可。(如：loveu)。

20

第4题：

输入一串大写字母，对其在伪代码第33行进行如下操作：

input[j] = (7+9*(input[j]-'A'))%26+'A'

即是的仿射密码，a=9，b=7。

密文已给出，存在0x429A30处。

解密即可。~~int~~ message[i] = (cipher[i]-7)*9^-1 (mod 26)。

flag："HANGON"

20

第5题：

输入8字节(64bit)数据进行某种加密。

最一开始调用sub_40100F函数，传入3V4变量，V4中存的字符串为"TakeEasy"，猜测为密钥。进入后，发现程序流程与DES密钥扩展流程一致：

sub_401046 => PC1置换
sub_401014 => ShiftLeft
sub_40100A => PC2置换。

子密钥存在unk_420C9C中。

而sub_401200函数流程也与DES加密流程

[redacted]
2019

一致，因此确认加密为DES加密。
密文、密钥已给出，解密即可。

解出flag：itiseasy.

18