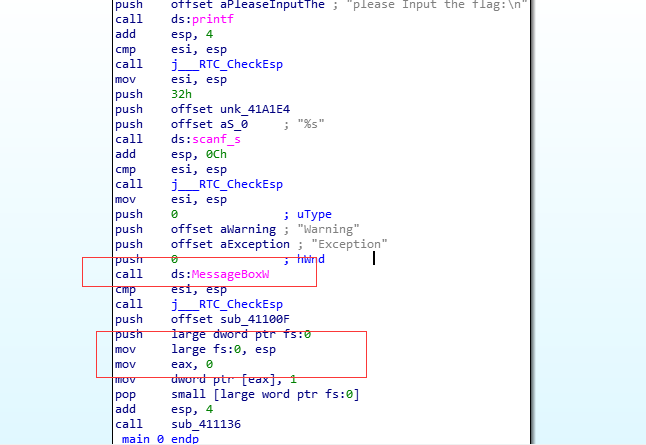
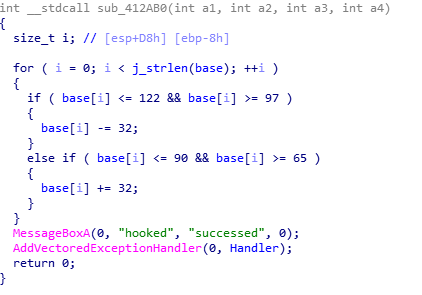
# 0x0 Hook

首先调用MessageBox，再触发异常。



要知道的是MessageBox是被Hook了的，执行的函数是sub\_412AB0。

Hook用的代码应该是这个网址的<https://blog.csdn.net/Simon798/article/details/99627345>。



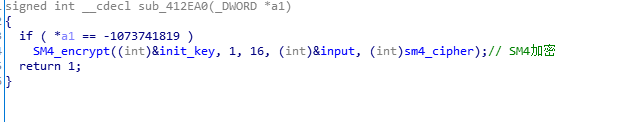
可以看到base表被改变了，这里是第一次改变，改变后表是“abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789+/”。

# 0x1 SM4加密

触发异常后会先执行sm4加密的密钥初始化。



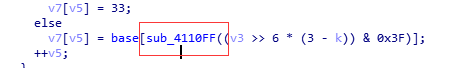
然后会执行sub\_412EA0的SM4加密

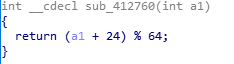


然后再执行sub\_412C30函数，打乱的比较数据的顺序，然后进行了base64加密。



需要注意的是在base64加密函数里面的sub\_4110FF，进行了第二次编码表变化。





现在编码表是yzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789+/abcdefghijklmnopqrstuvwx。

# 0x2 脚本

from pysm4 import decrypt  
  
#-------base64-----------------  
diy\_baes = 'yzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789+/abcdefghijklmnopqrstuvwx!'  
base = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/="  
cipher = "1UTAOIkpyOSWGv/mOYFY4R!!"  
new\_cipher4 = ""  
for i in range(0,len(cipher),2):  
 new\_cipher4 += cipher[i+1]  
 new\_cipher4 += cipher[i]  
new\_cipher = ""  
for i in range(len(new\_cipher4)):  
 new\_cipher += base[diy\_baes.find(new\_cipher4[i])]  
print new\_cipher  
#-------base64-----------------  
  
#--------cipher\_num-------------  
byte = new\_cipher.decode("base64")  
cipher\_num = ""  
for i in range(len(byte)):  
 cipher\_num += "%2x"%(ord(byte[i]))  
cipher\_num = int(cipher\_num.replace(' ','0'),base=16)  
print cipher\_num  
#--------cipher-------------  
  
#-----------key\_num----------  
str = "where\_are\_u\_now?"  
key\_num = ""  
for i in range(len(str)):  
 key\_num += "%x"%(ord(str[i]))  
key\_num = int(key\_num,base=16)  
print key\_num  
#-----------key----------  
  
  
clear\_num = decrypt(cipher\_num, key\_num)  
print hex(clear\_num)[2:-1].decode('hex')

flag：SM4foRExcepioN?!