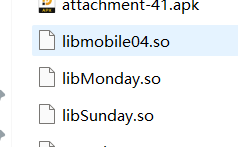
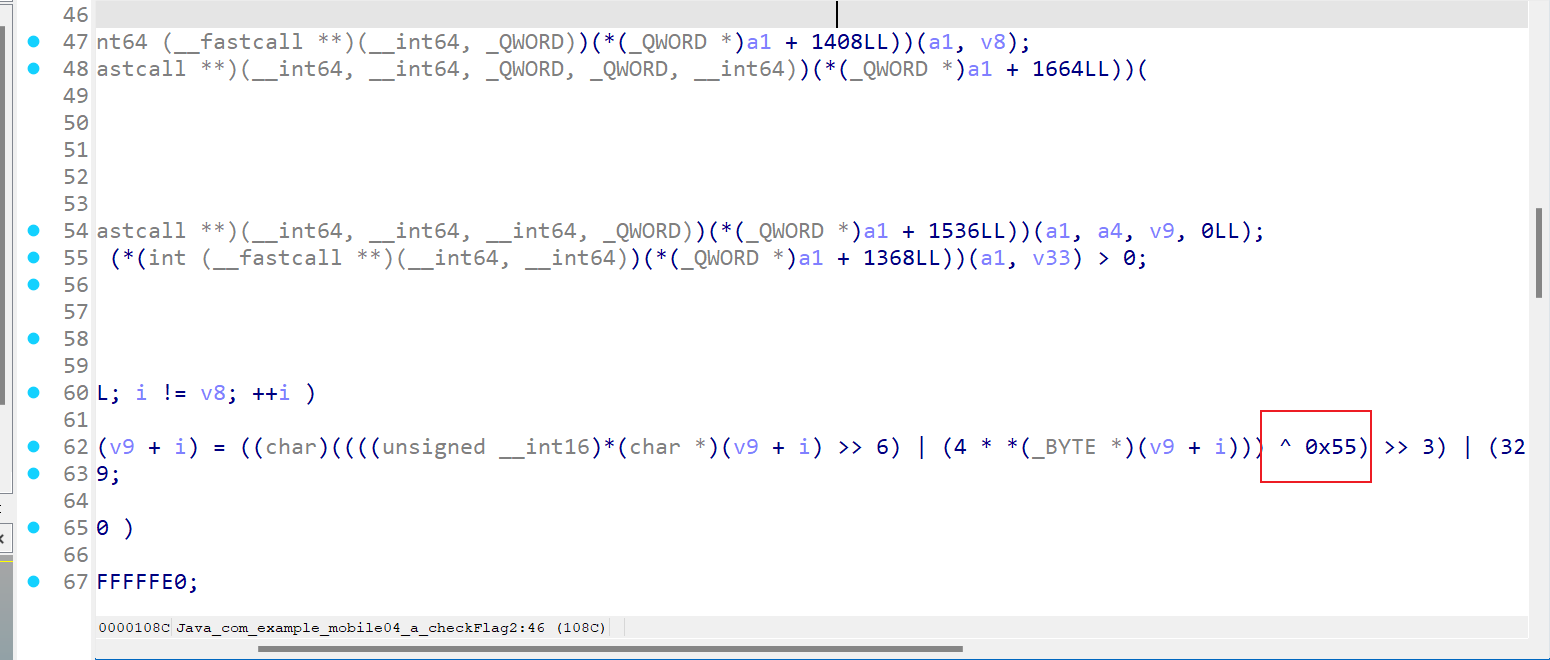
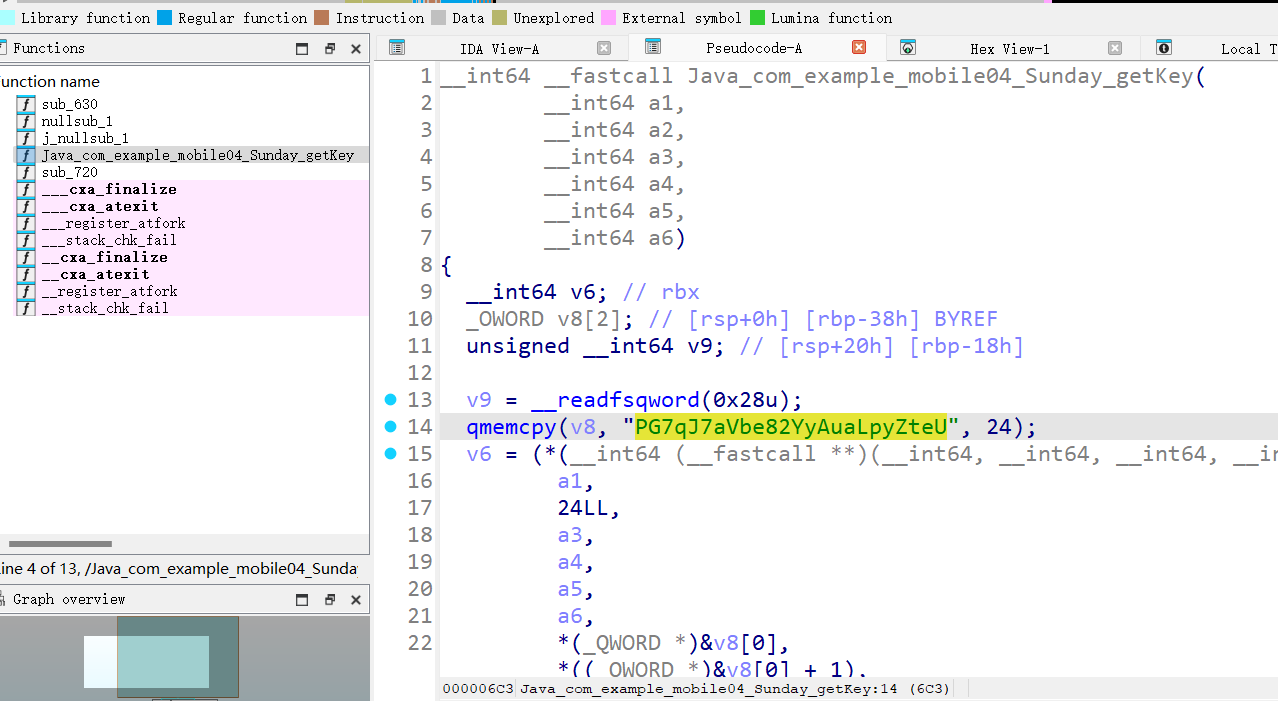
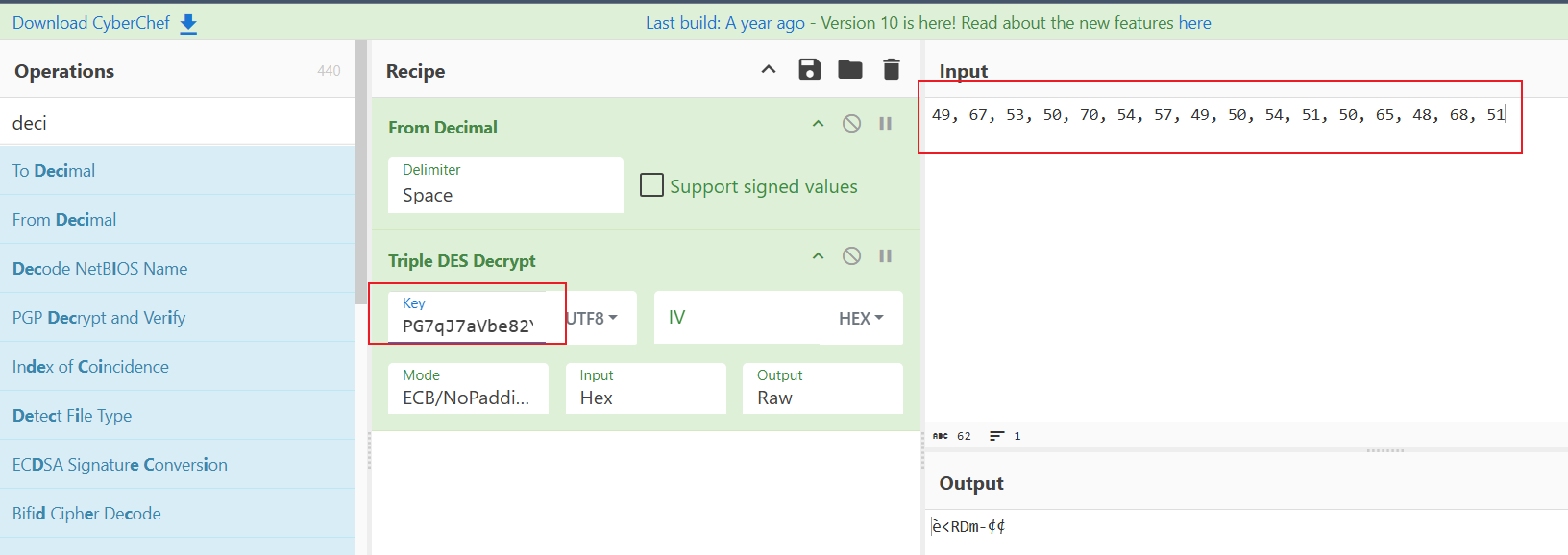
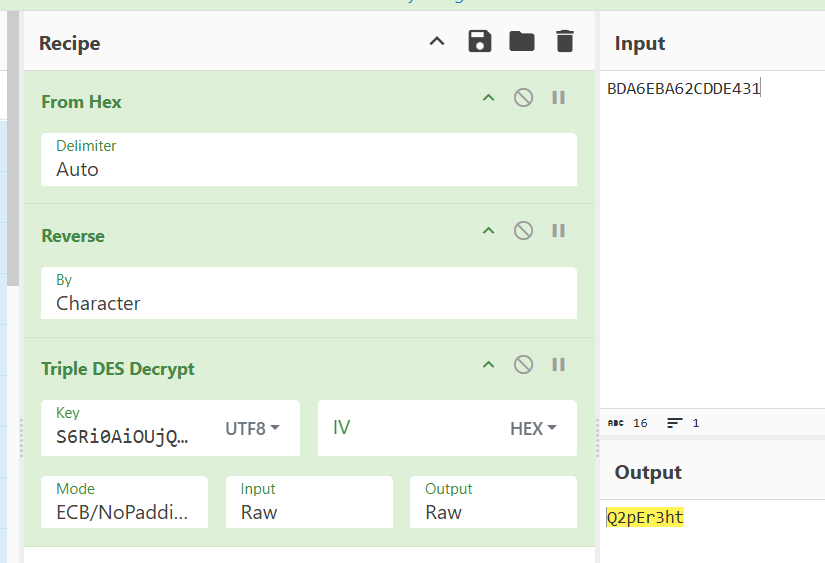
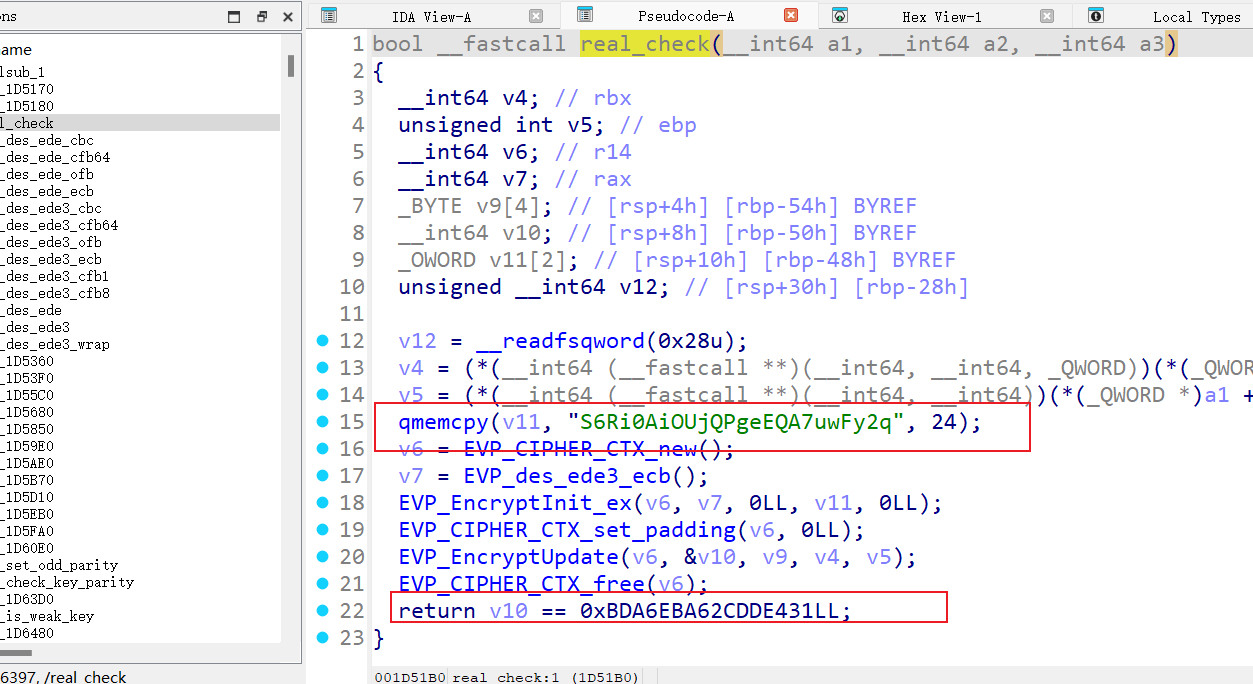
mobile2

先dump下来dex文件 直接用dexdump就可以获取到checkflag1，在java层，一个des解密，密钥在Sunday.so

checkflag2在assets目录下，加密的so层，这个so的加密逻辑在Monday这so里，就是简单的位移和异或，每个用户的异或值不一样

也是一个des解密，解出两部分flag拼一起

1. apk解压，lib x8664拿到三个so  
     
   asset x8664拿到enreal  
   2.mobile04搜Java\_com\_example\_mobile04\_MainActivity\_getEncryptedSegment，拿到adex的字节值填到上面脚本s里 3.monday.so搜Java\_com\_example\_mobile04\_a\_checkFlag2，看异或多少替换 data[i] ^= 0x55  
     
   4.拿到decrypted.dex复制里面的数值，sunday.so搜字符串  
     
   然后去赛博厨子   
   5.decode\_enreal ida反编译搜real\_check，复制字符串和hex值赛博厨子   
   6.拼接两个解密的字符串就是flag

s = []

with open("decrypted.dex", "wb") as f:

f.write(bytes(s))

with open("enreal", "rb") as f:

data = list(f.read())

for i in range(len(data)):

data[i] = (data[i] << 2) | (data[i] >> 6)

data[i] &= 0xff

data[i] ^= 0x55

data[i] = (data[i] >> 3) | (data[i] << 5)

data[i] &= 0xff

with open("decode\_enreal", "wb") as f:

f.write(bytes(data))