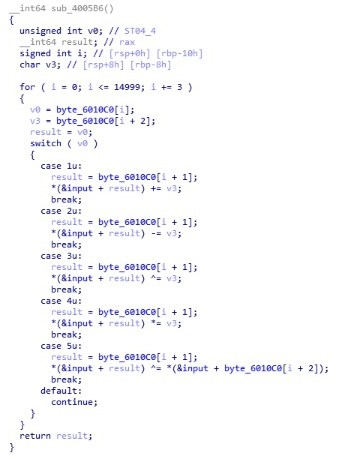
## 题目分析

拖进IDA进行分析



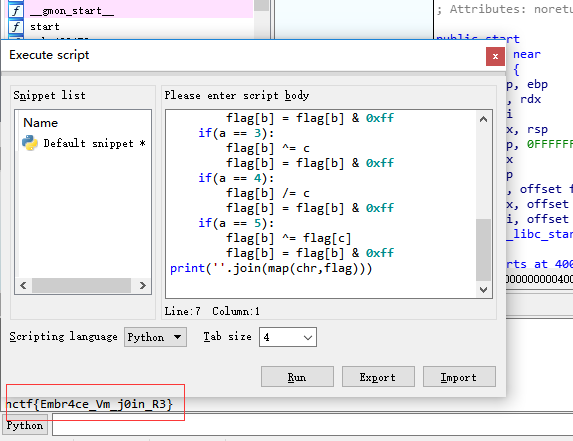
然后点进sub\_4005B6函数。



sub\_4005B6是个逻辑很清晰简单的VM。

我们选择使用IDAPython脚本来求解flag。

我们点击file->script command



## 脚本

adr1 = 0x6010C0  
adr2 = 0x601060  
flag =[]  
  
for i in range(0,24\*4,4):  
 print "%x"%Dword(adr2+i)  
 flag.append(Dword(adr2+i))  
  
for i in range(14997,-1,-3):  
 a = Byte(adr1+i)  
 b = Byte(adr1+i+1)  
 c = Byte(adr1+i+2)  
 if(a == 1):  
 flag[b] -= c  
 flag[b] = flag[b]&0xff  
 if(a == 2):  
 flag[b] += c  
 flag[b] = flag[b] & 0xff  
 if(a == 3):  
 flag[b] ^= c  
 flag[b] = flag[b] & 0xff  
 if(a == 4):  
 flag[b] /= c  
 flag[b] = flag[b] & 0xff  
 if(a == 5):  
 flag[b] ^= flag[c]  
 flag[b] = flag[b] & 0xff  
print(''.join(map(chr,flag)))