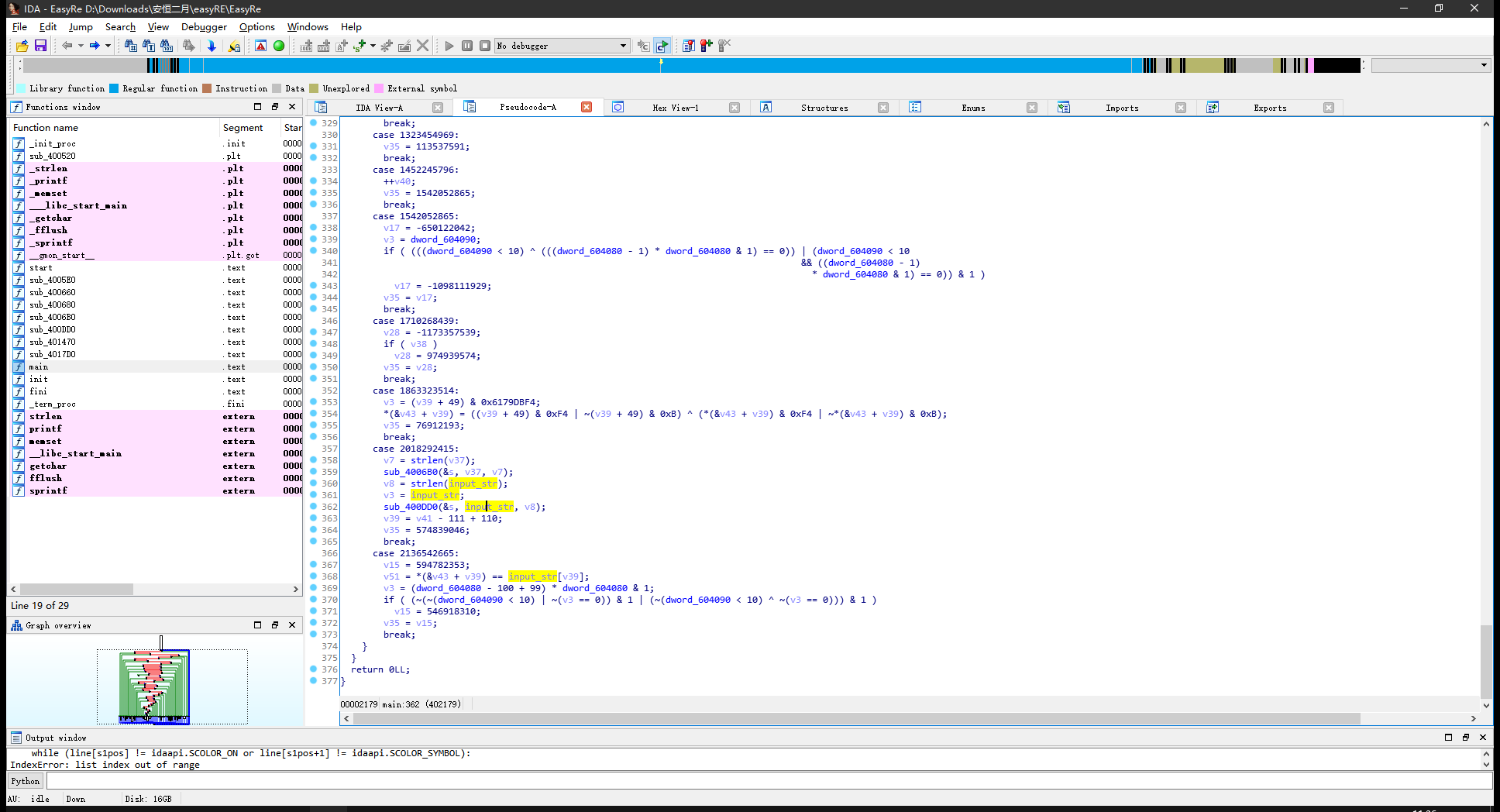
EasyRE

拖进IDA，发现平坦化控制流，但觉得不会出太大难度的题

跟踪输入字符串，发现可疑部分

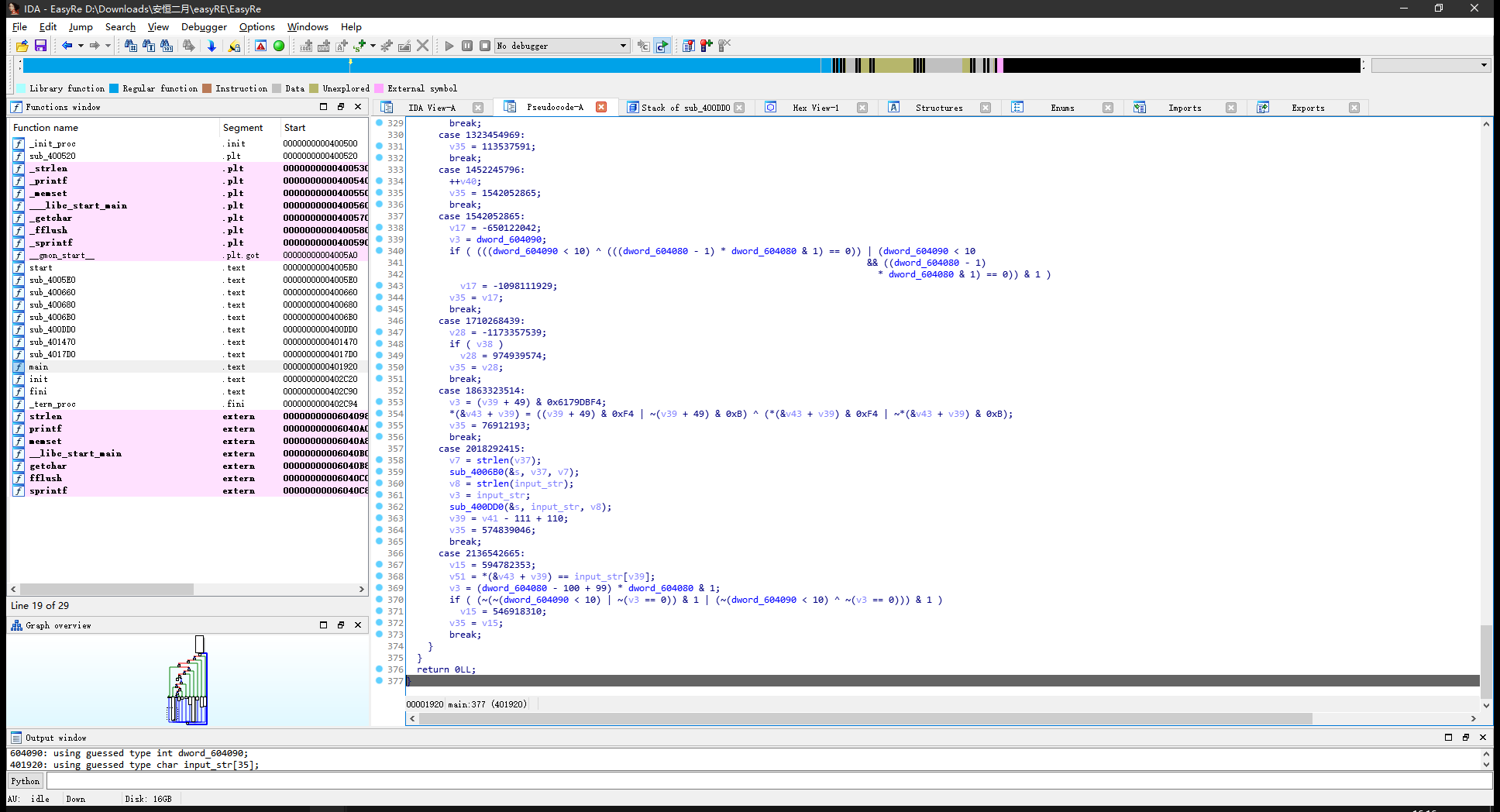


去网上找符号执行去平坦化控制流搞了半天没搞出来。。。

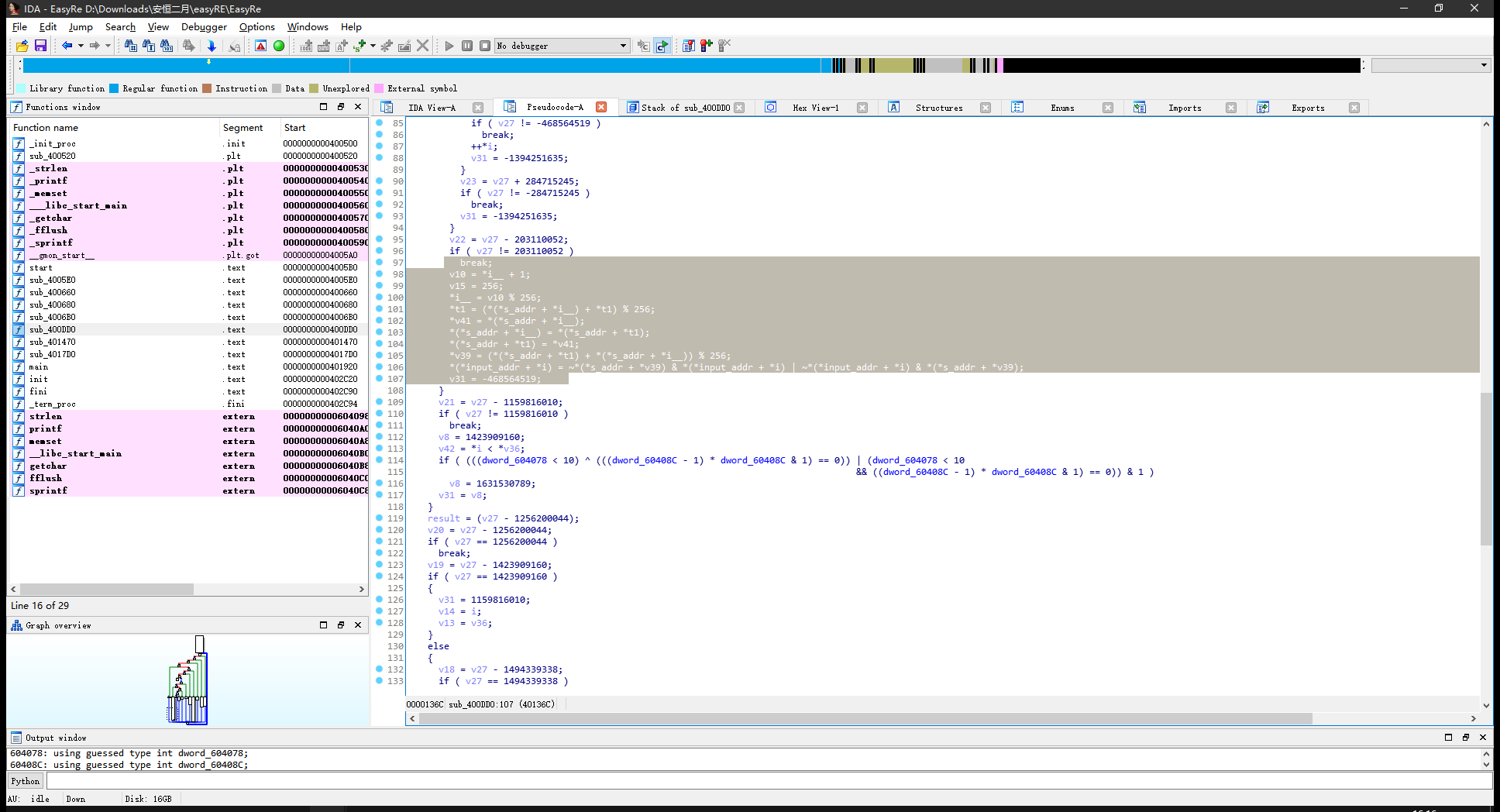
搞去平坦或控制流出来了结果跑不起来

只能头铁怼，

发现其是先对输入进行了处理，然后进行对比



处理过程为：



有几个值都是固定的，稍微分析一下，就可以写出解密脚本：

s = [  
 0x87, 0x95, 0x35, 0x1D, 0x20, 0xEF, 0x7C, 0x9D, 0x3A, 0x60,  
 0x44, 0x24, 0xAD, 0x76, 0x51, 0x8E, 0x18, 0x54, 0xCA, 0x81,  
 0xA2, 0x91, 0xEC, 0x5D, 0xE2, 0x8A, 0xF6, 0x06, 0x11, 0x28,  
 0xD3, 0x80, 0x7F, 0x2A, 0x32, 0x09, 0x16, 0x1E, 0x7A, 0xB3,  
 0x85, 0x93, 0x9C, 0xBF, 0xE8, 0x7D, 0x38, 0x88, 0xFA, 0x8C,  
 0x89, 0xA7, 0x40, 0xE7, 0x4D, 0xB4, 0xC1, 0x04, 0x66, 0xE1,  
 0x3D, 0x43, 0x47, 0xC9, 0x26, 0xA0, 0xCF, 0x31, 0x59, 0x0E,  
 0xC7, 0xB1, 0x79, 0x86, 0xC5, 0x14, 0x9B, 0xDD, 0x70, 0xDC,  
 0xA5, 0xBD, 0xA4, 0xD6, 0xD0, 0xE3, 0x69, 0xF0, 0x19, 0x9A,  
 0xD7, 0xDE, 0x6C, 0xF5, 0xC2, 0x67, 0xE6, 0x92, 0x99, 0xA8,  
 0x77, 0x2B, 0x1A, 0x6B, 0x98, 0x53, 0x33, 0xE0, 0xBC, 0xF3,  
 0x2C, 0x23, 0x4B, 0x7E, 0x0C, 0x52, 0xDA, 0x5B, 0xE9, 0x37,  
 0xB7, 0xAB, 0x5C, 0x3B, 0x02, 0xC3, 0xFF, 0x83, 0x10, 0xF4,  
 0xAA, 0x4A, 0xC8, 0x15, 0xD1, 0x56, 0xAE, 0xEE, 0x82, 0xB5,  
 0xFD, 0xFC, 0x97, 0xAF, 0x74, 0x65, 0xF2, 0x5F, 0x30, 0x73,  
 0x64, 0x0F, 0x00, 0x72, 0xC6, 0xF7, 0xF8, 0xB9, 0x57, 0x03,  
 0x8D, 0xF1, 0xBB, 0xB0, 0x36, 0x05, 0x42, 0xCC, 0x17, 0xCD,  
 0xD4, 0x34, 0xED, 0x94, 0xFB, 0x9F, 0x0A, 0xF9, 0x90, 0x78,  
 0x46, 0xCB, 0x41, 0xDF, 0xB8, 0x7B, 0x61, 0x45, 0x39, 0xDB,  
 0x49, 0x9E, 0x01, 0x2F, 0x50, 0xCE, 0x4F, 0xEB, 0x55, 0x62,  
 0x0D, 0x0B, 0x1B, 0xD2, 0x2D, 0xC0, 0xA1, 0x96, 0x08, 0x68,  
 0x12, 0x21, 0x25, 0x6F, 0xA6, 0x4C, 0xD8, 0xD9, 0x07, 0x3C,  
 0x63, 0xD5, 0x71, 0xA3, 0x3E, 0x6D, 0x22, 0x58, 0xB2, 0xE4,  
 0x1F, 0x5A, 0x2E, 0x13, 0x27, 0x84, 0xA9, 0xBA, 0xAC, 0x3F,  
 0x48, 0xBE, 0x4E, 0x5E, 0x1C, 0xB6, 0xC4, 0x6E, 0x75, 0x8B,  
 0xE5, 0xEA, 0xFE, 0x6A, 0x29, 0x8F, 0x5C, 0xC9, 0x56, 0xBC,  
 0x03, 0xDC, 0x89, 0x5F, 0x26, 0x9F, 0x9C, 0xB1, 0x95, 0xCD,  
 0x11, 0xB0, 0x50, 0xC2, 0x87, 0x0C, 0xC2, 0x4E, 0xE5, 0x00  
]  
  
input\_s = "a"\*23  
**if** 0:  
 input\_list = [  
 97, 97, 97, 97, 97, 97, 97, 97, 97, 97, 97, 97, 97, 97, 97, 97, 97, 97, 97, 97, 97, 97, 97  
 ]  
**else**:  
 input\_list = [0x5C, 0xC9, 0x56, 0xBC, 0x03, 0xDC, 0x89, 0x5F, 0x26, 0x9F,  
 0x9C, 0xB1, 0x95, 0xCD, 0x11, 0xB0, 0x50, 0xC2, 0x87, 0x0C,  
 0xC2, 0x4E, 0xE5]  
  
  
t = []  
  
print(input\_list)  
  
t1 = 0  
index = 1  
  
**for** i **in** range(23):  
  
 t1 = (s[index] + t1) % 256  
 v41 = s[index]  
 s[index] = s[t1]  
 s[t1] = v41  
 v39 = (s[t1] + s[index]) % 256  
  
 temp = ~s[v39] & input\_list[i] | ~input\_list[i] & s[v39]  
 # temp = s[v39] ^ input\_list[index]  
 t.append(temp)  
  
 index += 1  
  
print(t)  
  
**for** i **in** t:  
 print(chr(i), end='')  
  
print()  
**for** i **in** t:  
 print(hex(i), end=", ")

得：

flag{rC4\_0Llv2\_1s\_Ea3Y}