## 一、babyre

这题直接写个魔改的rc4算法计算s_box的值得到smc加密的异或值，然后进行patch操作即可还原出真实的judge加密逻辑：

```
s_box =
[0x83,0x24,0x84,0xcf,0x6c,0x8f,0x35,0x80,0x62,0xe6,0x3b,0x0c,0xc4,0x7c,0xad,0x
1b,0xbe,0xbc,0x75,0x01,0x91,0x56,0xf5,0xb8,0x03,0xc9,0xcd,0xa8,0x85,0x56,0xdc,
0xbb,0x5a,0xd4,0x52,0x09,0xd5,0xeb,0x8b,0x3c,0x24,0xfa,0xda,0x42,0x68,0xb4,0xf
9,0x42,0x8a,0xd0,0x13,0x52,0xe4,0x87,0xf3,0x09,0xc2,0xcd,0x7e,0x17,0x53,0x72,0
xfc,0x1b,0x53,0x99,0x77,0x86,0x10,0x7b,0x61,0x44,0x94,0xc2,0x00,0x5d,0x18,0x00
,0xa9,0xb0,0x38,0xc5,0x12,0x51,0x2d,0xd5,0xa4,0x5e,0x3b,0xae,0xba,0x74,0x17,0x
fa,0xc0,0xb4,0xad,0x38,0xd2,0xa2,0xf4,0x0e,0x5e,0xf9,0x2a,0x27,0x23,0x80,0x28,
0x86,0x46,0x80,0x04,0x7d,0xb9,0xb6,0xb5,0x42,0xe1,0x38,0x3c,0x99,0xb4,0x14,0xe
3,0xb9,0x8e,0x29,0x2c,0x97,0x5c,0x07,0xb9,0xb1,0xda,0xf6,0x3d,0x60,0x43,0x49,0
x67,0x04,0x32,0xb5,0x65,0x4e,0x7f,0xa4,0xd4,0xf5,0x29,0x49,0x2e,0x83,0x6a,0x93
,0x99,0x10,0xf8,0x96,0xa9,0xdf,0x7d,0xb6,0x1a,0x75,0x7a,0xdc,0xb5,0xec,0xf4,0x
64,0x8e,0x09,0xf3,0xef,0x69,0x04,0x48,0xf5,0x35,0x98,0x61,0x0f,0x9b,0xe9,0xb8,
0x24,0x57,0xcd,0xac,0xe5,0x1e,0x63,0x7d,0x6e,0x08,0x98,0xf2,0x55,0x78,0x57,0x0
c,0xf7,0xac,0x38,0x44,0xfb,0xb7,0x37,0x9e,0x0d,0x5f,0x0c,0xfc,0xc7,0x3d,0xfb,0
xf6,0xb4,0xca,0x6a,0xac,0x8c,0xc0,0x48,0xe8,0x9c,0x6e,0x2c,0xa7,0xc2,0x96,0x58
,0x6b,0x67,0x34,0xa7,0x2e,0x6f,0xfa,0x7c,0x0a,0x33,0x45,0x05,0xca,0x6f,0x4d,0x
9f,0x90,0xc6,0xa1,0xbf,0xc9,0x21,0x68,0x88,0xed,0xce,0xc9,0xf5,0x5b,0xf6,0x1a,
0xce,0x4a,0x0e,0xce,0xba,0x6f,0x32,0x65,0x25,0xc5,0x07,0xbe,0x4b,0xd5,0x96,0xc
d,0x7e,0x51,0x99,0x6b,0xd0,0xdb,0x7f,0xf8,0x3b,0xf8,0x18,0x57,0xf3,0xa9,0xf6,0
x1e,0x1c,0x4a,0xbb,0x15,0xc5,0xc5,0xcd,0x4b,0xe8,0xe7,0xa7,0x18,0x43,0x8e,0xb4
,0x2e,0x6a,0xa7,0x72,0x4c,0x84,0xc0,0xaf,0x4b,0x41,0x58,0x96,0x5c,0x48,0xa7,0x
d3,0x9a,0x03,0x16,0x4f,0x74,0x2a,0x59,0x7f,0xf4,0x6d,0xa6,0xcd,0xcd,0x93,0xbc,
0xe4,0xbf,0x03,0xfb,0xd6,0xc3,0xf4,0x35,0xac,0xad,0x40,0xd0,0x3e,0xd7,0xa5,0x5
0,0x71,0x0f,0x6a,0x20,0xa5,0xf0,0xa0,0x34,0x27,0x20,0x0f,0x34,0x60,0x37,0xb2,0
x0e,0x0a,0x76,0xfd,0xd4,0x93,0x4d,0xb6,0xb9,0x4e,0xad,0x98,0x9e,0xd9,0x25,0x65
,0x20,0x40,0x01,0xa1,0xc9,0xf4,0x11,0xa9,0x9c,0xe7,0x40,0x9a,0xfa,0x5c,0xac,0x
72,0x2e,0x0b,0xf7,0x2a,0xd4,0x29,0x00,0x05,0xed,0x35,0xe3,0xbc,0xc5,0xa8,0x37,
0x79,0xa7,0x17,0xbc,0xe7,0x36,0x9a,0x4e,0xa7,0x37,0xeb,0x6a,0xa8,0x19,0x81,0x9
0,0xc0,0x65,0x58,0x74,0xc1,0x1e,0x86,0x81,0x10,0xf3,0x99,0xb1,0x34,0x4c,0x5e,0
x10,0xc9,0x92,0x7e,0x61,0x8e,0x9e,0xb4,0x12,0x7b,0x70,0xab,0x20,0xba,0xaf,0x4c
,0xba,0x2c,0x67,0x87,0x98,0xe0,0x87,0x0f,0x8e,0x4e,0x12,0x85,0xb7,0x17,0x98,0x
4b,0xa4,0x53,0x2e,0x4f,0xb2,0x44,0x5d,0xed,0xde,0x1d,0xd7,0x3e,0x79,0xca,0xd3,
0x06,0xed,0xdb,0x82,0xf8,0x70,0x62,0xc8,0xdb,0x16,0xca,0xcd,0xee,0x7b,0x6a,0x9
5,0xcd,0xc3,0x9b,0x1c,0xa1,0x47,0xa7,0x79,0x7a,0x46,0x9f,0x85,0x89,0x74,0xf7,0
x9c,0x86,0xd5,0xcf,0x57,0xfa,0xf7,0xe8,0x57,0xe7,0x2f,0xd9,0x6f,0x3c,0xca,0x13
,0xd0,0xb6,0xa4,0xb9,0x9a,0xb4,0x25,0x87,0xeb,0xa2,0x3e,0xf0,0x12,0xe1,0x42,0x
6e,0x2b,0x76,0x3e,0x24,0xbe,0xbd,0x03,0x5e,0xb6,0x61]

n = (0x0000000000402969-0x000000000040272D)
for i in range(n):
  PatchByte(0x000000000040272D+i, Byte(0x000000000040272D+i) ^ s_box[i])
```

二、计算aes加密的key

直接将密文拖进去程序内存，改1为0即可得到key

```
key=“th1s1sth3n1c3k3y”
```

三、对最后一步进行爆破，能得到30多组解，只有一组能解出正确的flag，反向进一步逆向那个迭代异或，从而得到aes加密的密文，进行2段aes解密出flag：

```
# -*- coding: utf-8 -*-
from Crypto.Cipher import AES
from Crypto.Util.Padding import unpad
from binascii import *
import hashlib
import libnum
from Crypto.Util.number import *
enc = [189, 173, 180, 132, 16, 99, 179, 225, 198, 132, 45, 111, 186, 136, 116, 196, 144, 50, 234, 46, 198, 40, 101, 112, 201, 117, 120, 160, 11, 159, 166]

for j in range(256):
    a = [j]
    for i in range(31):
        a.append(((enc[i] ^ ((a[i]^0x13)*2+7))-(a[i]%9)-2)&0xff)
    # s = "".join(map(chr,a))
    if a[31]==0xc4:
        print(a)

flag = [0x4d,0x77,0x5e,0x0f,0xb3,0x4d,0x99,0xa6,0x8a,0xfa,0x54,0xb3,0x1e,0x96,0x91,0x7c,0x18,0x85,0xf8,0x30,0x5e,0x61,0xba,0x34,0x1c,0xe9,0x84,0x45,0x0b,0x38,0xbe,0xc4]
#这是正确的flag，测试出来的，有30多组，一个个测试

for i in xrange(len(flag)-1,-1,-1):
  for j in xrange(i//4-1,-1,-1):
    flag[i]^=flag[j]
print flag
flag = [77, 119, 94, 15, 254, 0, 212, 235, 176, 192, 110, 137, 122, 242, 245, 24, 115, 238, 147, 91, 134, 185, 98, 236, 137, 124, 17, 208, 7, 52, 178, 200]

c1 = b'\x4d\x77\x5e\x0f\xfe\x00\xd4\xeb\xb0\xc0\x6e\x89\x7a\xf2\xf5\x18'
c2 = b'\x73\xee\x93\x5b\x86\xb9\x62\xec\x89\x7c\x11\xd0\x07\x34\xb2\xc8'

des_crypto = b'\x0a\xf4\xee\xc8\x42\x8a\x9b\xdb\xa2\x26\x6f\xee\xee\xe0\xd8\xa2'
#将密文放进去内存，然后改下1为0获得输入key=th1s1sth3n1c3k3y
aes_key = b"th1s1sth3n1c3k3y"
def aes_decrypt(cipher, key=aes_key):
    aes = AES.new(key,mode=AES.MODE_ECB)
    return aes.decrypt(cipher)

print aes_decrypt(c1)+aes_decrypt(c2)
#GWHT{th1s_gam3_1s_s0_c00l_and_d}
```