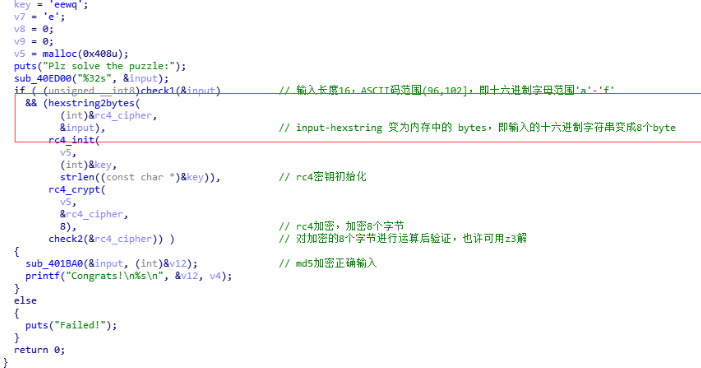
题目分析：



1. sub\_401C70函数会判断输入字符串的长度和逐位判断字符所在区间（‘a’ <= str[i] <= 'f'）

2. sub\_401B60用于将输入的16进制字符串转换为byte型数组（使用sprintf格式化输出）

3. sub\_401850和sub\\_4018D0用于初始化sbox和rc4加密，其中密钥为qwee

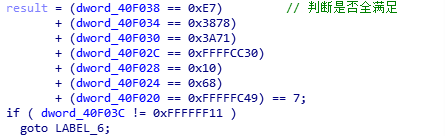
4. sub\_401950用于检查dword数据运算结果，用于检查输入字符串是否正确

5. sub\_401BA0用于md5加密flag并输出flag

调试程序，在rc4加密的异或运算处下断点dump下八个重要数据，分别为[0x7C,0xAB,0x2D,0x91,0x2F,0x98,0xED,0xA9]



逆向sub\_401950，可发现经rc4处理后的密文必为0~9，并保证以下条件即可：



写出C爆破脚本：

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*start\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

#include <stdio.h>

#include <stdbool.h>

#include <string.h>

bool Check(char \*str);

int main(){

int i = 0;

long a = 99999999;

//12345678

while(i <= a){

char str[10] = {0};

sprintf(str,"%08d",i);

if(Check(str)){

printf("TRUE!!!!!: %s",str);

goto label;

break;

}

if(i % 1000 == 0){

puts(str);

}

i++;

}

puts("falied\n");

label:

getchar();

getchar();

}

bool Check(char \*str){

int dword\_40F000 = 0xA;

int dword\_40F020 = 0x8A;

int dword\_40F024 = 0x1A1;

int dword\_40F028 = 0x12A;

int dword\_40F02C = 0x269;

int dword\_40F030 = 0x209;

int dword\_40F034 = 0x68;

int dword\_40F038 = 0x39F;

int dword\_40F03C = 0x2C8;

int result = 0;

for(int i = 0;i < 8;i++){

switch (str[i] - 48)

{

case 0:

dword\_40F028 &= dword\_40F038; // 12Ah

dword\_40F02C \*= dword\_40F028;

break;

case 1:

if ( !dword\_40F02C )

goto LABEL\_6;

dword\_40F028 /= dword\_40F02C;

dword\_40F024 += dword\_40F034;

break;

case 2:

dword\_40F030 ^= dword\_40F034;

dword\_40F03C += dword\_40F020;

break;

case 3:

dword\_40F03C -= dword\_40F030;

dword\_40F030 &= dword\_40F024;

break;

case 4:

dword\_40F034 \*= dword\_40F020;

dword\_40F02C -= dword\_40F038;

break;

case 5:

dword\_40F020 ^= dword\_40F02C;

dword\_40F038 -= dword\_40F03C;

break;

case 6:

if ( !dword\_40F03C )

goto LABEL\_6;

dword\_40F034 |= dword\_40F024 / dword\_40F03C;

dword\_40F024 /= dword\_40F03C;

break;

case 7:

dword\_40F038 += dword\_40F028;

dword\_40F034 |= dword\_40F024;

break;

case 8:

dword\_40F020 \*= dword\_40F02C;

dword\_40F030 -= dword\_40F03C;

break;

case 9:

dword\_40F028 += dword\_40F034;

dword\_40F02C ^= dword\_40F030;

default:

break;

}

}

//printf("str = %s\n %0x %0x %0x %0x %0x %0x %0x %0x\n",str,dword\_40F038,dword\_40F034,dword\_40F030,dword\_40F02C,dword\_40F028,dword\_40F024,dword\_40F020,dword\_40F03C);

result = (((dword\_40F038 == 0xE7) // 判断是否全满足

+ (dword\_40F034 == 0x3878)

+ (dword\_40F030 == 0x3A71)

+ (dword\_40F02C == 0xFFFFCC30)

+ (dword\_40F028 == 0x10)

+ (dword\_40F024 == 0x68)

+ (dword\_40F020 == 0xFFFFFC49)) == 7);

if ( dword\_40F03C != 0xFFFFFF11 )

goto LABEL\_6;

if(result == 1){

return true;

}

LABEL\_6:

return false;

}

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*end\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

爆破结果为：61495072

得到的八个数字，然后写出python脚本得到正确输入。

xor\_data = [0x7C,0xAB,0x2D,0x91,0x2F,0x98,0xED,0xA9]  
result\_data = [6,1,4,9,5,0,7,2]  
flag = ""  
for i in range(len(xor\_data)):  
 flag += "%x"% (xor\_data[i] ^ result\_data[i])

得到结果：7aaa29982a98eaab

运行程序，输入正确字符串，得到flag：

flag{5cb92582-66a8-e5b7-d3bf-3b99df8ac7f0}