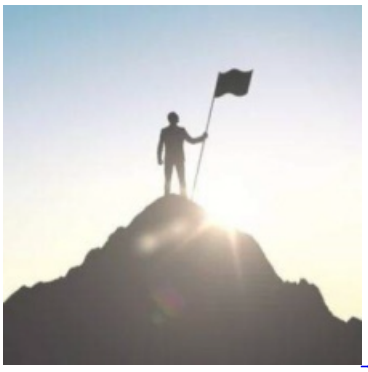
XCTF crypto Easy_Crypto

原创

A_dmins 于 2019-06-08 17:39:22 发布 975 收藏 1

分类专栏： CTF题 一天一道CTF XCTF

本文链接：https://blog.csdn.net/qq_42967398/article/details/91346318



XCTF crypto Easy_Crypto

一天一道**CTF题目，能多不能少**

下载文件，得到两个文件，一个源码（用notpad++打开有格式，记事本看的眼睛痛）：

```
get buf unsign s[256]

get buf t[256]

we have key:hello world

we have flag:??????????????????????????????


for i:0 to 256

set s[i]:i

for i:0 to 256
    set t[i]:key[(i)mod(key.lenth)]

for i:0 to 256
    set j:(j+s[i]+t[i])mod(256)
        swap:s[i],s[j]

for m:0 to 37
    set i:(i + 1)mod(256)
    set j:(j + S[i])mod(256)
    swap:s[i],s[j]
    set x:(s[i] + (s[j]mod(256))mod(256))
    set flag[m]:flag[m]^s[x]

fprint flagx to file
```

可以看出，这个就是解密的脚本，给了我们enc文件，我们照着这个文件源码来就好了
编写解密脚本：

```
key = "hello world"
flag = open('enc.txt','r',encoding = 'ISO-8859-1').read()   #这个编码问题真的秀，不加这个会出现编码错误

s = list(range(256))            #初始化列表

j = 0

for i in range(256):
 j = (j + s[i] + ord(key[i % len(key)])) % 256
 s[i],s[j] = s[j],s[i]

strings = ""
i = 0
j = 0
for m in flag:
 i = (i + 1) % 256
 j = (j + s[i]) % 256
 s[i],s[j] = s[j],s[i]
 x = (s[i] + (s[j] % 256)) % 256
 strings += chr(ord(m) ^ s[x])
print(strings)
```

get flag！！