攻防世界 Crypto高手进阶区 5分题 Easy_Crypto

原创

思源湖的鱼 于 2021-01-10 15:06:37 发布 163 收藏

分类专栏： ctf 文章标签： ctf 攻防世界 crypto

本文链接：https://blog.csdn.net/weixin_44604541/article/details/112428129

前言

继续ctf的旅程

攻防世界Crypto高手进阶区的5分题

本篇是Easy_Crypto的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

解题过程

得到一段代码和一个密文

```
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
```

这就根据伪码逆着来就是了

```
s = list(range(256))
t = []
key = "hello world"

for i in range(256):
    t.append(key[i % len(key)])
print(t)

j = 0
for i in range(256):
    j = (j + s[i] + ord(t[i])) % 256
    s[i], s[j] = s[j], s[i]
print(s)

c = open("enc.txt","rb").read()
i = 0
j = 0
flag = ""
for ci in c:
    i = (i + 1) % 256
    j = (j + s[i]) % 256
    s[i], s[j] = s[j], s[i]
    x = (s[i] + (s[j] % 256)) % 256
    flag += chr(ci ^ s[x])
print(flag)
```

```
------------------ RESTART: C:\Users\Y390\Desktop\enc\1.py ------------------
['h', 'e', 'l', 'l', 'o', ' ', 'w', 'o', 'r', 'l', 'd', 'h', 'e', 'l', 'l', 'o',
 ' ', 'w', 'o', 'r', 'l', 'd', 'h', 'e', 'l', 'l', 'o', ' ', 'w', 'o', 'r', 'l',
 'd', 'h', 'e', 'l', 'l', 'o', ' ', 'w', 'o', 'r', 'l', 'd', 'h', 'e', 'l', 'l',
 'o', ' ', 'w', 'o', 'r', 'l', 'd', 'h', 'e', 'l', 'l', 'o', ' ', 'w', 'o', 'r',
 'l', 'd', 'h', 'e', 'l', 'l', 'o', ' ', 'w', 'o', 'r', 'l', 'd', 'h', 'e', 'l',
 'l', 'o', ' ', 'w', 'o', 'r', 'l', 'd', 'h', 'e', 'l', 'l', 'o', ' ', 'w', 'o',
 'r', 'l', 'd', 'h', 'e', 'l', 'l', 'o', ' ', 'w', 'o', 'r', 'l', 'd', 'h', 'e',
 'l', 'l', 'o', ' ', 'w', 'o', 'r', 'l', 'd', 'h', 'e', 'l', 'l', 'o', ' ', 'w',
 'o', 'r', 'l', 'd', 'h', 'e', 'l', 'l', 'o', ' ', 'w', 'o', 'r', 'l', 'd', 'h',
 'e', 'l', 'l', 'o', ' ', 'w', 'o', 'r', 'l', 'd', 'h', 'e', 'l', 'l', 'o', ' ',
 'w', 'o', 'r', 'l', 'd', 'h', 'e', 'l', 'l', 'o', ' ', 'w', 'o', 'r', 'l', 'd',
 'h', 'e', 'l', 'l', 'o', ' ', 'w', 'o', 'r', 'l', 'd', 'h', 'e', 'l', 'l', 'o',
 ' ', 'w', 'o', 'r', 'l', 'd', 'h', 'e', 'l', 'l', 'o', ' ', 'w', 'o', 'r', 'l',
 'd', 'h', 'e', 'l', 'l', 'o', ' ', 'w', 'o', 'r', 'l', 'd', 'h', 'e', 'l', 'l',
 'o', ' ', 'w', 'o', 'r', 'l', 'd', 'h', 'e', 'l', 'l', 'o', ' ', 'w', 'o', 'r',
 'l', 'd', 'h', 'e', 'l', 'l', 'o', ' ', 'w', 'o', 'r', 'l', 'd', 'h', 'e', 'l']
[172, 88, 68, 171, 39, 122, 11, 54, 98, 37, 194, 120, 214, 183, 41, 50, 24, 160,
 36, 15, 189, 31, 213, 102, 246, 203, 35, 94, 241, 118, 236, 108, 251, 117, 252,
 168, 42, 138, 8, 44, 243, 142, 33, 137, 59, 217, 4, 247, 173, 254, 97, 66, 239,
 113, 32, 56, 139, 220, 83, 169, 78, 60, 80, 96, 119, 87, 91, 197, 218, 77, 207,
 107, 230, 86, 18, 7, 3, 63, 199, 116, 72, 49, 244, 26, 253, 196, 52, 177, 82, 1
91, 215, 73, 204, 219, 216, 150, 101, 167, 248, 195, 22, 242, 153, 237, 233, 103
, 14, 92, 132, 13, 198, 55, 249, 76, 145, 140, 58, 161, 9, 16, 28, 210, 208, 157
, 128, 12, 147, 104, 131, 85, 6, 235, 125, 179, 45, 165, 158, 185, 184, 181, 151
, 222, 47, 67, 21, 121, 149, 43, 129, 211, 27, 225, 205, 152, 61, 146, 29, 79, 1
00, 231, 164, 155, 90, 200, 226, 48, 144, 53, 130, 71, 143, 123, 227, 250, 38, 1
82, 70, 170, 34, 245, 62, 178, 180, 57, 46, 148, 193, 202, 124, 174, 2, 201, 110
, 232, 188, 51, 141, 234, 99, 162, 95, 30, 115, 154, 89, 163, 192, 93, 65, 166,
212, 111, 156, 135, 64, 133, 19, 5, 74, 238, 0, 186, 20, 223, 114, 23, 229, 127,
 134, 190, 175, 221, 10, 240, 81, 126, 187, 75, 69, 228, 106, 255, 40, 17, 84, 2
09, 159, 109, 176, 206, 224, 136, 25, 112, 105, 1]
EIS{55a0a84f86a6ad40006f014619577ad3}
```


得到flag

结语

简单题