攻防世界 Crypto高手进阶区 4分题 onetimepad

原创

思源湖的鱼 于 2020-12-22 13:18:42 发布 508 收藏 3

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/111514621

前言

继续ctf的旅程

攻防世界Crypto高手进阶区的4分题

本篇是onetimepad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

得到一个密文文件和一段py

```python
#!/usr/bin/env python
# coding=utf-8

from os import urandom

def process(m, k):
    tmp = m ^ k
    res = 0
    for i in bin(tmp)[2:]:
        res = res << 1;
        if (int(i)):
            res = res ^ tmp
        if (res >> 256):
            res = res ^ P
    return res

def keygen(seed):
    key = str2num(urandom(32))
    while True:
        yield key
        key = process(key, seed)

def str2num(s):
    return int(s.encode('hex'), 16)

P = 0x1000000000000000000000000000000000000000000000000000000000000425L

true_secret = open('flag.txt').read()[:32]
assert len(true_secret) == 32
print 'flag{%s}' % true_secret
fake_secret1 = "I_am_not_a_secret_so_you_know_me"
fake_secret2 = "feeddeadbeefcafefeeddeadbeefcafe"
secret = str2num(urandom(32))

generator = keygen(secret)
ctxt1 = hex(str2num(true_secret) ^ generator.next())[2:-1]
ctxt2 = hex(str2num(fake_secret1) ^ generator.next())[2:-1]
ctxt3 = hex(str2num(fake_secret2) ^ generator.next())[2:-1]
f = open('ciphertext', 'w')
f.write(ctxt1+'\n')
f.write(ctxt2+'\n')
f.write(ctxt3+'\n')
f.close()
```

密文内容

```
af3fcc28377e7e983355096fd4f635856df82bbab61d2c50892d9ee5d913a07f
630eb4dce274d29a16f86940f2f35253477665949170ed9e8c9e828794b5543c
e913db07cbe4f433c7cdeaac549757d23651ebdccf69d7fbdfd5dc2829334d1b
```

逆着来

```
from os import urandom

def process(m, k):
    tmp = m ^ k
    res = 0
    for i in bin(tmp)[2:]:
        res = res << 1;
        if (int(i)):
            res = res ^ tmp
        if (res >> 256):
            res = res ^ P
    return res

def keygen(seed):
    key = str2num(urandom(32))
    while True:
        yield key
        key = process(key, seed)

def str2num(s):
    return int(s.encode('hex'), 16)

src1 = 0xaf3fcc28377e7e983355096fd4f635856df82bbab61d2c50892d9ee5d913a07f
src2 = 0x630eb4dce274d29a16f86940f2f35253477665949170ed9e8c9e828794b5543c
src3 = 0xe913db07cbe4f433c7cdeaac549757d23651ebdccf69d7fbdfd5dc2829334d1b

fake_secret1 = "I_am_not_a_secret_so_you_know_me"
fake_secret2 = "feeddeadbeefcafefeeddeadbeefcafe"

k2 = src2 ^ str2num(fake_secret1)
k3 = src3 ^ str2num(fake_secret2)

kt = k3
for i in range(255):
    kt = process(kt, 0)

seed = kt ^ k2
print "SEED:", seed
assert process(k2, seed) == k3

kt = k2
for i in range(255):
    kt = process(kt, 0)

k1 = kt ^ seed
print "K1:", k1
assert process(k1, seed) == k2

m = k1 ^ src1
print hex(m)[2:-1].decode("hex")
```

得到flag：`flag{t0_B3_r4ndoM_en0Ugh_1s_nec3s5arY}`

结语

然后查到一个很好的数学过程

攻防世界-密码学-onetimepad