De1CTF 之 Crypto1 xoz WriteUp

原创

傅小凤- 于 2019-08-07 13:38:18 发布 328 收藏 1

分类专栏： 计算机安全 CTF 文章标签： CTF 信息安全 密码学

本文链接：https://blog.csdn.net/qq_33877253/article/details/98741813


计算机安全 同时被 2 个专栏收录

7 篇文章 0 订阅

订阅专栏


CTF

2 篇文章 0 订阅

订阅专栏

De1CTF 之 Crypto1 : xoz WriteUp

De1CTF中Crypto方向第一题——xoz

```
from itertools import *
from data import flag,plain

key=flag.strip("de1ctf{").strip("}")
assert(len(key<38))
salt="WeAreDe1taTeam"
ki=cycle(key)
si=cycle(salt)
cipher = ''.join([hex(ord(p) ^ ord(next(ki)) ^ ord(next(si)))[2:].zfill(2) for p in plain])
print cipher
# output:
# 49380d773440222d1b421b3060380c3f403c3844791b202651306721135b6229294a3c3222357e766b2f15561b35305e3c3b670e49382c29
5c6c170553577d3a2b791470406318315d753f03637f2b614a4f2e1c4f21027e227a4122757b446037786a7b0e37635024246d60136f780254
3e4d36265c3e035a725c6322700d626b345d1d6464283a016f35714d434124281b607d315f66212d671428026a4f4f79657e34153f3467097e
4e135f187a21767f02125b375563517a3742597b6c394e78742c4a725069606576777c314429264f6e330d7530453f22537f5e3034560d2214
6831456b1b72725f30676d0d5c71617d48753e26667e2f7a334c731c22630a242c7140457a42324629064441036c7e646208630e745531436
b7c51743a36674c4f352a5575407b767a5c747176016c0676386e403a2b42356a727a04662b4446375f36265f3f124b724c6e3465447062776
4102506342001662922 5b43432428036f29341a2338627c47650b264c477c653a67043e6766152a485c7f33617264780656537e5468143f305
f4537722352303c3d4379043d69797e6f3922527b24536e310d653d4c33696c635474637d0326516f745e610d773340306621105a7361654e
3e392970687c2e335f3015677d4b3a724a4659767c2f5b7c16055a126820306c14315d6b59224a27311f747f336f4d5974321a22507b22705a2
26c6d446a37375761423a2b5c29247163046d7e4703224437750830075172712632 6f117f7a38670c2b23203d4f27046a5c5e1532601126292
f577776606f0c6d0126474b2a73737a41316362146e581d7c1228717664091c
```

解题过程

---

1. 根据题目信息可知，

$$cipher = plain \oplus key \oplus salt$$

得到的。

2. 先将cipher、salt转为10进制后计算

$$decode = cipher \oplus salt.$$

查看desalt中相同数字出现频率，猜测密钥长度可能为30. 猜测明文主要由英文字母、数字和常用标点（","、"."等）组成，key主要由字母、数字、”_"组成。

根据此猜想，对key进行爆破，具体代码如下：

```
l=30 #猜测密钥长度为30
PossibleFlag=[] #存储可能的key值
for k in range(l):
    pf=[] #key中第k个字符的可能值
    j=1 #遍历ASSCII码中10个数字+52个字母+"_"
    while(j<123):
        bool=1
        if((j>=ord('0') and j<=ord('9'))or(j>=ord('A') and j<=ord('Z'))or(j>=ord('a') and j<=ord('z'))or(j==ord('_'))):
            #判断解密后明文是由英文字母、数字和常用标点（","、"."等）组成
            for i in range(len(decode)//l):
                res=decode[i*l+k]^j #将decode与可能为key的字符异或
                if(res<32 or res>122 or (res<=96 and res>=91) or (res>=35 and res<=39) or res==34 or res==42):
                    bool=0
                    continue
            if(flag==1):
                pf.append(chr(j))
        j=j+1
    PossibleFlag.append(pf)
    print(k,end=' ')
    print(pf)
```

得到每一位key的可能值：

```
0 ['W']
1 ['2', '3', 'i', 'j', 'k']
2 ['l']
3 ['b', 'c']
4 ['0', 'h', 'j']
5 ['4', '5', 'l']
6 ['3']
7 ['t']
8 ['N', 'O', 'P', 'S']
9 ['j']
10 ['o']
11 ['0', '1', 'i', 'u']
12 ['4', '7', 'n', 'o']
13 ['u']
14 ['5', '8', '9', 'a', 'l', 'm']
15 ['4', '5', 'l', 'o']
16 ['u']
17 ['n']
18 ['1']
19 ['5', 'o']
20 ['j']
21 ['O']
22 ['t']
23 ['3']
24 ['m']
25 ['1', 'j']
26 ['0', '1', '9', 'c', 'h']
27 ['5', '6', 'm', 'z']
28 ['3', 'i', 'k', 'z']
29 ['W', 'Z']
```

分别取可能key中的第一项解密密文，得到部分正确的明文：

`lo ga0th!I e5 nnt l5ve thd6ywi ti li7e dyervFos th?y in u;<e a!tio,saod d(ross n5te;Buus9ti s!mx 1east u2at!lov?s whaus-he y!dds)isd,Wi5 io de)pite n5yvi ev hsypldasd> tn do.e.Nor!2+e mhnd <arr wh.h uhy .onguea ytu nd ee5igiteeaNos te4der fd65in g!tn ;asd tn/chds p(one,Nn!yta sue- 7or!smd6l,!des3re to!1< i nwiue=To!anxzseosua6 feasus.it h!tie< amondtBuu myzfive v:-s, oos 4y givdzseoseszcanDir ,ad e!ooeyfonlir2 hdartzfrom r6+vi nf uh<e,Vho!6eawes /nswayd7yth e!lhk<ners n< a!manvThy ps<,d hdast9s rlaw? aod v;ssal v!<tc h!tn ;e.Nnlxzmy!pla=ue tht yfa r!l!c6unu mxzgahn,T2at shds-ha`

观察明文，猜测”mx“可能为”my“，”l5ve“可能为”love“，”lov？s“可能为”loves“… 据此调整key中各项，得：

lo faith I d5 nnt love thd6ywi ti mine eyesvFos they in u;<e a!thousand e(ross note;Buus9ti s!my heart t2at!loves whaus-he y!despise,Wh5 io despite n5yvi ev is please> tn dote.Nor!2+e mhne ears wi.h uhy tonguea ytu nd delightedaNos tender fd65in g!to base to/chds prone,Nn!yta sue, nor sme6l,!desire to!1< i nwitedTo anyzseosual feasus.it h!thee alonetBuu my five v:-s, oor my fivezseoses canDir ,ad e!one foolis2 hdart from r6+vi nf thee,Who 6eawes unswayd7yth e!likeness o< a!man,Thy ps<,d hdart`s slav? aod vassal v!<tc h!to be.Onlyzmy!plague tht yfa r!I count myzgahn,That shds-ha

搜索已解密的单词:“faith”、“love”、“thousand”、“my heart”，得到莎士比亚的诗《SONNET 141： PARAPHRASE》，对照诗文修改key，得到正确flag:

```
flag="W3lc0m3tOjo1nu55un1ojOt3m0cl3W"
```