网鼎2018CTF第四场 _Crypto

原创

0x0 shenyue

理清代码流程，按照给的注册流程跑一遍

```
==== administration console ====
1. sign up
2. log in
3. private key generation
-1. command execution
> 1
id: 123
pw: 123
successfully registered
> 2
id: 123
pw: 123
logged in as 123
> 3
which command do you want to execute: 123
generating your key associated with 123
you can use the key to execute a command
your id+cmd combination results in b48499a53ed7f0849c2426390d8650d58d6cfad3f51a48f358242bf0d1c49d25
Kindly reminder: please don't give your key to anyone
> -1
what command? 123
who signed this command? 123
give me the signed document: b48499a53ed7f0849c2426390d8650d58d6cfad3f51a48f358242bf0d1c49d25
ok, let me check if this sign is issued by this system
ok, good good
flag is: flag{5a5885ff-6870-47d0-8056-1cbef8fc38b1}
```

0x1 number

根据多次给的随机数找p，通过素数分解：

X1 * p + z = A1

X2 * p + z = A2

相减得（x1-x2）* p = a1 -a2，上http://factordb.com/index.php分解找到

P=20643184508375497509901425309830189219256484252546253313212672404909511152151751962105566142893662607952878805280324792967821152826173910569606109232157178321954025088541763767496991471749807755881672057143612683492373146478874912031449429877547343200007317921565201931558587150989127697616749556886072226108488640969646333132066766640911278089510374856595417814519288982765907919236374979232083949184447529843964240473737357957726119171581175545581351787814630542239184690006874044284138392010446102143023504991769427644639437580992687579429050105266693507629625329212765592593452506965964060515249687177513999999079

从X1 * p + flag % p = A1公式看出A1 / p == flag % p，flag == A1 / p + p*i

得到i=0时，解出flag。

```
z =204278710027668642984663723467554341041652238644649604783911294133769957064321382318161297654498202 9

p = 20643184508375497509901425309830189219256484252546253313212672404909511152151751962105566142893662 6

for i in xrange(1000):
    s = hex(z % p + i * p)
    if "666c6167" in s:
        print s
        break
```

0x2 shanghai

先做词频分析不对，测了其他的，在这个网站上跑出来了，维吉尼亚密码。

https://www.guballa.de/vigenere-solver

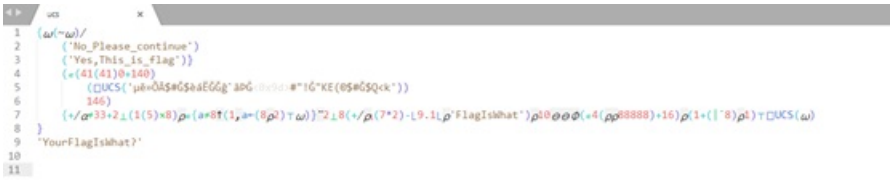
```
epeats it until it matches the length of the plaintext, for example, the key

 holds the letters a to z (in shifted order). although there are 26 key rows
: {l, e, m, o, n}. flag, '{' and 'vigenereisveryeasyhuh' and '}' for success.
corresponding key row. the next letter of the key is chosen, and that row is
 msg-col] is the enciphered letter.

paired with l, the first letter of the key. therefore, row l and column a of
is used. the letter at row e and column t is x. the rest of the plaintext is
```

0x3 APL

先Base64解码，然后拖到sublime，在github上面找到高亮的语法



到这步需要找到APL语言的语法学习分析了,看到一篇讲的挺详细：

https://xz.aliyun.com/t/2666