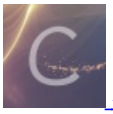
DASCTF X SU-2022-Crypto-FlowerCipher(利用已知条件爆破)

原创

Mango|Feng 于 2022-03-30 21:00:28 发布 60 收藏

分类专栏： python 笔记 密码学 文章标签： python 安全 算法



DASCTF X SU-2022-Crypto-FlowerCipher(利用已知条件爆破)

之前有写过DASCTF X SU-2022-Crypto-FlowerCipher之暴力暴力求解法(z3约束器)

然后虽然很简单粗暴，但我们还是换一种思路来解这道题。

感谢茂霖哥哥的解析

解析也不过再次赘述了,可以看我上一篇文章里面有写.

这里重点提两点

- (1):flower = random.randint(0, 4096)，已告知随机数范围，可以爆破
- (2):验证爆破的flower是否正确在于:return x * (key ** 3 + flower)，将return返回值除以x后减去flower的值是否能开三次方根

基于以上两点以及之前的分析，我们能写出爆破解密脚本:

```
from Crypto.Util.number import *
from gmpy2 import *

L_k = 157201972689453483884294293513030069253873889272923047175945112593901941008508898527476533871972053924310530690436323403742526295294197768744108179277709223108086325816661818990
R_k = 139721425176294317602347104909475448503147767726747922243703132013053043430193232376860554749633894589164137720010858254771905261753520854314908256431590570426632742469003
flag=[]
while(L_k!=1):
    R_k2 = L_k%R_k
    tmp = L_k-R_k2
    for i in range(0,4096):
        if(iroot((tmp//R_k)-i,3)[1]):
            flag.append(chr(int(iroot((tmp//R_k)-i,3)[0])))
            break
    L_k=R_k
    R_k=R_k2
flag.reverse()
for j in flag:
    print(j,end="")
#3e807b66ef26d38e671ddcbb9c108250
```

总结

代码看起来简洁了许多许多,爆破条件也很巧妙。