easy_wa

发表于 2021-01-21 分类于 Challenge， 2020， 网鼎杯， 玄武组， Crypto
Challenge | 2020 | 网鼎杯 | 玄武组 | Crypto | easy_wa

点击此处获得更好的阅读体验

WriteUp来源

本WP由Vanish提供

题目考点

- *lrlr*

解题思路

bytectf原题lrlr的一个part

https://blog.csdn.net/qq_33458986/article/details/100699263

calc是一个多项式在GF(2)下的平方运算，我们要做的应该是求根。

但是这里给出的既约多项式的阶不大，我们一直平方下去，很快就能回到起点。所以直接拿密文去calc就行了。

先交互，过那个恶心的PoW ~~跟青龙组那个一样，再看看名字，同一个出题人，凑！~~，输入token拿到4组密文

然后每组分别解密

```
from os import urandom as ua
from Crypto.Util.number import *

magic=32805

def calc(m,p):
    res=0
    lens=hlen(p)
    for i in bin(m)[2:]:
        res*=2
        res^=m if i=='1' else 0
        res^=p if hlen(res) == lens else 0
    return res

def check(s):
    for i in s:
        if i not in "flag{0123456789bcde-_}\x00":
            return False
    return True

flags=[3723147309,80167590975210625 64,267529443716352603115102819467183104162,1100684987530421545357531311904678765141496031129550782143092830064584543786 60]
FLAG=""
r = 2
for flag in flags:
    r*=2
    while True:
        flag=calc(flag,magic + (1<<r*8))
        if check(long_to_bytes(flag)[:10]):
            FLAG+=(long_to_bytes(flag))
            print FLAG
            break
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2020/网鼎杯/玄武组/Crypto/qK1ndhamVCULjaM99EKfiR.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # 2020 # Crypto # 网鼎杯 # 玄武组
Safe_box
easy_sign_in