

# XCTF 幂数加密 WP

原创

lqvir 于 2020-12-13 20:07:16 发布 1489 收藏 2

文章标签: [密码学](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/weixin\\_46227016/article/details/111144229](https://blog.csdn.net/weixin_46227016/article/details/111144229)

版权

[原题目链接-幂数加密](#)

## 思路

下载附件得到一串数字

8842101220480224404014224202480122

没有头绪, 于是采用“题目攻击“

搜索幂数加密得到二进制加密方法, 得到

二进制幂数加密法就是应用这个原理, 由于英文字母只有26个字母, 由公式可知, 只要2的0、1、2、3、4、5次幂就可以表示31个单元。

通过用二进制幂数表示字母序号数来加密。例如

明文: donotpullyoureggsinonebasket

字母序号: 4 15 14 15 20 16 21 12 12 1 12 12 25 15 21 18 5 7 7 19 9 14 15 14 5 2 1 19 11 5 20

由于

$4 = 2^2$  所以D加密过之后是2: 15 =  $2^4 + 2^0 + 2^1 + 2^2 + 2^3$  所以O加密后是0100 同理得到上述明文的加密后的

并没有什么用。于是放弃了, 看了题解。

根据题解得到题目有提到一共八个字母, 那么原数字可以看成8段, 恰好7个0, 那么一段一个数字, 每个数字个位数字之和都小于26 (有点幂数加密的味道), 可以看成是偏移量, 就可以得到明文。

脚本如下

```
ans=[88421,122,48,2244,4,142242,248,122]
for i in ans:
    temp=0
    while i:
        temp+=i%10
        i//=10
    temp=ord('A')+temp-1
    print(chr(temp),end="")
```