【XCTF 攻防世界】CRYPTO 密码学 新手练习区 幂数加密

原创

Kal1 于 2020-08-07 21:29:38 发布 491 收藏 1

分类专栏： CTF刷题 密码学 文章标签： 密码学 python 安全

本文链接：https://blog.csdn.net/weixin_45844670/article/details/107870291

题目链接：https://adworld.xctf.org.cn/task/answer?type=crypto&number=5&grade=0&id=5120&page=1

下载附件，得到一串数字。没有头绪。查看wp

得知这是 **二进制幂数加密法**

百度链接： 二进制幂数加密法

从给出的一串字符可以看出，除第一组以外，每一个以0分隔的一组排列的数字都是从小到大

那么可以确定，以0分隔的每一组都是一个字符

不明白的可以举个例子：

明文：donotpullallyoureggsinonebasket

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=2^0+2^1+2^2+2^3所以O加密后是0123。同理得到上述明文的加密后的密文

密文：2 0123/123 0123 24/4 024 23 23/0 23 23/034 0123 024 14/02 012 012 014/03 123 /0123 123 02/1 0 014 013 02 24

那么我们直接用python脚本跑一下，可以得到flag

WELLDONE

```
a="884210122048022440401422420248012 2"
a=a.split("0")
flag=''
for i in range(0,len(a)):
    str = a[i]
    list=[]
    sum=0
    for j in str:
       list.append(j)
       length = len(list)
    for k in range(0,length):
       sum+=int(list[k])
    flag+=chr(sum+64)
print(flag)
```