

攻防世界 | 幂数加密

原创

Bravo!!! 于 2020-09-15 18:30:06 发布 1510 收藏 3

分类专栏: CTF 文章标签: 攻防世界 crypto

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_47982238/article/details/108605756

版权



[CTF 专栏收录该内容](#)

20 篇文章 2 订阅

订阅专栏

先看一下什么是幂数加密

二进制幂数加密法, 由于英文字母只有26个字母。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。

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: 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

题目描述: 你和小鱼终于走到了最后的一个谜题所在的地方, 上面写着一段话“亲爱的朋友, 很开心你对网络安全有这么大的兴趣, 希望你一直坚持下去, 不要放弃, 学到一些知识, 走进广阔的安全大世界”, 你和小鱼接过谜题, 开始了耐心细致的解答。flag为cyberpeace 你解答出的八位大写字母

题目上说结果为八位大写字母, 所以要把txt文件中的数字分为8组, 按0位间隔正好八组

8842101220480224404014224202480122

88421 0122 048 02244 04 0142242 0248 0122

23 5 12 12 4 15 14 5

W E L L D O N E

所以最终拿到flag: cyberpeace{WELLDONE}