ctf-攻防世界crypto基础区-幂数加密

原创

萌萌哒的baola 于 2020-08-01 11:16:08 发布 644 收藏 3

分类专栏： ctf题解

本文链接：https://blog.csdn.net/Claming_D/article/details/107727191

文章目录

0x01 题目

题目来源： CFF2016

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}

附件内容：

```
884210122048022440401422420248012 2
```

题目标题虽然是幂数加密，但是考察的确是云隐加密，两者的加密原理是一样的

0x02 预备知识

2.1 幂数加密

对26个字母进行排序得到

```
A  B  C  D  E  F  G  H  I  J  K  L  M  N  O  P  Q  R  S  T  U  V  W  X  Y  Z
1  2  3  4  5  6  7  8  9  10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
```

二进制数除了0和1的表示方法外，在由二进制转换成十进制的时候，还可以表示成2的N次方的形式。例如：$15=2^0+2^1+2^2+2^3$
并且任意的十进制数都可以用2^n或2^n+2^m+……的形式表示出来。
二进制幂数加密法就是应用这个原理，将从左到右取幂数进行排列，eg. 15==>0123

> 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
> 其中空格表示字母的间隔，/表示单词的间隔。
> 参考百度百科：https://baike.baidu.com/item/二进制幂数加密法/2410151?fr=aladdin
> 密文的特点是：密文只有01234

2.2 云隐加密

0124加密，又称云隐加密。其加密原理和幂数加密差不多，只不过没有取幂数，而是直接取每项的值求和

> 15 = 1+2+4+8
> 26=1+
> 那么密文就是1248

加密原理：使用 01248 四个数字，其中 0 用来表示间隔，其他数字以加法表示1-26。

0x03 题目分析

密文以01248组成，符合01248加密特点，可见这里并不是幂数加密
根据加密原理，写出如下python3脚本：

```
"""
云隐解密脚本
"""
ciphertext = "884210122048022440401422420248012 2"
ciphertext = ciphertext.split('0')  # 以0做分割，分成8块，方便对每块做加法
result = ""
for block in ciphertext:  # 遍历所有块，每块对应一个字母
    sum = 0
    for i in range(len(block)):  # 对每块内容做加法，得到对应的数字
        sum += int(block[i])
    result += chr(65 + sum - 1)  # A的ascii码是65，而sum是1->26，表示A->Z ，所以要减1，变成0->25再加上65，变成ascii：6
5-90表示A->Z
print(result)
```

0x04 总结

1.了解云隐加密原理
2.了解幂数加密原理

参考资料

百度百科：https://baike.baidu.com/item/二进制幂数加密法/2410151?fr=aladdin
博客：https://www.jianshu.com/p/038df5e957c5