

实验吧密码学WriteUp(四)

原创

Neil-Yale 于 2017-03-19 15:22:08 发布 5926 收藏

文章标签: [密码学](#) [base64](#) [密码](#) [解密](#) [CTF](#)

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/yalecaltech/article/details/63684999>

版权

1. 疑惑的汉字 (<http://www.shiyanbar.com/ctf/1876>)

复制密文内容百度得知是当铺密码

解密得到一串数字

于是再ASCII

得到flag

2. 奇怪的字符串 (<http://www.shiyanbar.com/ctf/1877>)

看到数字于是ascii

解码后发现后面有==

于是base64解之即可

3. 神秘字母 (<http://www.shiyanbar.com/ctf/1892>)

题目涉及线性代数中的逆矩阵的转置矩阵 (还好上学期学了线代)

先进行逆变换得到逆矩阵, 然后再进行转置得到转置矩阵进行乘法解密

根据矩阵乘法的规则将其排成2列, 注意用数字代替字母 (不是ascii, 而是1代表a, 2代表b...)

然后将密文dloguszjluswogaqy 写成

d l 4 12 6 12

o g 15 7 1 7

u s 21 19 1 0 9 19

z i 26 9 8 9

j l 10 12 12 12

u s 21 19 9 19

w o 23 15 19 15

g a 7 1 5 1

q y 17 25 19 25

将结果再按照 (a1,b=2...) 转回去就行了

4. 围在栅栏中的爱 (<http://www.shiyanbar.com/ctf/1917>)

毫无疑问。先摩斯解码得到一串字母，然后根据意识qwe=abc，我们知道qwe连在一起是键盘的排序，题目给的hint的意思就是说qwerty=abcdef.....，相应地带入解码

由于题目是栅栏的xxxxx，于是再尝试栅栏

2栏:

rvhaaosybleini

7栏:

rabnayahsevoli

题目中有“爱”，也就是love，所以选择七栏

解密得到flag

5. RSAROLL (<http://www.shiyanbar.com/ctf/1918>)

(背景知识:

算法描述:

- (1) 选择一对不同的、足够大的素数 p , q 。
- (2) 计算 $n=pq$ 。
- (3) 计算 $f(n)=(p-1)(q-1)$ ，同时对 p, q 严加保密，不让任何人知道。
- (4) 找一个与 $f(n)$ 互质的数 e ，且 1