实验吧——(crypto)困在栅栏里的凯撒 writeup

原创

嗯哼哈嘿 于 2019-05-19 21:29:09 发布 504 收藏

分类专栏： CTF 文章标签： CTF 实验吧 凯撒密码 栅栏密码 密码学

本文链接：https://blog.csdn.net/qq_39480875/article/details/90348098

题目：

小白发现了一段很6的字符：**NlEyQd{seft}**

由题目我们可以猜测这是关于栅栏密码和凯撒密码，而且要先解栅栏密码再解凯撒密码。

补充些**基本知识**：

1：恺撒密码

在密码学中，恺撒密码（英语：Caesar cipher），或称恺撒加密、恺撒变换、变换加密，是一种最简单且最广为人知的加密技术。它是一种替换加密的技术，明文中的所有字母都在字母表上向后（或向前）按照一个固定数目进行偏移后被替换成密文。例如，当偏移量是3的时候，所有的字母A将被替换成D，B变成E，以此类推。

2：栅栏密码

所谓栅栏密码，就是把要加密的明文分成N个一组，然后把每组的第1个字连起来，形成一段无规律的话。 不过栅栏密码本身有一个潜规则，就是组成栅栏的字母一般不会太多。（一般不超过30个，也就是一、两句话）

解题过程：

1：解栅栏密码

总共有12个字符，而且题目里有6，我们猜测 是2栏或是6栏，分别进行解密：

这里我使用网上在线解密网站：https://www.qqxiuzi.cn/bianma/zhalanmima.php

明显这种不行

2:解凯撒密码

因为我们不知道要右移几位，所以只能一步步试（而且移6位不能得到解答）

到11位的时候就会发现flag了：