BUUCTF Cipher

原创

smile*** 于 2020-04-26 12:31:53 发布 1581 收藏 2

分类专栏： CTF

本文链接：https://blog.csdn.net/qq_45784859/article/details/105766145

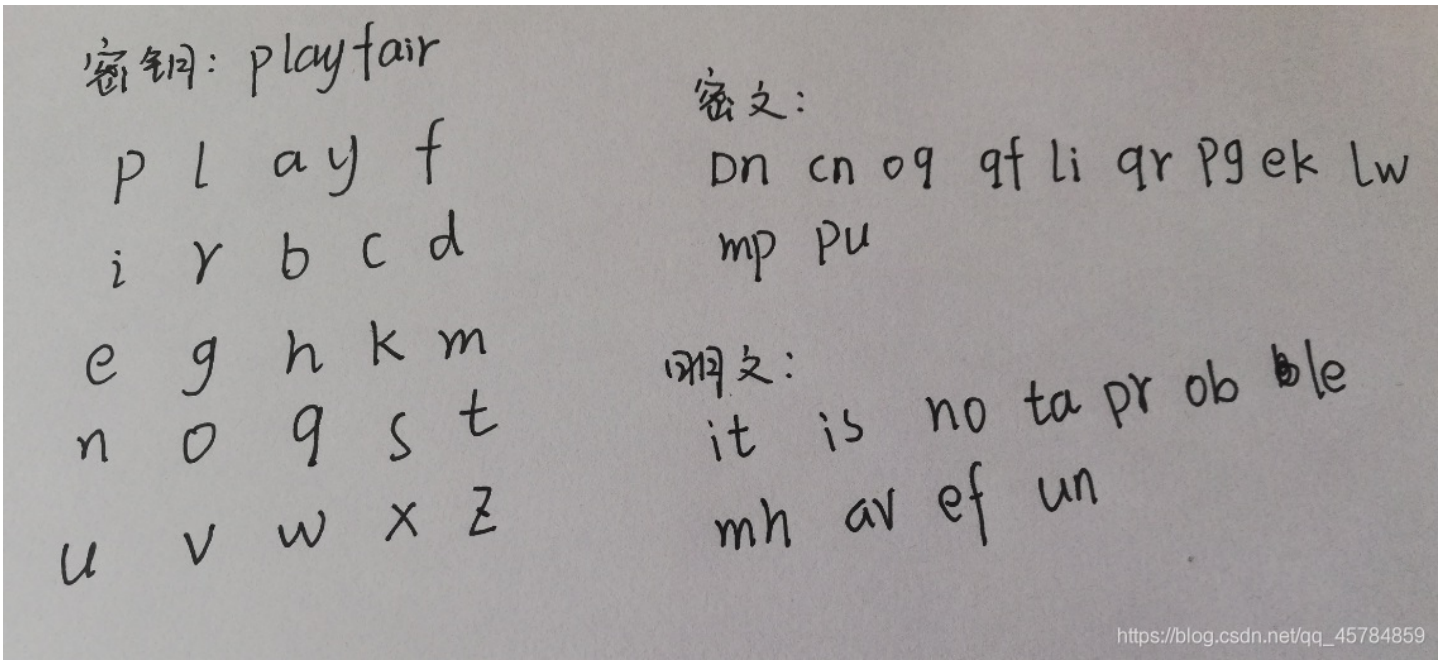
Cipher

题目

Cipher：还能提示什么呢？公平的玩吧（密钥自己找） Dncnoqqfliqrpgeklwmppu

思路

看过去一头雾水，也没有找到什么加密方式，最后通过https://www.cnblogs.com/Fools/p/12202266.html的wp发现这是Playfair密码，并且密钥是“公平的玩”-playfair，明文是Dncnoqqfliqrpgeklwmppu，可以通过网址进行在线解密，我是通过密码的原理进行解密，如下：



Playfair密码原理以及该题解题步骤

Playfair密码（Playfair cipher 或 Playfair square）一种替换密码，1854年由查尔斯·惠斯通（Charles Wheatstone）的英国人发明。

编制密码表

编一个55的密码表，共有5行5列字母。第一列（或第一行）是密钥,其余按照字母顺序，如果密钥过长可占用第二列或行。密钥是一个单词或词组，若有重复字母，可将后面重复的字母去掉。当然也要把使用频率最少的字母去掉（它依据一个55的正方形组成的密码表来编写，密码表里排列有25个字母。如果一种语言字母超过25个，可以去掉使用频率最少的一个。如，法语一般去掉w或k，德语则是把i和j合起来当成一个字母看待，英语中z使用最少，可以去掉它）。
密钥是playfair，去掉重复的后为playfir
密码表为

p	l	a	y	f
i	r	b	c	d
e	g	h	k	m
n	o	q	s	t
u	v	w	x	z

整理明文/密文

整理明文/密文，将明文/密文每两个字母组成一对。如果成对后有两个相同字母紧挨或最后一个字母是单个的，就插入一个字母X（或者Q）。
密文：Dncnoqqfliqrpgeklwmppu
Dn cn oq qf li qr pg ek lw mp pu

解密规则

（1） 若c1 c2在同一行，对应明文p1 p2分别是紧靠c1 c2 左端的字母。其中最后一列被看做是第一列的左方。
（2） 若c1 c2在同一列，对应明文p1 p2分别是紧靠c1 c2 上方的字母。其中最后一行被看做是第一行的上方。
（3）若c1 c2不在同一行，不在同一列，则p1 p2是由c1 c2确定的矩形的其他两角的字母。
密文 ：Dn cn oq qf li qr pg ek lw mp pu
明文： it is no ta pr ob le mh ve ef un

加密规则

（1）若p1 p2在同一行，对应密文c1 c2分别是紧靠p1 p2 右端的字母。其中第一列被看做是最后一列的右方。如，按照前表，fg对应gj，mr对应om
（2） 若p1 p2在同一列，对应密文c1 c2分别是紧靠p1 p2 下方的字母。其中第一行被看做是最后一行的下方。
（3）若p1 p2不在同一行，不在同一列，则c1 c2是由p1 p2确定的矩形的其他两角的字母（至于横向替换还是纵向替换要事先约好，或自行尝试）。如，按照前表，ir对应pa或ap。