【CTF-Crypto】PlayFair密码

原创

ironcarrot 于 2017-09-07 20:16:52 发布 902 收藏 1
分类专栏： CTF

PlayFair密码是古典密码的一种，由一个5*5的矩阵构成密钥；

为了方便描述，加密与解密的过程，这里引用一道实验吧的题目；

http://www.shiyanbar.com/ctf/1852

给出的密文是：The quick brown fox jumps over the lazy dog!

按照把这句话去掉空格按5*5写成一个矩阵的形式，i,j不单独分开，两个字母相等；

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

按顺序写，字母不能重复，如果未填充的位置就按照字母表补全；

这是需要解密的密文：ihxo{smzdodcikmodcismzd}

而密钥就是上面的表格；

现在将密文拆分成两个一组： ih xo sm zd od dc ik mo dc sm zd

那么现在就是需要根据密钥解密，解密的原则如下：

①以 ih 为例子，位置在对角线上，那么其对应的明文在其反对角线上，也就是 ct；

②以 xo 为例子，同行的字母组取其临近的一个字母，如果越格就往后推（不换行），x的左边是f，o的左边即为x，同理，sm即为pl；

③这里没有出现同列的情况，那就是按照字母顺序紧靠密文上端的字母；

btw，如果出现密文字母重复的情况，比如 communist，那就拆分为，co mx mu ni st即可。