

CTF解题记录-Misc-ADFGVX加密(附靶场链接)

原创

今天解题了吗? 于 2021-09-14 20:15:26 发布 144 收藏

分类专栏: [CTF Misc](#) 文章标签: [密码学](#)

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/qq_45537463/article/details/120295315

版权



CTF 同时被 2 个专栏收录

17 篇文章 0 订阅

订阅专栏



Misc

16 篇文章 0 订阅

订阅专栏

靶场链接: [封神台 - 高校专区](#)

刚开始接触CTF, 这道题的题目看得我一头雾水

杂项5:刚刚截获德军的密电

分数: 1

难度: ★☆☆☆☆

提示: 古典密码学中的内容 flag格式: flagxxxxx

描述:

刚刚截获了德军的密电, 密文很重要, 决定着战争的走向。

密电:

FA XX DD AG DD XA FF FF AX DX

CSDN @今天解题了吗?

通过百度“古典密码”+上面那段密电查到了应该是ADFGVX

ADFGVX

原始对应:

abcdefghijklmnopqrstuvwxyz0123456789

DV FF FG AG XD XV GV DX VG GA FD AV GX AX DG AD XX VV VD DD GD VF GG VA XF FX XG DA VX AF DF FV GF FA AA XA

按顺序:

abcdefghijklmnopqrstuvwxyz0123456789

AA AD AF AG AV AX DA DD DF DG DV DX FA FD FF FG FV FX GA GD GF GG GV GX VA VD VF VG VV VX XA XD XF XG XV XX

ADFGX密码

abcdefghijklmnopqrstuvwxyz

AF AA GF DA XF FD GA DD GD GD DX AG XA FX DF AX FA XD FG AD GG FF XG GX XX DG

A D F G X

A b t a l p

D d h o z k

F q f v s n

G g j c u x

X m r e w y

CSDN @今天解题了吗?

链接: [古典密码对照_怦然心动、的博客-CSDN博客_费娜姆密码](#)

通过对照表

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

解得flagabxxmo

ps: 之后看wp 原来题干中的德军+古典密码就是对应ADFGVX加密。

ADFGVX密码

语音

编辑

讨论

上传视频

本词条由“科普中国”科学百科词条编写与应用工作项目 审核。

ADFGVX密码是德军在**第一次世界大战**中使用的栏块密码。事实上，它是早先一种密码 ADFGX 的增补版。

1918年3月Fritz Nebel上校发明了这种密码，并提倡使用。它结合了改良过的Polybius方格替代密码与单行换位密码。这个密码以使用于密文当中六个字母 A, D, F, G, V, X命名。ADFGVX 是被法国**陆军中尉** Georges Painvin 所破解的。以古典密码学的标准来说，此密码破解的工作是属于格外困难的，在这期间，Painvin 更因此健康蒙受了严重损伤。他破解的方法是依靠于找到多份开头相同的讯息，这表示说它们是被相同的分解钥匙和移位钥匙加密的。

中文名	ADFGVX密码	发明者	Fritz Nebel
外文名	ADFGVX Cipher	最早应用	第一次世界大战中德军
发明时间	1918年3月	破解者	法国陆军中尉 Georges Painvin

CSDN @今天解题了吗?