CTF-Vigenere

原创

midsummer_woo 于 2022-04-06 22:37:52 发布 2494 收藏

分类专栏： ctf通关攻略 文章标签： 安全

本文链接：https://blog.csdn.net/lushuaibao/article/details/123991837

ctf通关攻略 专栏收录该内容

4 篇文章 1 订阅

订阅专栏

题目内容：

二战的鹰酱截获了敌军发送的密报，但是关于如何破解却无从下手。经过密码学专家分析，这是“不可破译的密码”。但那已经是上个世纪的事了，现在，我相信你肯定有办法。flag提交前添加flag{}

解题步骤

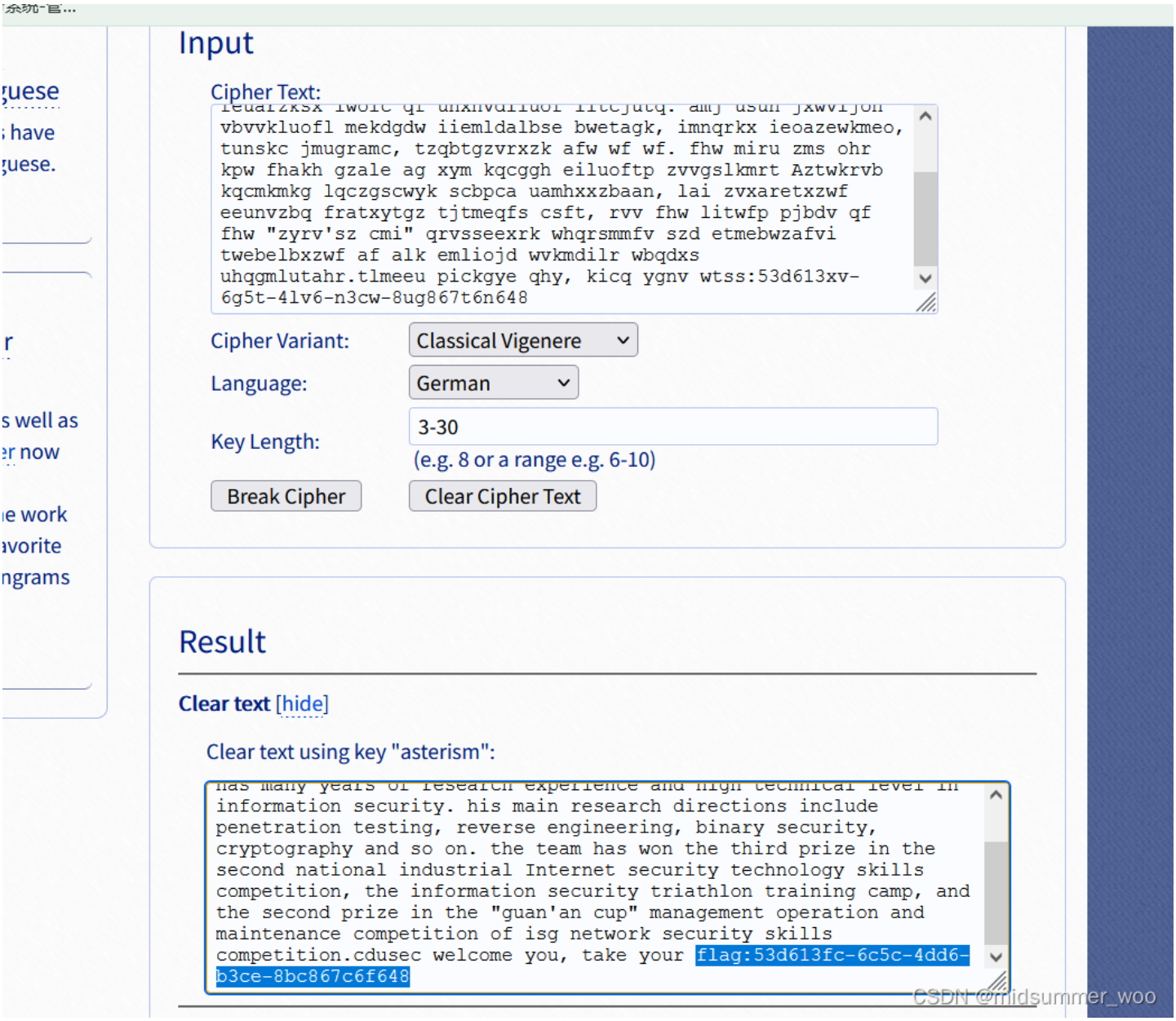
1.下载附件打开可以看见是个txt文件，文件内容如下：

`cvnwvk lqae bw wzgy czxrxlm gnaoiiaafy. am ara xaufwiu qf fwg mlfckmnv tru aajtwxr pmsd afw rfe zms ehvv bzmn lpiebq yeeuiia. zq hsl qrvq keskw fn jqswtvtp wjpwkmvvuq afw lzoz feuarzksx lwoic qf unxhvdiluof litcjutq. amj usun jxwvijoh vbvvkluofl mekdgdw iiemldalbse bwetagk, imnqrkx ieoazewkmeo, tunskc jmugramc, tzqbtgzvrxzk afw wf wf. fhw miru zms ohr kpw fhakh gzale ag xym kqcggh eiluoftp zvvgslkmrt Aztwkrvb kqcmkmkg lqczgscwyk scbpca uamhxxzbaan, lai zvxaretxzwf eeunvzbq fratxytgz tjtmeqfs csft, rvv fhw litwfp pjbdv qf fhw "zyrv'sz cmi" qrvsseexrk whqrsmmfv szd etmebwzafvi twebelbxzwf af alk emliojd wvkmdilr wbqdxs uhqgmlutahr.tlmeeu pickgye qhy, kicq ygnv wtss:53d613xv-6g5t-4lv6-n3cw-8ug867t6n648`

2.根据题目可知是Vigenere加密

在网站中进行破解解密`https://www.guballa.de/vigenere-solver`

得到flag



解题原理

维吉尼亚密码（又译维热纳尔密码）是使用一系列凯撒密码组成密码字母表的加密算法，属于多表密码的一种简单形式。
为了生成密码，需要使用表格法。这一表格（如图1所示）包括了26行字母表，每一行都由前一行向左偏移一位得到。具体使用哪一行字母表进行编译是基于密钥进行的，在过程中会不断地变换。
例如，假设明文为：
ATTACKATDAWN
选择某一关键词并重复而得到密钥，如关键词为LEMON时，密钥为：
LEMONLEMONLE
对于明文的第一个字母A，对应密钥的第一个字母L，于是使用表格中L行字母表进行加密，得到密文第一个字母L。类似地，明文第二个字母为T，在表格中使用对应的E行进行加密，得到密文第二个字母X。以此类推，可以得到：
明文：ATTACKATDAWN密钥：LEMONLEMONLE密文：LXFOPVEFRNHR
解密的过程则与加密相反。
例如：根据密钥第一个字母L所对应的L行字母表，发现密文第一个字母L位于A列，因而明文第一个字母为A。密钥第二个字母E对应E行字母表，而密文第二个字母X位于此行T列，因而明文第二个字母为T。以此类推便可得到明文。

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y