

# CTF Geek Challenge——第十一届极客大挑战Crypto Write Up

原创

Starzkg 于 2020-11-18 10:39:05 发布 483 收藏 1

分类专栏: [安全 #Crypto](#) 文章标签: [Crypto CTF](#)

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/weixin\\_43272781/article/details/109145114](https://blog.csdn.net/weixin_43272781/article/details/109145114)

版权



[安全](#) 同时被 2 个专栏收录

45 篇文章 2 订阅

订阅专栏



Crypto

2 篇文章 0 订阅

订阅专栏

比赛时间: 2020年10月17日早上9点

比赛时限: 一个月

## 0x1 二战情报员刘壮

### 二战情报员刘壮

作者: liuZhuang

简介: 你能知道刘壮在说什么? 得到的flag包裹上SYC[] .-./---  
-./-./---./...-./...-./-./-./...-./...-./---./...-./---./...-./...-./---

提示: 刘壮早上起床打摩丝

分数: 100

答案: **已提交**

[https://blog.csdn.net/weixin\\_43272781](https://blog.csdn.net/weixin_43272781)

密码学二战情报员hint: flag为全大写且为全字母数字

摩斯密码



# 成都养猪二厂

×

作者: ljahum+

简介: 题目地址: <https://share.weiyun.com/FdTTmTP7> 题目描述: v先生家里蛮大的, 还有很多啤酒。v先生之所以能过上这样快哉的生活可能是因为他的养猪场厂围上了高高的栅栏

提示: flag格式 SYC{xx\_xx\_xx},除SYC外其他字母小写 单词间隔开添加下划线

分数: 150

答案:

提交

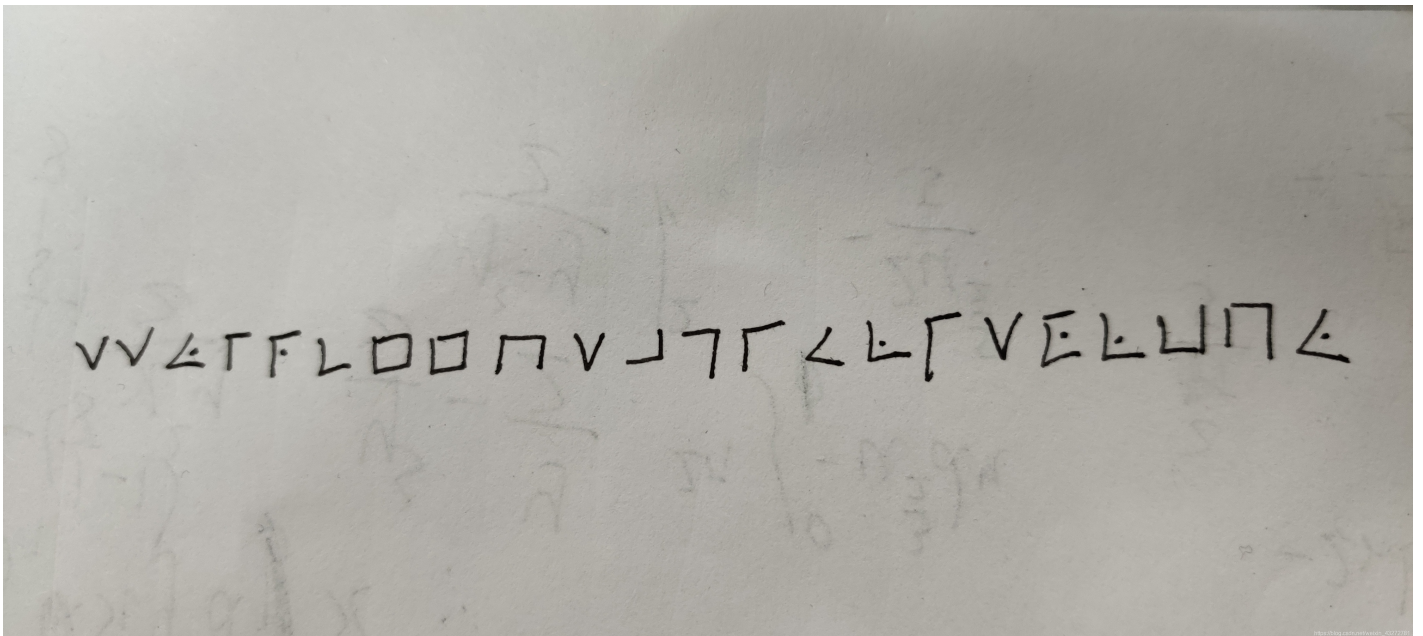
[https://blog.csdn.net/weixin\\_43272781](https://blog.csdn.net/weixin_43272781)

猪圈密码、栅栏密码

名称

..  
cipher.jpg  
hint.txt

cipher.jpg



hint.txt

v先生喝得迷迷糊糊的时候说了一些胡话,你从一堆嘟哝中听清楚了其中一小段:

...(嘟哝)..

```
(int)sth_import = 889464/114514;
```

...(嘟哝)...

<http://www.metools.info/code/c90.html>

加密的内容:

VV€FFL00NvJ7F<EΓV€EUN€

解密的内容:

ssyirceehsagiulisolbhy

[http://www.metools.info/code/railfencecipher\\_154.html](http://www.metools.info/code/railfencecipher_154.html)

889464/114514

7.7672948285799

(	)	%	C
7	8	9	+
4	5	6	x
1	2	3	-
0	.	=	+

[https://blog.csdn.net/weixin\\_43272781](https://blog.csdn.net/weixin_43272781)

转换前: ✕

ssyirceehsagiulisolbhy

栏目数: 7

加密>

解密>

删除待加密内容空格

转换后: ☐

sychishouseisreallybig

[https://blog.csdn.net/weixin\\_43272781](https://blog.csdn.net/weixin_43272781)

## 0x4 规规矩矩的工作

## 规规矩矩的工作

×

作者: ljahum+

简介: 题目地址: <https://share.weiyun.com/RPDWr2WQ> 题目描述: w1z当年玩蹦蹦蹦为了抽希尔氟了很多钱

提示: hint1:让我看看是谁不好好上线代课? hint2:decode程序可能加载的有点慢并且请在命令行内运行

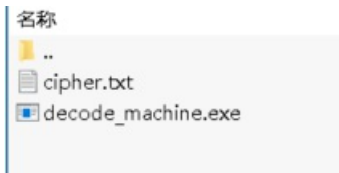
分数: 150

答案:

提交

[https://blog.csdn.net/weixin\\_43272781](https://blog.csdn.net/weixin_43272781)

### 线性代数



### cipher.txt

```
key_encrypt
1 1 1
1 2 3
1 3 6
enc:
12
12
10
```

## 0x5 babyRSA

**babyRSA** ×

作者: [ljahum+](#)

简介: 题目地址: <https://share.weiyun.com/lbPVqZN2> 题目描述: 因为每晚都有小毛贼翻过v先生的栅栏去对猪圈搞破坏, v先生的养猪场不久就倒闭了。失落的v先生感觉不会再爱这个世界了。在他起身去找工作之前留下了一张纸条。

分数: 200

答案:  提交

[https://blog.csdn.net/weixin\\_43272781](https://blog.csdn.net/weixin_43272781)

RSA

## 0x6 犇髻猊呀

**犇髻猊呀** ×

作者: [ljahum+](#)

简介: 题目地址: <https://share.weiyun.com/Y5qldy3K> 题目描述: v先生最近说话越来越奇怪了

提示: flag格式 SYC{xx\_xx\_xx},除SYC外其他字母小写




分数: 250

答案: 已提交

[https://blog.csdn.net/weixin\\_43272781](https://blog.csdn.net/weixin_43272781)

费杰尼亚(维吉尼亚) 密码

名称

-  ..
-  cipher.txt
-  hint.txt

cipher.txt

```
Oowfza errqbbirtqpl ks afiiklr cifgd ho unvxnigkctm bugokz iaf chnxhvek tkvgnvf xeccmjkr; errqbbirtqpve aehwektana nte wfavinxe iequge kbopnuigkogbt ucwomfu altczrtbpvf, oadjvt uuvi iyiokjbuos abzq vo usmm ig TGP vhxsm vu nh umnts bo dviegfzr
```

hint.txt

kbopnuigkogbt ucrwomfu altczrtbpf, oadj  
TGP vhxsm vu nh umnts bo dviegfzr

猜测:

中TGP明文为SYC

查表对照

	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

得密钥BIN

...prezace, gjeptongpma orgojnma sem  
t SYC uzkre it fu teask on vihwtere

其中

# 维吉尼亚密码

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。

**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。

中文名	维吉尼亚密码	性质	加密算法
外文名	Vigenère cipher	名词解释	恺撒密码的基础上扩展的多表密码
出 处	吉奥万巴蒂斯塔贝拉索先生的密码	组成元素	明文、密钥、密表

[https://blog.csdn.net/weixin\\_43272781](https://blog.csdn.net/weixin_43272781)

再猜测 **dviegfzr** 是 **Vigenère** 的密文

得密钥**CATBIN**

## 参考文章

[维吉尼亚密码加密/解密在线工具](#)