

第四届“安洵杯”密码学的try

原创

沐一·林 于 2021-11-10 21:42:20 发布 97 收藏 1

分类专栏: [密码学](#) 文章标签: [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/xiao__1bai/article/details/121257031

版权



[密码学](#) 专栏收录该内容

51 篇文章 1 订阅

订阅专栏

第四届“安洵杯”密码学的try

try

试着解密一下

答题格式: flag{****}

点我下载文件

Flag

提交

CSDN @沐一·林

首先下载TXT附件:

bju lcogx fisep vjf pyztj sdgh 13 gifc qsxw. pkiowxc
glv jqtio ekpy-hfgcouibkh qijgzkfoqur bj r twnovtvlfnvxqe sdxnie arw nqhhcregiu fg nuvj hegxyzwbz qgjkvqm rwwdy 1467 ith hwhv i ouoir gvtyiz fynk zs fazxkj
rzbcirr tmxjum irtuesibu. qgjkvqm'j wgujzu uryc jaqvscmj eytyejgjn ilxrv jidghvt csehj, evf irqzguij amtu dvjmpakil do rzoovrx xpg bzbzie sw xpg sjziiffrlkb irtuesib
kd opk gvtyizvusb. regii, mv 1508, lecitrw kvqvzuouyf, me lqu mjzq tpbzkcfcag, mazvrbg opk xnflpi tuxbg, e pvzxeqeg kuqceseivv ea bni imxivetu xqvlrv. klm
vhdbnizmlw kkfcmx, lbavzmt, eite tesmmlgt v xstsvvawklz, zokvh rrl rhzloggespm uonbkk ssi wexjport fvxegui kotuii etrvxjvkf.[gzxivyjv tirhvh]

ejqo qy rba brwyd va zlr zzkmpèzh kotuii aiu emqmmaecpg funkxmoiu fg iyjdr oekxqujv jkpyeis qp xda 1553 hsbo ce kkvmi jiy wzk. okeqit fnxkmaq vwmprnwf.[4]
lm dkdzt ycse xpg jvjapn vvgbc ea bxmglvqqwi wcz eqhvh i tukmgxvrx "gwwdomxwvke" (e sgo) ow yavxtl kkfcmx eytyejgjn mbiec cibvum. enieirw inrzzm nru
zskjcmshw lwmf q aqdiq trxbghi wl whfjxvkoqurf, fvptcij'a yguidi ugqib zlr trxbghi wl whfjxvkoqurf gfytf rz mgwvpp gpcdbmj, wvqgpg do nmripzxro c dze qil.
ovca yummm zcmetetno nqtky nszfi jz ylbvk tptqnm, oasnr bq rjbn tnvkmmu yi ijnrti, wt jmitwzmkxmf "epb uj oeeh" ineio cmgl klm ounagr. fvptcij'a siglfh bjkn
zkuhmiil ujmwtk fityzktj nuv brcc bju fme. ef mk ma tugizmiicc mcit bu wrglvm c icwx xip tptqnm, yypl rw ja q kzkzslw xtyqizi pseztmbosa, fvptcij'a ycfvq eci
xwtvhwvvidt uuvr wvgcti.[xqzegmfr vguymj]

fyezwm fu qqmiaèvv tcdbdaniq lzw lgixzotgmfr wh q nqsmeyi fcv iozurtii ecvefme gvtyiz duawxi glv gwwho wl lrric qky jn lvnrti, qp 1586.[5] bvbkv, vr klm 19vx
xmtxhvp, xpg yidkrgmfr wh rztrefs'j gqrxzz cef qzvwjmghygiu xw xybmtèvr. hrzqf avpt, ma lzw jqef, bni psuijtuvskvf prqmpjzl zlr qzvwjmghygmfr ja ivgort xyeb
jynbuvl lrh "qidjzkh glzw qofjzxeaz tsvhhdjxvse evf yiazinh eeugt v zkkeijwqxu vvj iyidivvqmg imclvv nqh cqs [zvkvrèzg] jcwaku lv lif djbnmak ks lq mdbn mg".[6]

xyi dkzwvèxi pmglmt wvqtq e iixwjbosa jfv jgyio kbpigxqqdvtrc fxvisi. djbkx nyklwt qil seglvqivyqgr plrvtgi gczavhxi lqtbaur (yinma eqmzupy) grptgt opk zvkvrèzg
sdxnie yefzqgfihpr me lqu 1868 fdmii "glv etrvxjx pmglmt" yi i ilvpuvmp'i himemmei. qp 1917, ixqkrgmwmk czzognr uiaehdjkh glv zqiuèzèk gvtyiz ci "duvsfwzftg ea
bxawcebkei".[7][8] bneg vvtcvqoqur jej rww tzakviii. gpchmy fnfseog yn stsjr ks pclz jxsxie e dchditx bj klm eykpkv nw vezno va 1854 hyg jrmtgt ow vyopzwp jyn
euux.[9] orwquad mtvvpvg dhjks xui tmxjum ith cyspqxzl zlr xvppylck ma xyi 19bj szzyec, syb glzv keepziz, uehm yovpcil ehtzxeaeccavi xwapq stgiuyjvgyyc
svmca opk gvtyiz kd opk 16xu gvrwbht.[6]

kxccczkzfcqi wymui zwzbz cyiq ej e kcbxcregmfr ikt wg zlr wnmau qmue frxnimp 1914 qil 1940.
zlr zzkmpèzh kotuii ma uyhxri rrfyoj j jk e smvpl eykpkv vj zx qu knmj ma gfrwvdxbosa azxp eykpkv qmjoa.[10] vxz kursiuizcj azegij sn czzogn, jfv mzqhxri, hwhv i
dhvay gvtyiz fyms zs vqgpmouib zlr zzkmpèzh kotuii hctyio zlr edizksv imimc ait. jcm isajvhmtqg'y qrwjeogi rmxci sei jzqc nmivrx, rrl vxz ctmbri iowbvzrc pvrsgt dyb
qrwjeogi. opxshkyscv jcm cee, xyi kqdamjieeki tgqymxwumg tzkcvzopl vvpqgt pxur gliim mut xnvnwv: "ucdxpkwgii ftwva", "kuqcpvxx xyxbuyl" eeh, iu jcm cee
grqm ve v krsfi, "tsug hzbxmoykmwp".[11]

wdthiex mizpqh bxmrh ks gzfvgx xui svwmui kotuii (gzgqoqtg glv zmtdvu-bmtièèvm eykpkv vr 1918), syb pe hizxrv nliw xz loh, glv gqrxzz cef wkmtn lpttieespm ve
vzetneetaida hierra'a vems nsimiz glzvzvncr tat ow zlr sei-bkcz xah n xwvwtuagievnn-vdhzigeonv gqrxzz [12]

是长文章的类型，首先根据做题习惯锁定题目类型是单一的密文类型。翻了一下笔记，逐个排除了 **poem codes诗歌加密** 和长密文的 **凯撒加密**。然后。。。然后就蒙住了，是没学过的密文类型啊。

突然灵机一动直接复制部分密文上网搜索看一下，结果发现是春秋的原题啊！！

bju lcogx fisep vjf pyztj sdgh 13 gifc qsxw. pkiowxc

网页 贴吧 知道 文库 图片 资讯 地图 采购

百度为您找到相关结果约340,000个 搜索工具

CTF-i春秋网鼎杯第四场部分writeup - pureqh - 博客园

 2018年8月30日 顺利得出flag为:flag{5a5885ff-6870-47d0-8056-1cbef8fc38b1} (其实这就是个送分题...) shanghai 下载题目,打开是这个 **bju lcogx fisep vjf pyztj sdgh13gifc qsxw. pkiowxc** glv jqt...

博客园 百度快照

为您推荐: 下一页word 网鼎杯

CTF-i春秋网鼎杯第四场部分writeup_weixin_33737774的博客...

2018年8月30日 顺利得出flag为:flag{5a5885ff-6870-47d0-8056-1cbef8fc38b1} (其实这就是个送分题...) shanghai 下载题目,打开是这个 **bju lcogx fisep vjf pyztj sdgh13gifc q...**

CSDN技术社区 百度快照

ctf音频yinxie_CTF-i春秋网鼎杯第四场部分writeup_周杰...

2021年1月16日 bju lcogx fisep vjf pyztj sdgh 13gific qsxw. pkiowxc glv jqtio ekpy-hfgcouibkh qijgz kfoqur bj r twnovtvlfnvxqe sdxnie arw nqhhcregiu fg nujuv hegxyzwbc ...

CSDN技术社区 百度快照

CSDN @沐一·林

发现是 Vigenere 密码，但是 Vigenere 密码 是要 密钥 的。但是网站 <https://www.guballa.de/vigenere-solver> 支持自动解密，扔进去就完事了。

Input

Cipher Text: **密文直接复制粘贴入文本框**

```
bju lcogx fisep vjf pyztj sdgh 13 gific qsxw. pkiowxc
glv jqtio ekpy-hfgcouibkh qijgzkfoqur bj r twnovtvlfnvxqe
sdxnie arw nqhhcregiu fg nujuv hegxyzwbc qgjkvqm rvwwdy 1467
ith hwwh i ouoir gvtviz fynk zs fazxkj rzbcirr tmxjum
irtuesibu. qgjkvqm'j wgujzu uryc jaqvscmj eytyejgjn ilxrv
jidghvt csehj, evf irqzguj amt u dvjmpekil do rzoxvrx xpg
bzbzie sw xpg sjzxiftfrlkdb irtuesib kd opk gvtvizvusb.
regii, mv 1508, lecitrw kvqvzuoyf, me lqu mjzq
tbpzkzcfqg, mazvrbrgt opk xnflpi tuxbg, e pvzxqegg kuqcseivv
ca hpi imvixetu uculru klm rbdhniemly klfemy lbaymt cito
```

Cipher Variant: Classical Vigenere

Language: German

Key Length: 3-30
(e.g. 8 or a range e.g. 6-10)

Break Cipher

Clear Cipher Text

然后点击 Break Cipher

CSDN @沐一·林

Result

Clear text [hide]

Clear text using key "icqvigenere":

```
lemonlemonle
each row starts with a key letter. the rest of the row holds the
letters a to z (in shifted order). although there are 26 key rows
shown, a code will use only as many keys (different alphabets)
there are unique letters in the key string, here just 5 keys: {l,
e, m, o, n}. flag, '{' and 'sqrwewepbhaernkjkgabxo' cem '}' sbn
yxpugujrir hkfortu fo gua sqnfciv, bhpykenvxg cnggaxe js vjv trl
ozddai yzuy oa zmfrp cem rny n yzfucxn yrpzqm rpezyurnkp wl wuzwt
```

ypv ojetqiybazozb xga ixi. adk zzky nycqrn ur ouq mvh vf vnarp.

Details [\[show\]](#)

可以看到结果

Key length statistics [\[show\]](#)

flag{sqrwewepbhaernkjkgabxo}

Histogram [\[show\]](#)

Runtime: 0.026 seconds

CSDN @沐一·林

补充 **Vigenere** 密码：

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。

在一个凯撒密码中，字母表中的每一字母都会作一定的偏移，例如偏移量为3时，A就转换为了D、B转换为了E……而维吉尼亚密码则是由一些偏移量不同的恺撒密码组成。

左边重复关键字决定了密文对应的行

最上面是明文

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	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	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	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	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	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	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	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	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	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	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	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	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
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	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	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	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	N	O	P	Q
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

密文在中间这里

CSDN @沐一·林

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。

.
. .
.

解毕！敬礼！