攻防世界-密码题目-shanghai

原创

Kvein Fisher 于 2020-05-09 14:47:06 发布 989 收藏

分类专栏： 攻防世界 文章标签： 密码学

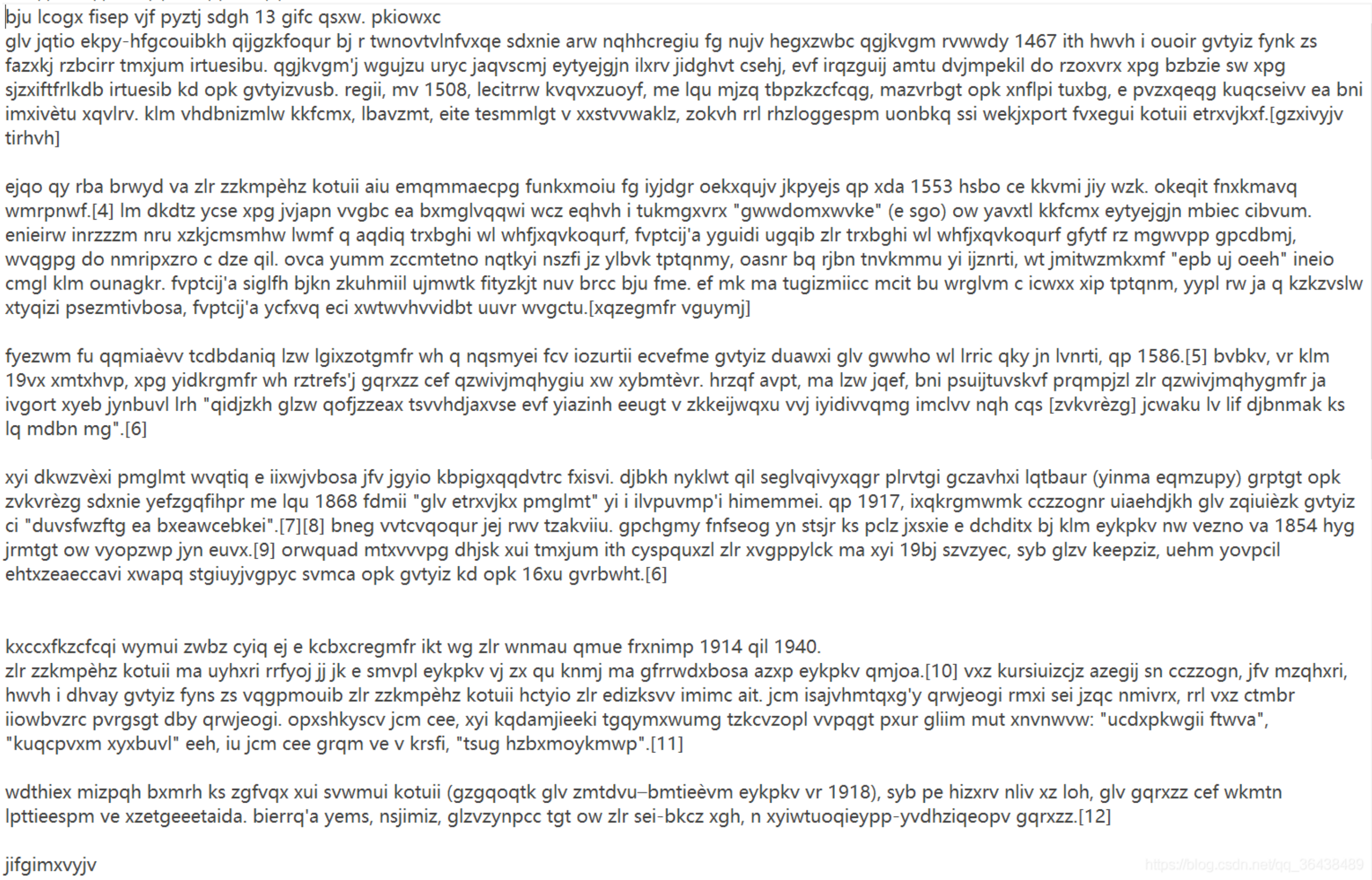
本文链接：https://blog.csdn.net/qq_36438489/article/details/106012127

版权

攻防世界 专栏收录该内容

6 篇文章 0 订阅

订阅专栏



bju lcogx fisep vjf pyztj sdgh 13 gifc qsxw. pkiowxc
glv jqtio ekpy-hfgcouibkh qijgzkfoqur bj r twnovtvlnfvxqe sdxnie arw nqhhcregiu fg nujv hegxzwbc qgjkvgm rvwwdy 1467 ith hwvh i ouoir gvtyiz fynk zs fazxkj rzbcirr tmxjum irtuesibu. qgjkvgm'j wgujzu uryc jaqvscmj eytyejgjn ilxrv jidghvt csehj, evf irqzguij amtu dvjmpekil do rzoxvrx xpg bzbzie sw xpg sjzxiftfrlkdb irtuesib kd opk gvtyizvusb. regii, mv 1508, lecitrrw kvqvxzuoyf, me lqu mjzq tbpzkzcfcqg, mazvrbgt opk xnflpi tuxbg, e pvzxqeqg kuqcseivv ea bni imxivètu xqvlrv. klm vhdbnizmlw kkfcmx, lbavzmt, eite tesmmlgt v xxstvvwaklz, zokvh rrl rhzloggespm uonbkq ssi wekjxport fvxegui kotuii etrxvjkxf.[gzxivyjv tirhvh]

ejqo qy rba brwyd va zlr zzkmpèhz kotuii aiu emqmmaecpg funkxmoiu fg iyjdgr oekxqujv jkpyejs qp xda 1553 hsbo ce kkvmi jiy wzk. okeqit fnxkmavq wmrpnwf.[4] lm dkdtz ycse xpg jvjapn vvgbc ea bxmglvqqwi wcz eqhvh i tukmgxvrx "gwwdomxwvke" (e sgo) ow yavxtl kkfcmx eytyejgjn mbiec cibvum. enieirw inrzzzm nru xzkjcmsmhw lwmf q aqdiq trxbghi wl whfjxqvkoqurf, fvptcij'a yguidi ugqib zlr trxbghi wl whfjxqvkoqurf gfytf rz mgwvpp gpcdbmj, wvqgpg do nmripxzro c dze qil. ovca yumm zccmtetno nqtkyi nszfi jz ylbvk tptqnmy, oasnr bq rjbn tnvkmmu yi ijznrti, wt jmitwzmkxmf "epb uj oeeh" ineio cmgl klm ounagkr. fvptcij'a siglfh bjkn zkuhmiil ujmwtk fityzkjt nuv brcc bju fme. ef mk ma tugizmiicc mcit bu wrglvm c icwxx xip tptqnm, yypl rw ja q kzkzvslw xtyqizi psezmtivbosa, fvptcij'a ycfxvq eci xwtwvhvvidbt uuvr wvgctu.[xqzegmfr vguymj]

fyezwm fu qqmiaèvv tcdbdaniq lzw lgixzotgmfr wh q nqsmyei 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 qzwivjmqhygiu xw xybmtèvr. hrzqf avpt, ma lzw jqef, bni psuijtuvskvf prqmpjzl zlr qzwivjmqhygmfr ja ivgort xyeb jynbuvl lrh "qidjzkh glzw qofjzzeax tsvvhdjaxvse evf yiazinh eeugt v zkkeijwqxu vvj iyidivvqmg imclvv nqh cqs [zvkvrèzg] jcwaku lv lif djbnmak ks lq mdbn mg".[6]

xyi dkwzvèxi pmglmt wvqtiq e iixwjvbosa jfv jgyio kbpigxqqdvtrc fxisvi. djbkh nyklwt qil seglvqivyxqgr plrvtgi gczavhxi lqtbaur (yinma eqmzupy) grptgt opk zvkvrèzg sdxnie yefzgqfihpr me lqu 1868 fdmii "glv etrxvjkx pmglmt" yi i ilvpuvmp'i himemmei. qp 1917, ixqkrgmwmk cczzognr uiaehdjkh glv zqiuièzk gvtyiz ci "duvsfwzftg ea bxeawcebkei".[7][8] bneg vvtcvqoqur jej rwv tzakviiu. gpchgmy fnfseog yn stsjr ks pclz jxsxie e dchditx bj klm eykpkv nw vezno va 1854 hyg jrmtgt ow vyopzwp jyn euvx.[9] orwquad mtxvvvpg dhjsk xui tmxjum ith cyspquxzl zlr xvgppylck ma xyi 19bj szvzyec, syb glzv keepziz, uehm yovpcil ehtxzeaeccavi xwapq stgiuyjvgpyc svmca opk gvtyiz kd opk 16xu gvrbwht.[6]

kxccxfkzcfcqi wymui zwbz cyiq ej e kcbxcregmfr ikt wg zlr wnmau qmue frxnimp 1914 qil 1940.
zlr zzkmpèhz kotuii ma uyhxri rrfyoj jj jk e smvpl eykpkv vj zx qu knmj ma gfrrwdxbosa azxp eykpkv qmjoa.[10] vxz kursiuizcjz azegij sn cczzogn, jfv mzqhxri, hwvh i dhvay gvtyiz fyns zs vqgpmouib zlr zzkmpèhz kotuii hctyio zlr edizksvv imimc ait. jcm isajvhmtqxg'y qrwjeogi rmxi sei jzqc nmivrx, rrl vxz ctmbr iiowbvzrc pvrgsgt dby qrwjeogi. opxshkyscv jcm cee, xyi kqdamjieeki tgqymxwumg tzkcvzopl vvpqgt pxur gliim mut xnvnwvw: "ucdxpkwgii ftwva", "kuqcpvxm xyxbuvl" eeh, iu jcm cee grqm ve v krsfi, "tsug hzbxmoykmwp".[11]

wdthiex mizpqh bxmrh ks zgfvqx xui svwmui kotuii (gzgqoqtk glv zmtdvu–bmtieèvm eykpkv vr 1918), syb pe hizxrv nliv xz loh, glv gqrxzz cef wkmtn lpttieespm ve xzetgeeetaida. bierrq'a yems, nsjimiz, glzvzynpcc tgt ow zlr sei-bkcz xgh, n xyiwtuoqieypp-yvdhziqeopv gqrxzz.[12]

jifgimxvyjv

网鼎杯的一道密码题shanghai，本write up 主要是自己观看总结，思路是根据如下大佬博客所写：
https://myhloli.com/2018%e7%bd%91%e9%bc%8e%e6%9d%af-%e7%ac%ac%e5%9b%9b%e5%9c%ba-shanghai-writeup.html
拿到手像是凯撒密码加密，但是解码之后还是没有收获，最后了解是维吉尼亚密码，是凯撒密码的变形

关键代码：

```
orwquad mtxvvvpg dhjsk xui tmxjum ith cyspquxzl zlr xvgppylck ma xyi 19bj szvzyec, syb glzv keepziz, uehm yovpcil ehtxzeaeccavi xwapq stgiuyjvgpyc svmca opk gvtyiz kd opk 16xu gvrbwht.[6]
```

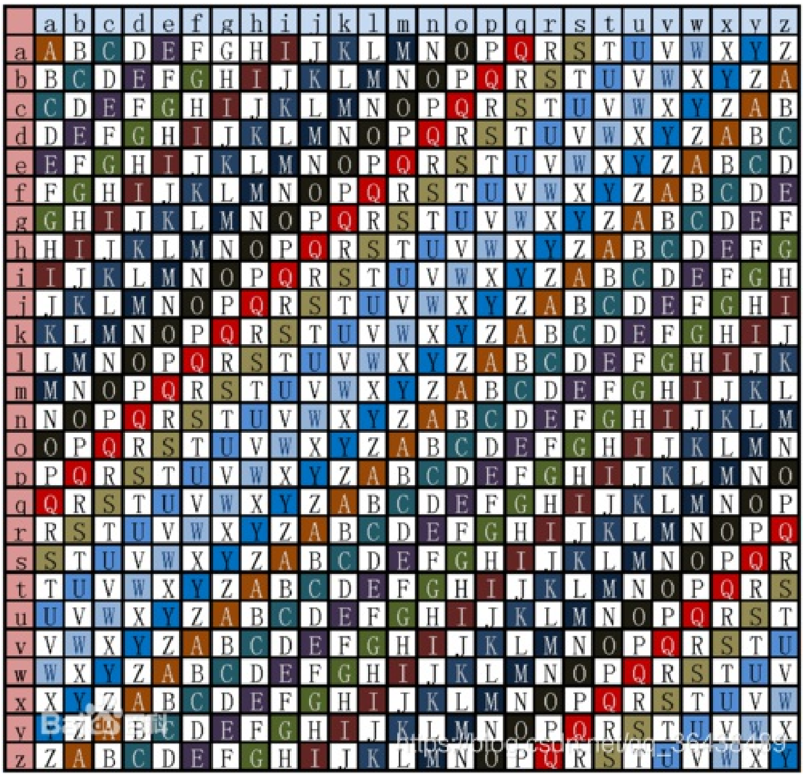
opk gvtyiz kd opk
可见前一个opk和后面的一个opk相隔11位，推测密码长度为11位

又因为看到
opk 16xu gvrbwht. xyi 19bj szvzyec
推测出 the 16th century the 19th century
在平时推测时有一些高频单词
a,is,in,of,and,the这些高频短词推算出部分密钥

最后推测密钥：
密文： opk 16xu gvrbwht.

密钥： vig en ereicqv

明文：the 16th century



	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

维吉尼亚密码可以根据这个矩阵得出
第一列为明文 第一行为密钥 行与列相交得到密文
通过此表可以得到密钥

密文： xyi 19bj szvzyec

密钥： ere ic qvigene

明文：the 19th century

最后得出 vig en ereicqv
ere ic qvigene
由于维吉尼亚的密钥是凯撒的循环 最后得出

密钥为vigenereicq 或者 icqvigenere
找解维吉尼亚密码网站即可
https://www.qqxiuzi.cn/bianma/weijiniyamima.php

或者直接用
https://guballa.de/vigenere-solver