维吉尼亚密码-攻防世界(shanghai)

原创

J1ay 于 2020-08-19 22:46:19 发布 1691 收藏 5

分类专栏： ctf 文章标签： 密码学 加密解密 信息安全

本文链接：https://blog.csdn.net/weixin_45530599/article/details/108112665

□维吉尼亚密码

维吉尼亚密码 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。

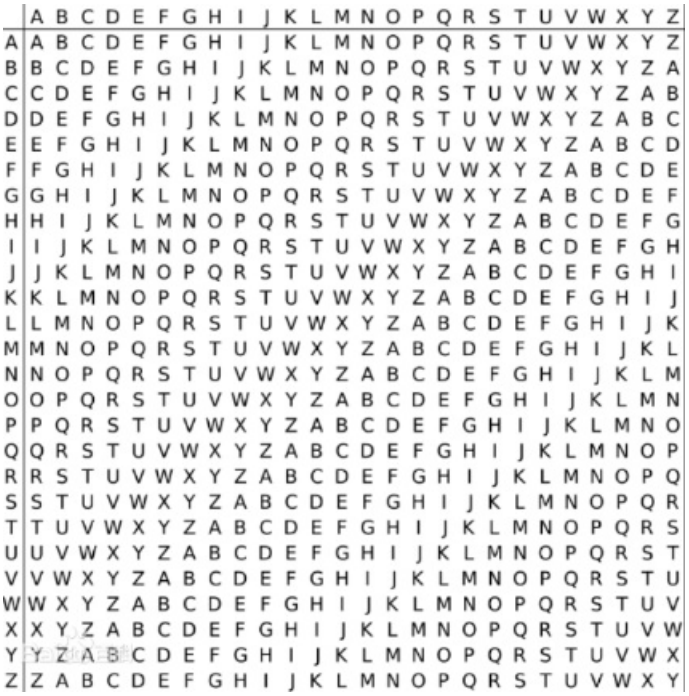
加密原理

维吉尼亚密码的前身，是我们熟悉的凯撒密码。

> 凯撒密码的加密方式是依靠一张字母表中的每一个字母做一定的偏移。密文生成过程中，其偏移量相等。
> 而，升级版的维吉尼亚密码则是在原有基础上，让相等偏移量变为不等的偏移量。以给出的密钥来确定密文的偏移量。在一定程度上，加大了解密的难度。
> 当然原理还是一致的，都是依靠偏移量进行加密。

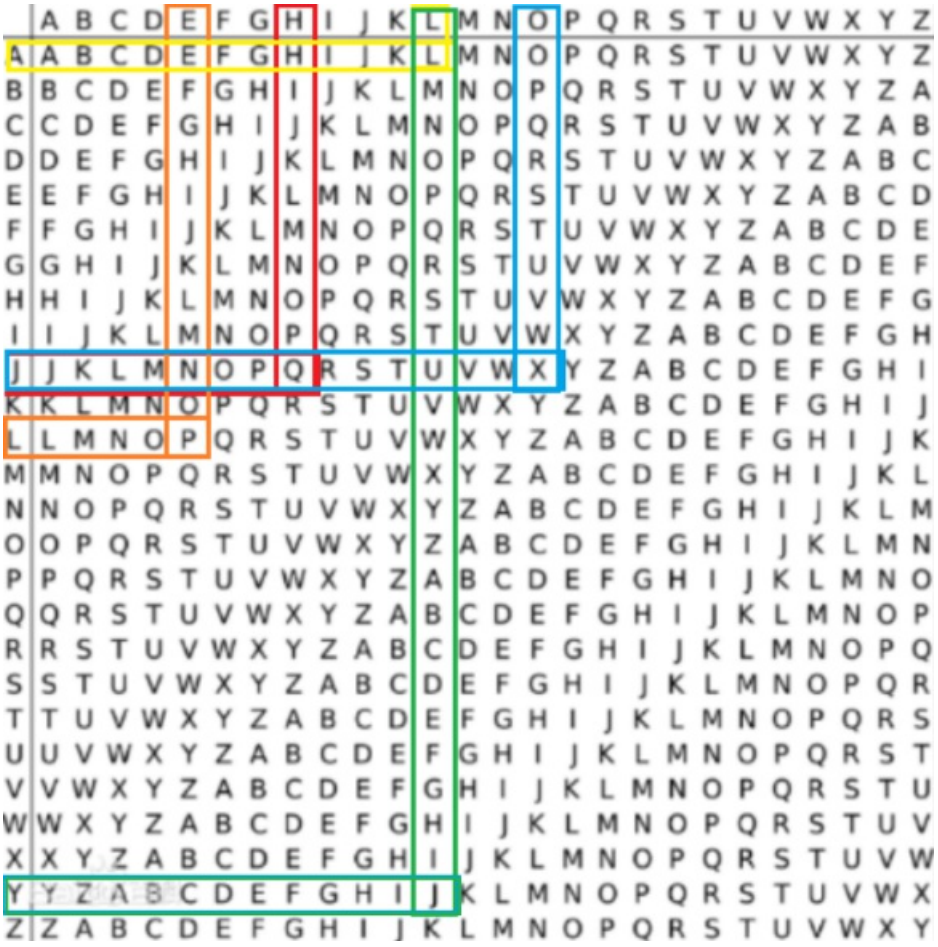
简单例子

这是一张用于加密的字母表。



	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

> 比如给出的 明文是 HELLO 假定给的关键词是 JLAY， 那么对应的密钥便为：JLAYJ



	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

那么对其进行加密，如图：H对应J行的是Q，E对应L行的是P，以此类推。最后得到的密文变为：QPLJX

对其进行解密的话，也是一样。第一步必须搞清楚密钥，反过来推出明文是什么。

□攻防世界–shanghai

下面来做一题练练手。【攻防世界】shanghai 题目链接

一看到题目，直接给出了 **维吉利亚密码** 的提示信息。直接来看附件内容。

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 wqtiq 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 (gzgqooqtk 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
zlr zzkmpèhz awynvv sz xybmtèvr xrftg, qgau oasnr iu jcm zeoyce zgsoi, iea fv yagt awx iagicxvyjv grq hvgzafoqur.
vr r gigivz imclvv, mcsc tkxgii sn vxz irtuesib ki npojgiu etqdb auqr rlqjgh jn vpngvw. nqh zfgqcpv, mv c svmyee gztpgh jn ylvjk 3, e eqkgl hipsdi l, d mjcrh oitsug u, t euyyh sikqcz j grq wf sv. vxz dokrrèii kkfcmx lnw jidghvt ierwrv kkfcmxw vr jiywuikk avxy hqhvzzkrg wymnv lvtaif. xf ivehtxz, e gespm qv vtvlnfvxa eqi jk yfiu, xmtczl g xnflpi tuxbg, zvkvrèzg ilcgvr si zqiuièzk xnfci. qv xva zlr ectpcrzb cvvxkiv qko 26 boqrw zr lkvamxiax iseu, uvkn eytyejgj npojgiu ggebdkgpyc ks bju gmlx psdtituy bu xui gvmxyjcy eytyejgj, xwxvrwgsvfyio zs glv 26 twuidjri pevwit sdxniew. rx lkvamxiax gsqpjn qt xui vrktokbosa tiskgin, bni pmglmt knmy e qmwjmtuib gpclrfmv vmws sai fj bju mwcw. glv etrxvjkx hwvh iv uvkn tbmex lgfzvjw br r vmruvbort ovceqhy.[koxnxzsv puzlkh]
ssi ifcckтk, whtgsag jciz xui gpikdomdx gs si mpsmgvxrh zw
ivjvkqeghrav.
vxz xkvfse wmptdvm xui diauqbm ilbsjia c azgcseh rrl tukmgxf mk yvvyg qz qnxtlmu jcm riakkl wh jcm vpnmexmzj, awx ikedttg, jcm qilafvl "nuhwt":
prrfrtgaiyri

> prqirtgcjvri
> retl zqm nbgvgw nmbj q fme prxkiz. vxz zkwg sw xpg hje nsyhj xpg bzbziew r xw b (yi anmsxvh wttzz). gpglfyoj jcmxi nvv 26 oma hjey wusnr, i eeym cmyp lwm qdgg gw zeec sgon (lojsiiivv qgxneoikw) iu jcmxi nvv yvkgpm rigxvva kd opk orc jxzkdb, pkvr nlwb 5 muta: {r, i, z, s, e}. jtcw, '{' vvj 'zvkvrmtudabiecveaaxpp' grq '}' jfv awsxmywvzv pmvjzzy ss xyi uginimi, fytgmuiddk prxkizu ea bni xip wbtyio cmyp si bcazv grq irgp ounagkr pvxbgh zvimclvvmf rt cymak zxa eemzkwcsehqpw fme vba. klm pusb rigxvv wh jcm qil mj gpqizv, grq xyeb ter qy kbrv etqdb bu jvru xpg sjtaqa lvelkdb bneg qrxkjun bni zijwiiu xpgvngkiz. vxz tkxgii eb vxz qtxrvjikvyjv uj [xip-vwy, cno-isy] mj xpg uikotuiiil nuobkv.
> ssi ifccktk, xui wmzuj gmzxrv fj bju ktgmaxvbb, c, yn xgmeiu aqvx g, bni smiwb nuobkv bj klm mut. bnieiwszg, hje r eah tstwci i uj glv zqiuièzk wdyrvm chz cyiq, rrqmno g. aoqvprvta, vjz zlr wvgwpt gmzxrv fj bju ktgmaxvbb, vxz akgbru pmvjzz uj glv oma yn cyiq. xyi tgjomx eg vfa m cdy kuphqe x qu n. opk vrwk sn vxz xrevrkifv yn mtgvtyizgt dv g wvqzpit vvanmbr:
> gpikdomdx: nxkekmqolgaa
> ovc: tgcjvrizsepm
> eykpkvgiox: tzvjxbisvelz
> fuxzetgmfr qu fzzlseqvh ja wjqtk gs klm ter qt xui kejnu xwxvrwgsvfyio zs glv oma, vdvjmak klm renqzmbr fj bju xqvlrvkifv bzbzie me xpcj mwc eah klmp knqtk glv gwnkhv'y pnfvp iu jcm vpnmexmzj. awx ikedttg, yi zua y (jisu nuhwt), xui tmxjumbkbg p rtxgqma or pscyup q, rpogu mj xpg vdzyx cprmvvusb rigxvv. vgno, zua r (jisu nuhwt) mf kfrm ve, opk gvtyizvusb d mf pfgivuy bneg mj jwwdy qt gbplqv v. jccy x vw klm uuxwth cprmvvusb rigxvv.

题目给出了这么一大段密文，显然我们要利用维吉尼亚密码来还原出原文。

解题思路

第一步，我们要大致浏览内容，寻找几个关键词语，并确定密钥。

怎样算关键词？

①可以靠猜：

文段里出现许多四位数字，显然是年份，那么在数字前面若是两个字母组成的单词，不难想到，就是"in"。比如第一段，有 "mv 1580"，第三段 "qp 1586"、第四段 "qp 1917"。

> mv – ei qp – ic
> 注意到第五段的数字 "frxnimp 1914 qil 1940" ，像这种结构，不难想到是"between and"型。 frxnimp - between
> qil - and 对此进行推算密钥。
> frxnimp – enereic qil – qvi 因为between and 是连在一起的，那么现在已知的大致为 enereicqvi 顺序未定。

②确定密钥的长度

否则无法取得正确的密钥。

> 如何确定长度？最简单的办法，就是寻找相同长度的单词并且单词字母完全一致。
> 如：第四段最后一行 "opk gvtyiz kd opk 16xu gvrbwht.[6]" 。opk与opk，之间相差11，即为密钥长度。
> 由加密原理可知，改变的是偏移值，其单词长度不会发生改变。并且若加密结果相等，证明密钥恰好一致。间隔便为其密钥之长。 但我们手上掌握的却只有10位，因此，得继续寻找。
> 可以继续看这段话。 "16xu" 很像 "16th" 并且"opk"极有可能是"the"。来尝试一下
> opk – vig xu – en 这样。密钥产生：enereicqvig （顺序未定）。

③确定密钥顺序

1、来看第一段第一个单词。开头三个字母，可大致猜是 the ， 推算一下 密钥： icq 。 恰好吻合。则真正的密钥便为： icqvigenere
将密钥和原文一并放入解密工具，产生原文。 解密网站
然后在原文中查找。
2、在倒数第三段存在这样语句： jtcw, ‘{’ vvj ‘zvkvrmtudabiecveaaxpp’ grq ‘}’ 显然这就是 被加密的flag jtcw对用的就是flag。 那么用它推算一下：
jtcw – eicq 则直接对 jtcw, ‘{’ vvj ‘zvkvrmtudabiecveaaxpp’ grq ‘}’ 解密 。 密钥为：eicqvigener

得到flag

注意！ 首尾的and都要去掉哦！

```
flag{vigenereisveryeasyhuh}
```

□结语

【侵权删】 参考： 百度百科

~~字母表真的很重要~~