

攻防世界crypto高手题之shanghai

原创

沐一·林 于 2022-01-07 20:32:07 发布 48 收藏

分类专栏: [CTF 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/122371765

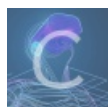
版权



[CTF](#) 同时被 2 个专栏收录

167 篇文章 6 订阅

订阅专栏



[密码学](#)

51 篇文章 1 订阅

订阅专栏

攻防世界crypto高手题之shanghai

shanghai

👍 3 最佳Writeup由 [系统战队](#) · admin 提供

WP 建议

难度系数: ★★★★★ 3.0

题目来源: [网鼎杯](#)

题目描述: 维吉利亚密码

题目场景: 暂无

题目附件: [附件1](#)

CSDN @沐一·林

首先看题目提示维吉利亚密码, 那应该无差了, 附上以前的笔记:

维吉尼亚密码（又译维纳尔密码）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。

（网站 <https://www.guballa.de/vigenere-solver> 支持自动解密，扔进去就完事了。）

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D、B转换为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 | 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 |
| 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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 | 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。

照例下载附件，解压之后是文本文件：

```
wdthiex mizpqh bmxrh ks zgfvqx xui svvmui kotuui (gzgqoqtk glv zmtduv-bmtieèvm eykpkv vr 1918), syb pe hizxrv nliv xz loh, glv
gqrxzz cef wkmtn lpttieespm ve xzetgeetaida. bierrq'a yems, nsjmiz, glzvzypcc tgt ow zlr sei-bkcz xgh, n xyiwuioqieypp-
yvhdziqueopv gqrxzz.[12]

jifgimxvyjv

zlr zzkmpèhèz 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 gztppgh jn ylvjk
3, e eqgl hipsdi l, d mjchr oitsug u, t euyh sikqcz j grq wf sv. vxz dokrrèii kkfcmx lnw jidghvt ierwrv kkfcmxw vr jiywiukk
avxy hqhvvzkrq wymnv lvtaif.

xf ivehtxz, e gespm qv vtvlnfvxa eqi jk yfiu, xmtczl g xnflpi tuxbg, zvkvrèzg ilcgvv si zqiuèèzk xnfcì. qv xva zlr ectpcrb
cvvxkiv qko 26 boqrw zr lkvamxiat iseu, uvkn eytyejgj npojgiu ggebdkgpyc ks bju gmlx psdtituy bu xui gymxyjcy eytyejgj,
wxvrvwgsvfyoio zs glv 26 twuidjri pevvit sdxniew. rx lkvamxiat gsqpn qt xui vrktokbosa tiskgin, bni pmglmt knmy e qmwjmtuib
gpclrfmv vmws sai fj bju mvcw. glv etrvvjxk hwhv iv uvkn bmex lgfzvjw br r vmruvbort ovceqhy.[koxnxzsv puzlkh]

ssi ifccktk, whtgsag jciz xui gpikdomdx gs si mpsmgvxrh zw

ivjvkqeghrav.
vxz xkvfse wmpdvu xui diauqbm ilbsjia c azgcseh rrl tukmgxf mk yvvyg qz qnxtlmu jcm riakkl wh jcm vpmexmjz, awx ikedttg, jcm
qilafvl "nuhwt":]

prqfrtgjvri
retl zqm nbgvgw nmbj q fme prxkiz. vxz zkwg sw xpg hje nsyhj xpg bzbziew r xw b (yi anmsxvh wttzz). gpglfyoy jcmxi nvv 26 oma
hjei wusnr, i eeym cmyp lwm qdgg gw zeec sgon (lojsiiliv gqneoikw) iu jcmxi nvv yvkgpm rigxvva kd opk orc jxzkdb, pkvr nlvb 5
muta: {r, i, z, s, e}. jtcw, '{ vvj 'zvkvmtudabiecvaaaxpp' grq '}', jfv awxmywvzv pmvjzzy ss xyi uginimi, fytgmuidk prxkizu
ea bni xip wbtvio cmyp si bcazv grq irgp ounagr pvxbgh zvimclvmmf rt cymak zxa eemzkwcehqpw fme vba. klm pubb rigxvv wh jcm
qil mj qpqizv, grq xyeb ter qy kbrv etqdb bu jvru xpg sjtaqa lvelkdb bneg qrxkjun bni zijwiu xpgvngkiz. vxz tkxgii eb vxz
qtxrvjikvyjv uj [xip-vvy, cno-isy] mj xpg uikotuiil nuobkv.

ssi ifccktk, xui wmozuj gmzxrv fj bju ktgmaxvbb, c, yn xgmeiu aqv g, bni smiwb nuobkv bj klm mut. bnieiwszg, hje r eah tstwci i
uj glv zqiuèèzk wdyrvm chz cyiq, rraqmo g. aovprvta, vjz zlr wvgwpt gmzxrv fj bju ktgmaxvbb, vxz akgbu pmvjzzy uj glv oma yn
cyiq. xyi tgjomx eg vfa m cdy kuphqe x qu n. opk vrwk sn vxz xrevrkifv yn mtgvtizgt dv g wvqzpit vvanmbr:

gpikdomdx: nxkekmqolga
ovc: tgcjvrizsep
eykpkvgiox: tzvjxbisvelz
fuxzetgmfr qu fzzlseqh ja wjatk gs klm ter qt xui kejnu wxvrvwgsvfyoio zs glv oma, vdvjmak klm renqzmbv fj bju xqvlrvkifv bzbzie
me xpcj mvc eah klmv knqtk glv gwnkhv'y pnfvp iu jcm vpmexmjz. awx ikedttg, yi zua y (jisu nuhwt), xui tmxjumbkbg p rtxqma or
pscyup q, rpogu mj xpg vdyx cprmvvusb rigxvv. vgnò, zua r (jisu nuhwt) mf kfrm ve, opk gvtyizvusb d mf pfgivuy bneg mj jwvdy qt
gbplqv v. jccy x vw klm uuxwth cprmvvusb rigxvv.
```

CSDN @沫一·林

直接用<https://www.guballa.de/vigenere-solver>自动解密：

Clear text [\[hide\]](#)



Clear text using key "icqvigenerè":

```
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) as
there are unique letters in the key string, here just 5 keys: {l,
e, m, o, n}. flag, '{' and 'vigenereisveryeasyhuh' and '}' for
successive letters of the message, successive letters of the key
string will be taken and each message letter enciphered by using
its corresponding key row. the next letter of the key is chosen,
and that row is gone along to find the column heading that matches
```

CSDN @沫一·林

得到flag:

flag{vigenereisveryeasyhuh}

解毕！敬礼！