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

本文链接：https://blog.csdn.net/xiao__1bai/article/details/122371765

CTF 同时被 2 个专栏收录

167 篇文章 6 订阅

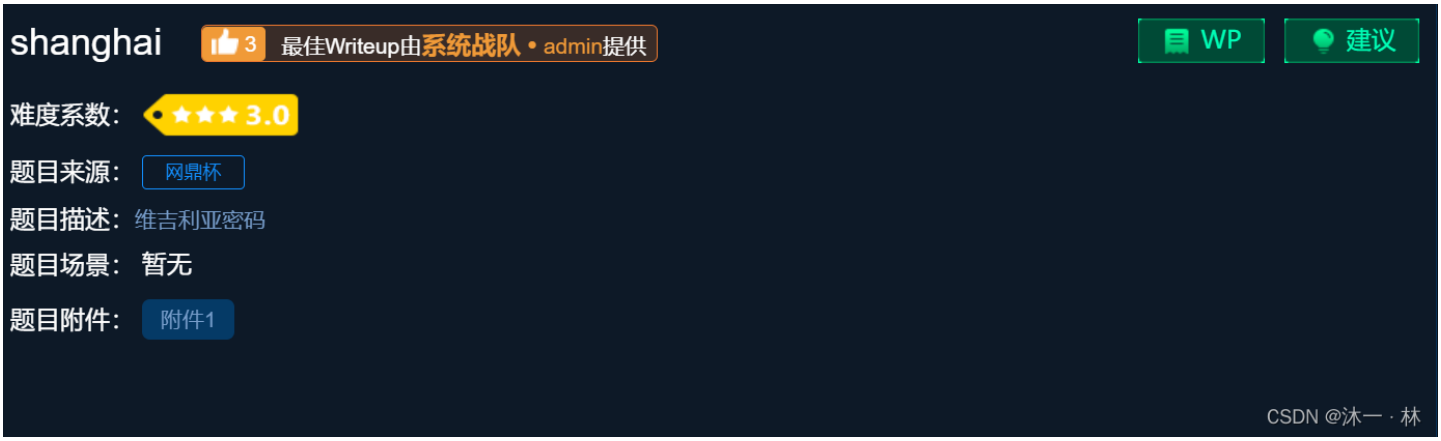
订阅专栏

密码学

51 篇文章 1 订阅

订阅专栏

攻防世界crypto高手题之shanghai



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。

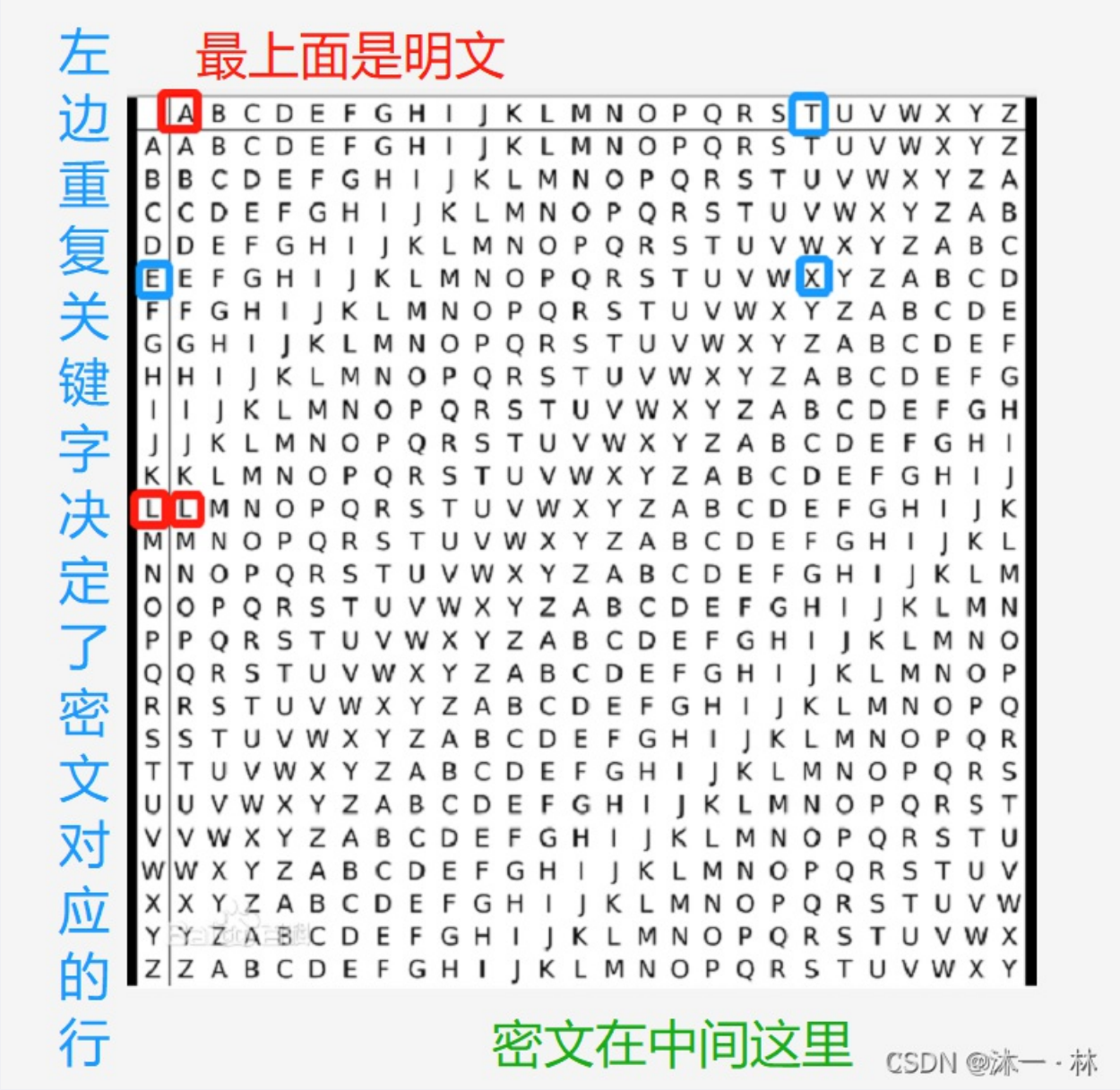
.

（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。

.



.

.

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。

.

.

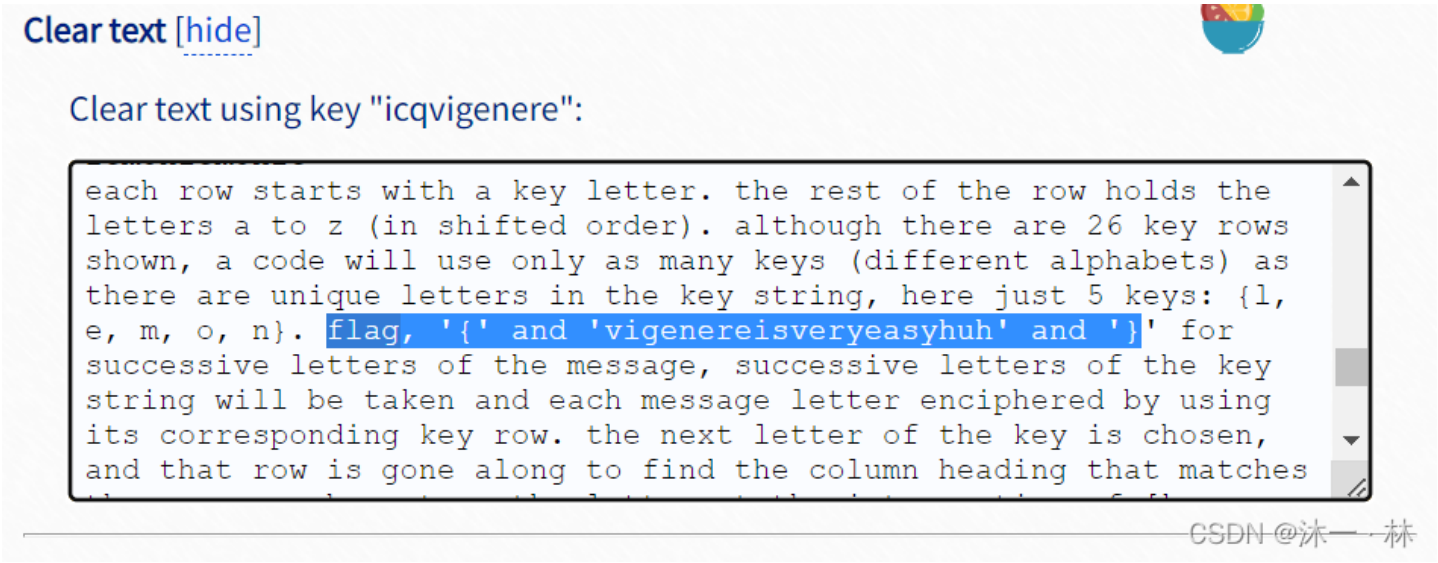
照例下载附件，解压之后是文本文件：

```
wdthiex mizpqh 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

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 ifccktk, 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":

prqfrtgcjvri
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.
```


.

.

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



.

.

得到flag：

flag{vigenereisveryeasyhuh}

.

.

解毕！敬礼！