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

本文链接：https://blog.csdn.net/xiao__1bai/article/details/121257031

第四届“安洵杯”密码学的try

首先下载TXT附件：

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 xzetqeeetaida, bierrq'a vems, nsiimiz, glzvzvnpcc tgt ow zlr sei-bkcz xqh, n xviwtuogievpp-vvdhzigeopv qqrxzz.[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i春秋的原题啊！！！

[ctf音频yinxie_CTF-i春秋网鼎杯第四场部分writeup_周杰...](#)

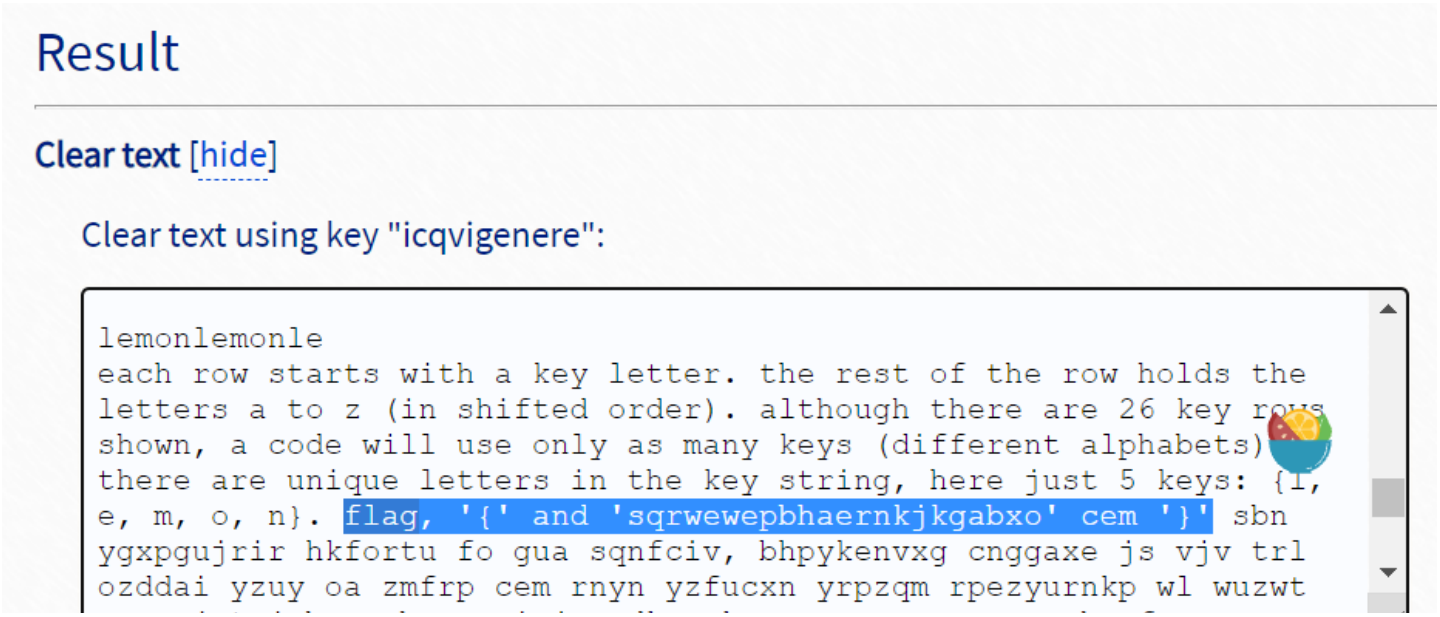
2021年1月16日 bju lcogx fisep vjf pyztj sdgh 13gifc qsxw. pkiowxc glv jqtio ekpy-hfgcouibkh qijgz kfoqur bj r twnovtvlnfvxqe sdxnie arw nqhhcregiu fg nujv hegxzwbc ...

CSDN技术社区 百度快照

.

.

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。



.

.

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。

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！