攻防世界 Crypto高手进阶区 3分题 shanghai

原创

思源湖的鱼 于 2020-12-15 11:06:39 发布 181 收藏

分类专栏： ctf 文章标签： ctf 维吉利亚密码 攻防世界 crypto

本文链接：https://blog.csdn.net/weixin_44604541/article/details/111193773

前言

继续ctf的旅程

攻防世界Crypto高手进阶区的3分题

本篇是shanghai的writeup

发现攻防世界的题目分数是动态的

就仅以做题时的分数为准了

解题过程

得到一个文本

bju lcogx fisep vjf pyztj sdgh 13 gifc qsxw. pkiowxc
glv jqtio ekpy-hfgcouibkh qijgzkfoqur bj r twnovtvlnfvxqe sdxnie arw nqhhcregiu fg nujv hegxzwbc qgj

ejqo qy rba brwyd va zlr zzkmpèhz kotuii aiu emqmmaecpg funkxmoiu fg iyjdgr oekxqujv jkpyejs qp xd

fyezwm fu qqmiaèvv tcdbdaniq lzw lgixzotgmfr wh q nqsmyei fcv iozurtii ecvefme gvtyiz duawxi glv gw

xyi dkwzvèxi pmglmt wvqtiq e iixwjvbosa jfv jgyio kbpigxqqdvtrc fxisvi. djbkh nyklwt qil seglvqivyxqgr pl

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 qm

wdthiex mizpqh bxmrh ks zgfvqx xui svwmui kotuii (gzgqoqtk glv zmtdvu–bmtieèvm eykpkv vr 1918), s

jifgimxvyjv

zlr zzkmpèhz awynvv sz xybmtèvr xrftg, qgau oasnr iu jcm zeoyce zgsoi, iea fv yagt awx iagicxvyjv grq h
vr r gigivz imclvv, mcsc tkxgii sn vxz irtuesib ki npojgiu etqdb auqr rlqjgh jn vpngvw. nqh zfgqcpv, mv c

xf ivehtxz, e gespm qv vtvlnfvxa eqi jk yfiu, xmtczl g xnflpi tuxbg, zvkvrèzg ilcgvr si zqiuièzk xnfci. qv xva

ssi ifccktk, whtgsag jciz xui gpikdomdx gs si mpsmgvxrh zw

ivjvkqeghrav.
vxz xkvfse wmptdvm xui diauqbm ilbsjia c azgcseh rrl tukmgxf mk ywvyg qz qnxtlmu jcm riakkl wh jcm

提示说是维吉利亚密码
可参考常见密码和编码总结 CTF中Crypto和Misc必备

那关键在于推测密钥

先确定长度

opk gvtyiz kd opk

opk和opk之间长度是11
这就是密钥长度

然后推测密钥
首先16xu 应该是 16th
而opk应该是the

这样就有

```
opk - vig
xu - en
```

然后注意到

frxnimp 1914 qil 1940.

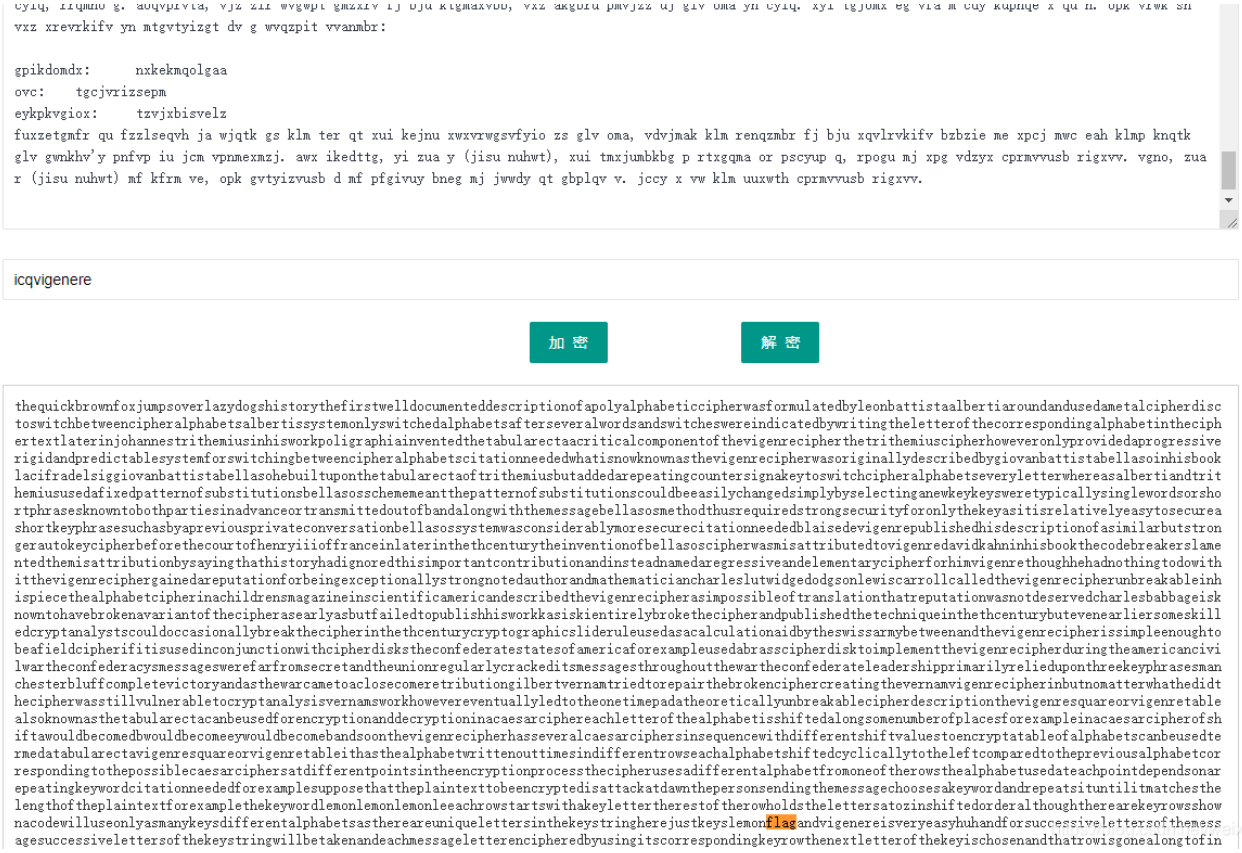
这应该是 between 和 and
那就有

```
frxnimp - enereic
qil - qvi
```

到目前
密钥应该有`enereicqvig`
内容已确定

然后确定密钥的顺序
可以爆破

猜测第一个词 bju 是 the
那密钥就是`icqvigenere`


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.
icqvigenere
加 密
解 密
thequickbrownfoxjumpsoverlazydogshistorythefirstwelldocumenteddescriptionofapolyalphabeticcipherwasformulatedbyleonbattistaalbertiaroundandusedametalcipherdisc
toswitchbetweencipheralphabetsalbertissystemonlyswitchedalphabetsafterseveralwordsandswitcheswereindicatedbywritingtheletterofthecorrespondingalphabetintheciph
ertextlaterinjohannestrithemiusinhisworkpoligraphiainventedthetabularectaacriticalcomponentofthevigenrecipherthetrithemiuscipherhoweveronlyprovidedaprogressive
rigidandpredictablesystemforswitchingbetweencipheralphabetscitationneededwhatisnowknownasthevigenrecipherwasoriginallydescribedbygiovanbattistabellasoinhisbook
lacifradelsiggiovanbattistabellasohebuiltuponthetabularectaoftrithemiusbutaddedarepeatingcountersignakeytoswitchcipheralphabetseveryletterwhereasalbertiandtrit
hemiususedafixedpatternofsubstitutionsbellasosschememeantthepatternofsubstitutionscouldbeeasilychangedsimplybyselectinganewkeykeysweretypicallysinglewordsorsho
rtphrasesknowntobothpartiesinadvanceortransmittedoutofbandalongwiththemessagebellasosmethodthusrequiredstrongsecurityforonlythekeyasitisrelativelyeasytosecurea
shortkeyphrasesuchasbyapreviousprivateconversationbellasossystemwasconsiderablymoresecurecitationneededblaisedevigenrepublishedhisdescriptionofasimilarbutstron
gerautokeycipherbeforethecourtofhenryiiioffranceinlaterinthethcenturytheinventionofbellascipherwasmisattributedtovigenredavidkahninhisbookthecodebreakerslame
ntedthemisattributionbysayingthathistoryhadignoredthisimportantcontributionandinsteadnamedaregressiveandelementarycipherforhimvigenrethoughhehadnothingtodowith
itthevigenrecipher gainedareputationforbeingexceptionallystrongnotedauthorandmathematicianCharleslutwidgedodgsonlewiscarrollcalledthevigenrecipherunbreakableinh
ispiecethealphabetcipherinachildrensmagazineinscientificamericandescribedthevigenrecipherasimpossibleoftranslationthatreputationwasnotdeservedcharlesbabbageisk
nowntohavebrokenavariantofthecipherasearlyasbutfailedtopublishhisworkkasiskientirelybrokethecipherandpublishedthetechniqueinthethcenturybutevenearliersomeskill
edcryptanalystscouldoccasionallybreakthecipherinthethcenturycryptographicslideruleusedasacalculationaidbytheswissarmybetweenandthevigenrecipherissimpleenoughto
beafieldcipherifitisusedinconjunctionwithcipherdisksthe confederatestatesofamericaforexampleusedabrasscipherdisktoimplementthevigenrecipherduringtheamericancivi
lwarthe confederacysmessageswerefarfromsecretandtheunionregularlycrackeditsmessagesthroughoutthewartheconfederateleadershipprimarilyrelieduponthreekeyphrasesman
chesterbluffcompletevictoryandasthewarcametoaclosecomeretributiongilbertvernamtriedtorepairthebrokencipher creatingthevernamvigenrecipherinbutnomatterwhathedidt
hecipherwasstillvulnerabletocryptanalysisvernamsworkhowevereventuallyledtotheonetimepadtheoreticallyunbreakablecipherdescriptionthevigenresquareorvigenretable
alsoknownasthetabularectacanbeusedforencryptionanddecryptioninacaesarcipher eachletteroftheal phabetisshiftedalongsomenumberofplacesforexampleinacaesarcipherofsh
iftawouldbecomedbwouldbecomeeywouldbecomebandsoonthevigenrecipherhasseveralcaesarciphersinsequencewithdifferentshiftvaluestoencryptatableofalphabetscanbeusedte
rmedatabularectavigenresquareorvigenretableithasthealphabetwrittenouttimesindifferentrowseachalphabetshiftedcyclicallytotheleftcomparedtothepreviousalphabetcor
respondingtothepossiblecaesarciphersatdifferentpointsintheencryptionprocessthecipherusesadifferentalphabetfromoneoftherowsthealphabetusedateachpointdependsonar
epeatingkeywordcitationneededforexamplesupposethattheplaintexttobeencryptedisattackatdawnthepersonsendingthemessagechoosesakeywordandrepeatsituntilitmatchesthe
lengthoftheplaintextforexamplethekeywordlemonlemonlemonleeachrowstartswithakeylettertherestoftherowholdsthelettersatozinshiftedoderalthoughtherearekeyrowsshow
nacodewilluseonlyasmanykeysdifferentalphabetsasthereareuniquelettersinthekeystringherejustkeyslemonflagandvigenereisveryeasyhuhandforsuccessivelettersofthemess
agesuccessivelettersofthekeystringwillbetakenandeachmessageletterencipheredbyusingitscorrespondingkeyrowthenextletterofthekeyischosenandthatrowisgonealongtofin
```

得到flag：`flag{vigenereisveryeasyhuh}`

## 结语

维吉利亚密码的应用
```