# 攻防世界_Crypto_Decrypt-the-Message

原创

好想变强啊 已于 2022-04-01 16:08:45 修改 3904 收藏

分类专栏： 攻防世界刷题记录 文章标签： 网络安全

于 2022-04-01 15:59:57 首次发布



本文链接：https://blog.csdn.net/qq_38798840/article/details/123898095



攻防世界刷题记录 专栏收录该内容

8 篇文章 0 订阅

订阅专栏

## 攻防世界刷题记录Crypto篇

---

### 文章目录



---

## 前言

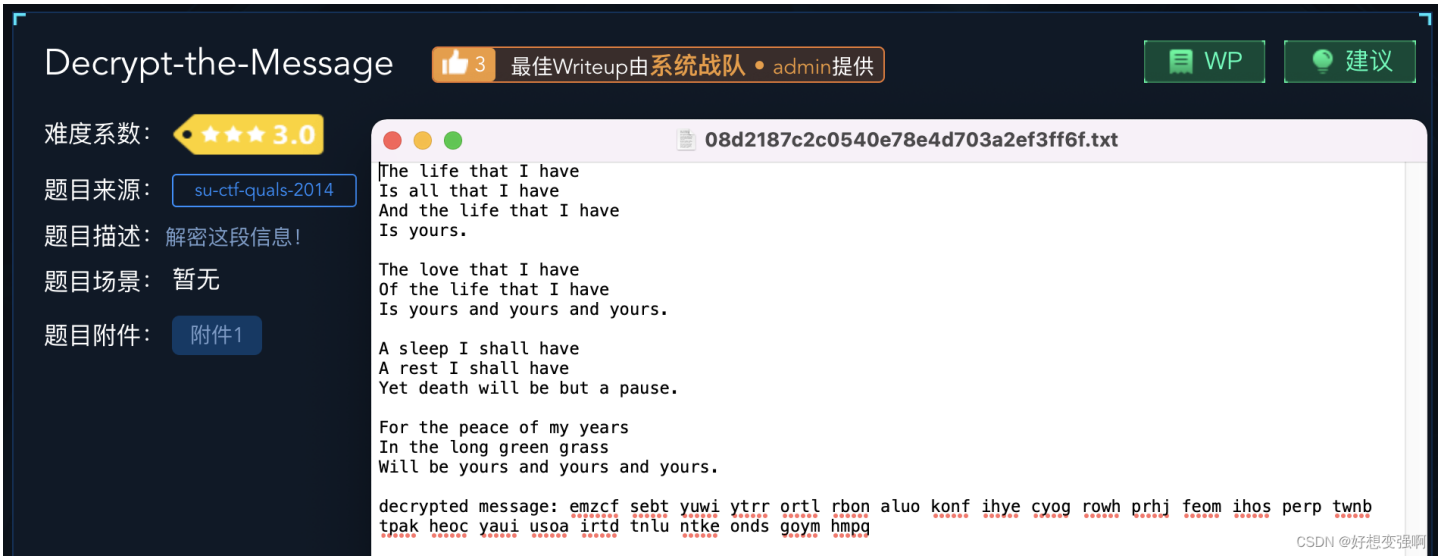
这应该是我在攻防世界网站遇到的第一道三分题，可以看到原题是出自2014年的一个比赛，八年前哎还真是有点久远了啊。看到很多人写的wp中所引用的GitHub上大佬的解题脚本也是7年前更新的了。但还是很想记录一下，因为现在我还没把这题做得很明白。

本题关键词：poem code

---

## 一、原题内容

题目给的txt像是一首诗，后来也印证了这题考察的确实是“poem code”。
下面还有一行decrypted message，看着有点懵，应该是“要解密的”信息。




## 二、解题步骤

### 1.了解poem code加密原理

poem code 的加密过程是：
1）选取一首诗中的若干单词用于加密，写出这些单词中的字母在字母表中的位置（数字，a是1b是2），如果遇到重复的字母就继续+1；
2）用于加密的单词有多少字母，就把明文内容分成这个长度的分组，按顺序把明文写出来，如果不能“填满”分组长度的整数倍，就用abcdefg……填充，再按照1）中选取的那些加密单词中字母位置对应的数字，重新排列明文中字母的位置得到密文。
（个人理解，关于直观一点的过程可以参考这个博客：https://blog.csdn.net/weixin_45530599/article/details/108027293

### 2.借助Python解密脚本解密

看到大部分别人的wp都提到这个GitHub地址里的Python脚本可以用来解题：
https://github.com/13957166977/crypto-tools/tree/master/poemcode
要注意这里是Python2。
尝试了一下确实可以复现。棒呆。
要注意GitHub中提示了我们“Note that the poem, msg and cipher has to be alphabetic letters only. No commatas, dots, whatgives.”大概就是诗歌和密文里不能有逗号和点这些标点符号只留下字母吧（空格和换行应该没影响）。
GitHub作者的提示：

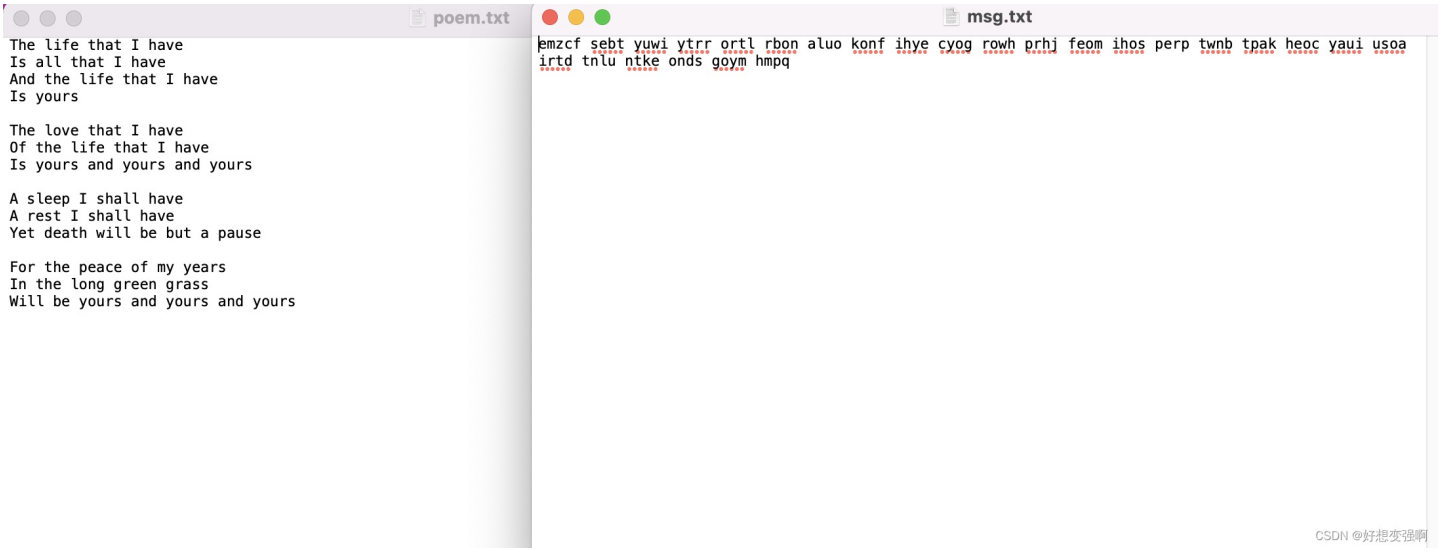
## Usage

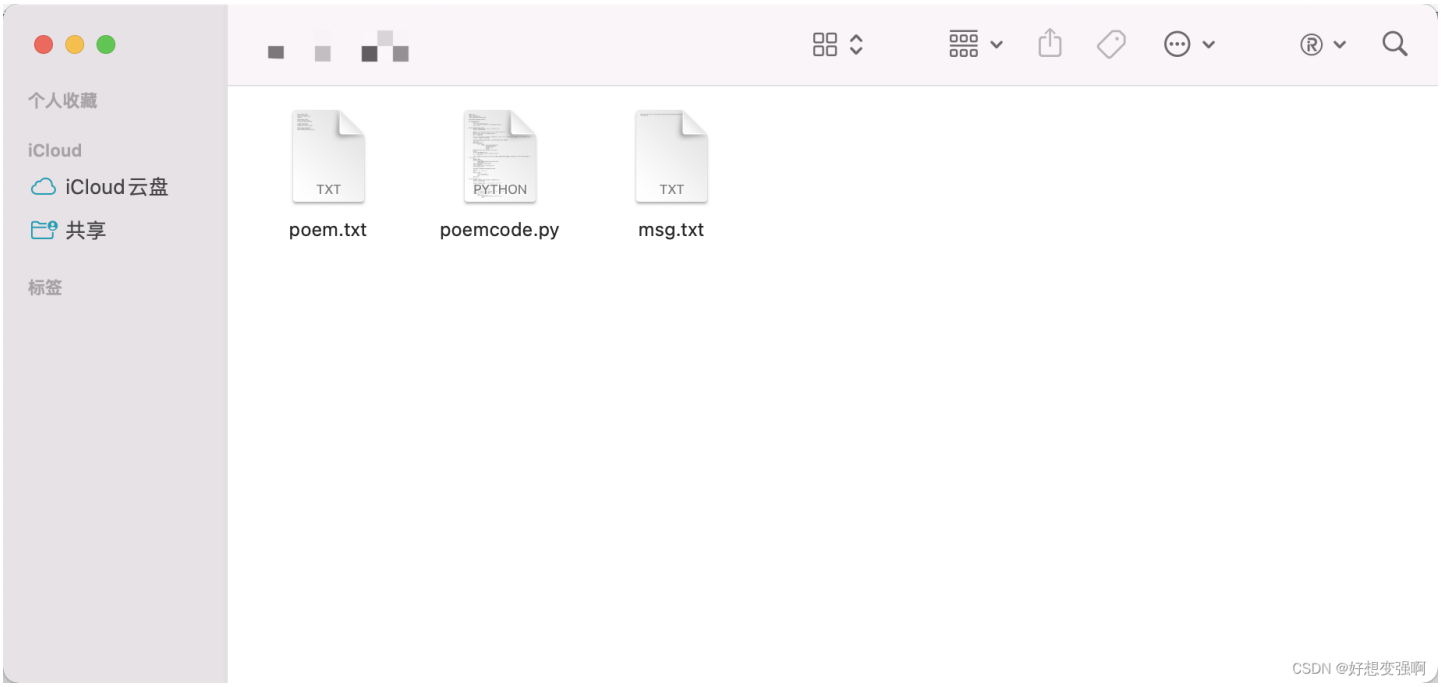
```
$ python poemcode.py poem msg
```

Note that the poem, msg and cipher has to be alphabetic letters only. No commatas, dots, whatgives.



我的复现过程：
1）把题目附件中的decrypted message剪切、粘贴到另一个文件命名为msg.txt，原题目附件中的标点也去掉，重命名为poem.txt。下载GitHub大佬的脚本poemcode.py，和上面两个txt放到同一目录下方便后续操作。




2）在该目录下进入终端，输入如下命令运行Python2脚本：

```
python poemcode.py poem.txt msg.txt
```

3）找到合理的内容就是结果

```
ihiynptuikfcrptytoraysheratepshoeyornuwrblteyotukraoonoowhlwntourbecdiepkasfmghj
uiblnort
ihnyptutikfcrpytooragysihetaepsnhoeyoruwrnbloteryokuraolonoowhwntdouyrbteceipkau
sfmghjiblsnomrtd
ifytkhicryporapttuyisheawoeryourrblenpstheyounnotowwhtourlaorobemibfcdghijlnopuk
arst
ifyintkhcrtyporaptuyisheartwoeyonurrblepstheyoutknnoowlwhtouraorobemidebfcghuijl
nopkarst
ifynttkhcrypoorapgtuyisiheatwnoeyourrnbleopstheryouknlnoowwhtdouryaorobtemiebufc
ghijlsnopmkarstd
ifhtukticryporaptyiysheewsopryourrblenthaeyoononatowwhtourlroubemcbafkdghijlnopu
rsit
ifhintuktcrtyporapyiysheertwsopyonurrblethaeyootknonaowlwhtourroubemcdebafkghuij
lnoprsit
ifhntutktcrypoorapgyiysiheetwsnopyourrnbleothaeryooknolnaowwhtdouryroubtemcebauf
kghijlsnopmrsitd
ifyuthiktcryptorapnyisheasweronyourprblettheyouonotnlowwhatourkrobemiabcdfughijk
lnoperst
ifytuothikcrnyptorapyisheansnweroyoturprbletheyoulodnotnowkwhatourrobemiuasbcdfg
heijklnoprst
ifyouthinkcryptographyistheanswertoyourproblemthenyoudonotknowwhatyourproblemisa
bcdefghijklmnopqrstu
pakprictiyorhftyselorohyphurbeewterunhwooaywtooonrbpofjhsgkeilncmbrt
ptaykpricihyorftyseplaorohyheurbewterauunhwooyowtoonrbpkoifjhsgecilnmbrt
```



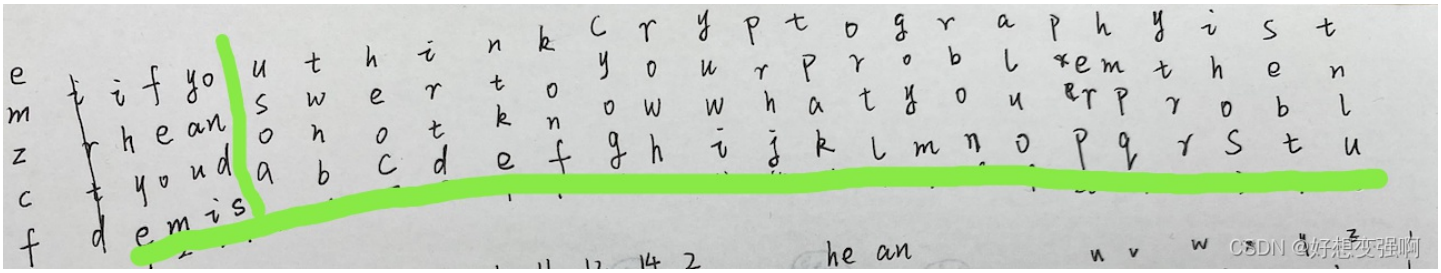
flag：ifyouthinkcryptographyistheanswertoyourproblemthenyoudonotknowwhatyourproblemisabcdefghijklmnopqrstu

---

## 三、自己的一点解题方法和疑惑

通过对poem code加密方式的大概了解，以及已知了答案是ifyouthinkcryptographyistheanswertoyourproblemthenyoudonotknowwhatyourproblemisabcdefghijklmnopqrstu，可以发现最后填充的内容abcdefghijklmnopqrstu是很长的而且可能就是按原字母表顺序填充。密文是emzcf sebt yuwi ytrr ortl rbon aluo konf ihye cyog rowh prhj feom ihos perp twnb tpak heoc yaui usoa irtd tnlu ntke onds goym hmpq，第一组5个字母，其余都是4个，按理说分组不应该不能“整除”，所以猜测最前面的emzcf不要，剩余25个4个字母的分组，共100个字母，就按25的分组长度，每组四个字母竖着写，最后一排的字母按abcdefghijklmnopqrstu排列（遇到重复的就根据上下文看是否合理），最后就还剩下最前面的4组字母顺序不知道了，但此时完全可以联系上下文排出来。

强行手动解密：




但是反过来找最初是按诗歌中的哪几个单词来加密的，似乎没找到合理的答案，有点累了先放一放，欢迎交流。