

xctf攻防世界 CRYPTO高手进阶区 Decrypt-the-Message

原创

18947943 于 2022-02-11 15:02:36 发布 1236 收藏

分类专栏: [攻防世界crypto之路](#) 文章标签: [安全](#) [CRYPTO](#)

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/18947943/article/details/122877557>

版权



[攻防世界crypto之路](#) 专栏收录该内容

26 篇文章 0 订阅

订阅专栏

1. 进入环境，下载附件

题目给的是txt文件，如图：

```
08d2187c2c0540e78e4d703a2ef3ff6f.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
The life that I have
Is all that I have
And the life that I have
Is yours.

The love that I have
Of the life that I have
Is yours and yours and yours.

A sleep I shall have
A rest I shall have
Yet death will be but a pause.

For the peace of my years
In the long green grass
Will be yours and yours and yours.

decrypted message: emzcf sebt yuwi ytrr ortl rbon aluo konf ihye cyog rowh prhj feom ihos perp twnb tpak heoc yaui
```

2. 问题分析

看了wp才知道，一首诗+一段密文，考察的是Poem Codes加密，具体是什么样子的呢？如下：

1. 先有一首诗

```
for my purpose holds to sail beyond the sunset, and the baths of all the western stars until I die.
```

2. 选出关键词

```
"for", "sail", "all", "stars", "die."
```

对其进行拆散：

forsailallstarsdie

接下来按照字母表顺序进行编号，若遇相同字母，则继续+1，先排序再进行操作：

```
ttt x unit x
C:\ProgramData\Anaconda3\python.exe D:/CodeWorkspace/PycharmProjects/practiceAndtest/unit.py
['a', 'a', 'a', 'd', 'e', 'f', 'i', 'i', 'l', 'l', 'l', 'o', 'r', 'r', 's', 's', 's', 't']

Process finished with exit code 0
```

那么第一个a为1，则第二个a下标为2，第三个为3，则d的下标为4，e为5，第一个i为6，第二个i为7，以此类推，那么表格如下

3. 得到索引表

那么可以列表

f	o	r	s	a	i	l	a	l	l	s	t	a	r	s	d	i	e
6	12	13	15	1	7	9	2	10	11	16	18	3	14	17	4	8	5

4. 分组诗句

由于选择的关键词总长度为18，那么也就是18位一组可以实现加密

接着搞个排列：

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
w	e	h	a	v	e	r	u	n	o	u	t	o	f	c	i	g	a
r	s	s	i	t	u	a	t	i	o	n	d	e	s	p	e	r	a
t	e	a	b	c	d	e	f	g	h	i	k	k	l	m	n	o	p

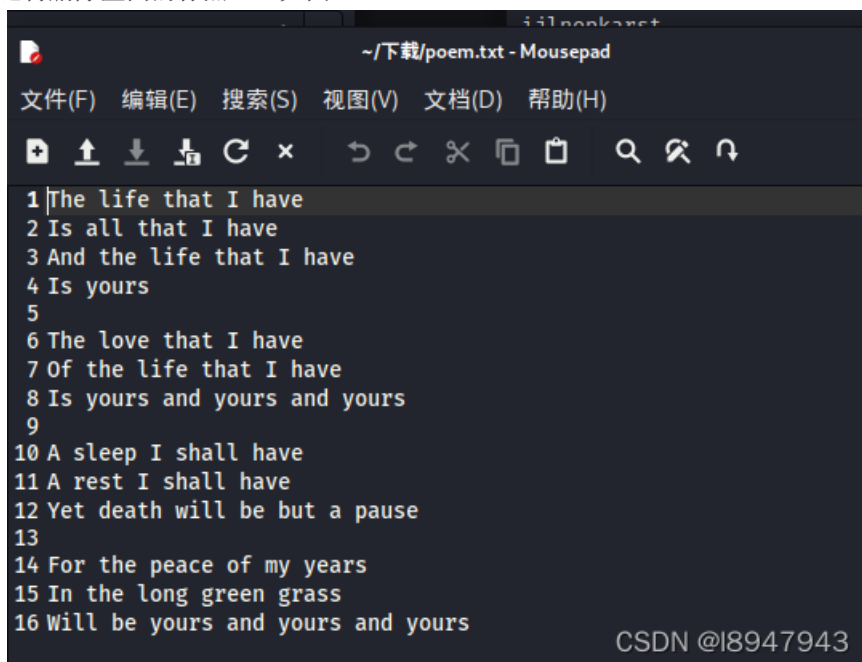
那么，诗歌片段中的第一个字母“r”；下面是6：第二个字母是“o”，下面是12。在我们的（填充的分组信息）中，第6列字母组合是“eud”，第12列字母组合是“tdk”。

以此类推，可以通过给出的关键词实现对信息的加密。

4. 使用git代码

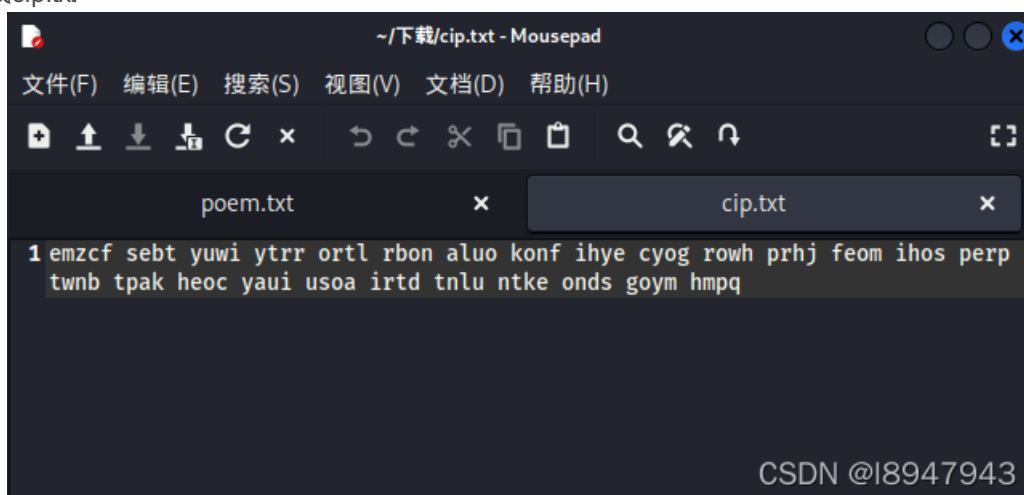
自己写不动，还是git吧，<https://github.com/13957166977/crypto-tools/tree/master/poemcode>，使用poemcode.py

将诗句存储成poem.txt（记得删除里面的标点），如图：



```
~/下载/poem.txt - Mousepad
文件(F) 编辑(E) 搜索(S) 视图(V) 文档(D) 帮助(H)
1|The life that I have
2 Is all that I have
3 And the life that I have
4 Is yours
5
6 The love that I have
7 Of the life that I have
8 Is yours and yours and yours
9
10 A sleep I shall have
11 A rest I shall have
12 Yet death will be but a pause
13
14 For the peace of my years
15 In the long green grass
16 Will be yours and yours and yours
CSDN @I8947943
```

将解密信息存储成cip.txt



```
~/下载/cip.txt - Mousepad
文件(F) 编辑(E) 搜索(S) 视图(V) 文档(D) 帮助(H)
poem.txt x cip.txt x
1 emzcf sebt yuwi ytrr ortl rbon aluo konf ihye cyog rowh prhj feom ihos perp
  twnb tpak heoc yau1 usoa irt d tnl u ntke onds goym hmpq
CSDN @I8947943
```

最后运行脚本：

```
python2 poemcode.py poem.txt cip.txt
```

结果如图:

```
文件 动作 编辑 查看 帮助
uijlnoprst
ifhntutktcrypoorapgyiysiheetwsnopyourrnbleohtaeryooknolnaowwhtdouryroubtemceb
aufkghijlsnopmrsitd
ifyuthiktcryptorapnyisheasweronyourprbletheyouonotnlowwhatourkrobemiabcdfugh
ijklnopest
ifytuothikcrnyptorapyisheansweroyoturprbletheyoulodnotnowkwhatourrobemiuasbc
dfgheijklnoerst
ifyouthinkcryptographyistheanswertoyourproblemthendyoudonotknowwhatyourproblem
isabcdefghijklmnopqrstu
pakprictiyorhftyseloroehyphurbeewterunhwooywtooonrbpofjhsgeilncmbrt
ptaykpriciorhftyseloroehyphurbeewterunhwooywtooonrbpkoifjhsgeilncmbrt
pyakphriciouriftystealoroehyphurbrewtepruunhwooywtooonrbapiofjchsgelndmb
rtk
iakptrfctiyorhypsrlorwoeyphurbeteounhwooywtoorrbsofjbhmgkeilncrpt
itaykptrfciorypshlaorwoeyheurbteeoauunhwooywtoorrbskoifjbhmgecilnrpt
iyakptrfcioriyprsthalorwoeyhursbrteepouunhwooywtoorrbsiofjbchmgelndr
ptk
patkptrchiyforypselworhpoyehuerbaterunnhoawoywotourbpobfjshkgceimlnrt
phatukpitrciyyforyselworsrhoyhauerbterounonhoawoywotourbpcobafjshkgceimlnrt
puatkpitryciyfoirtyseslworhpaoyhuerrbnteerounhoawoywottolrbopaobfjshkgceim
ldnurtc
ctakfphyiorpyityrsywloeeuhrbrahptoeonunorowytohuoarwbgbofmpierhijkpob
cthaukfpyyiorpityrsywloeeuhrbrahptoeonouonruwytohuoarwbgboafmpieelnjskrht
```

最终答案为:

ifyouthinkcryptographyistheanswertoyourproblemthendyoudonotknowwhatyourproblemisabcdefghijklmnopqrstu