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

原创

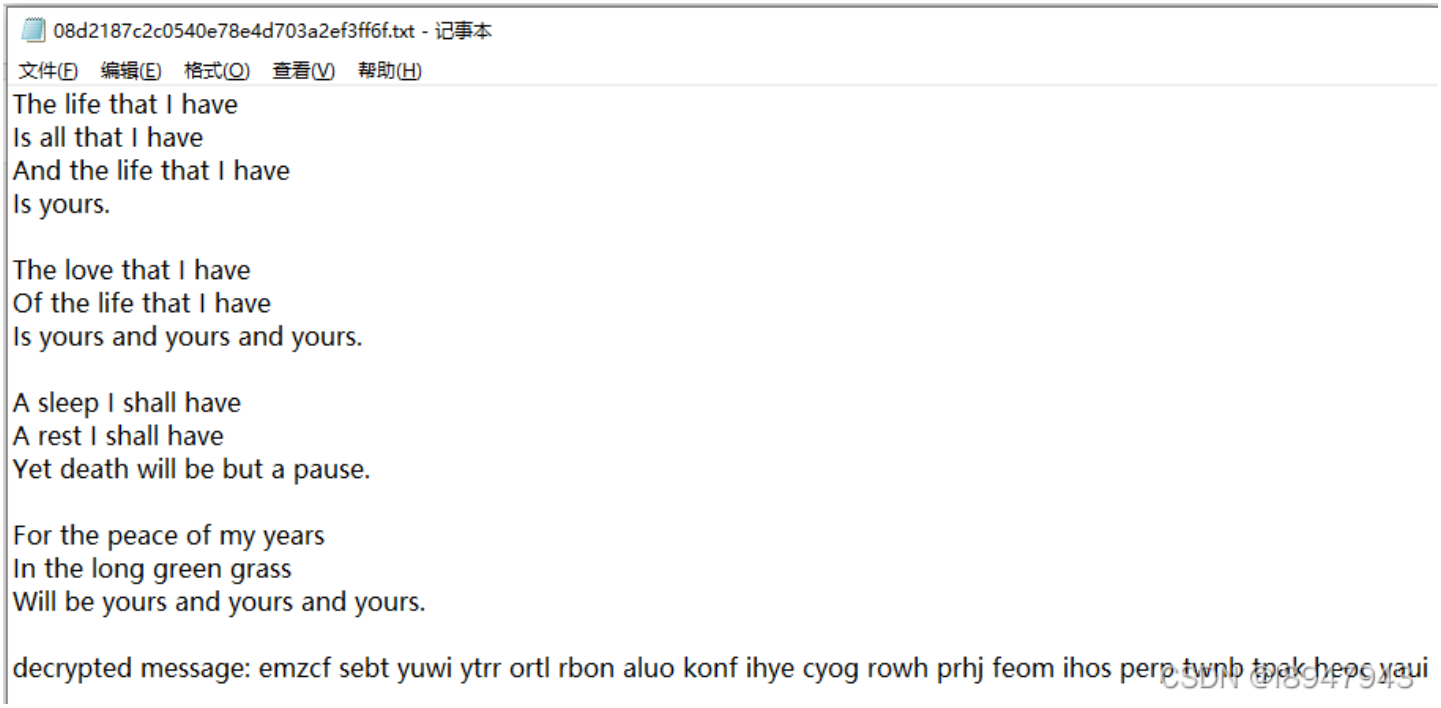
l8947943 于 2022-02-11 15:02:36 发布 1236 收藏

分类专栏： 攻防世界crypto之路 文章标签： 安全 CRYPTO

本文链接：https://blog.csdn.net/l8947943/article/details/122877557

1. 进入环境，下载附件

题目给的是txt文件，如图：



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.

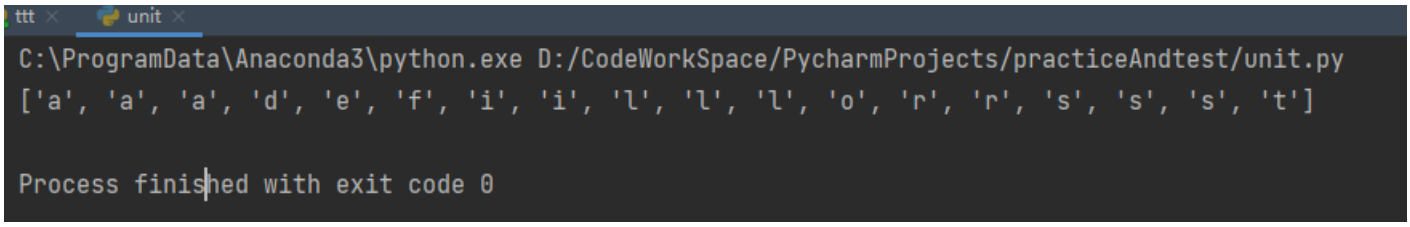
2. 选出关键词

> “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：



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

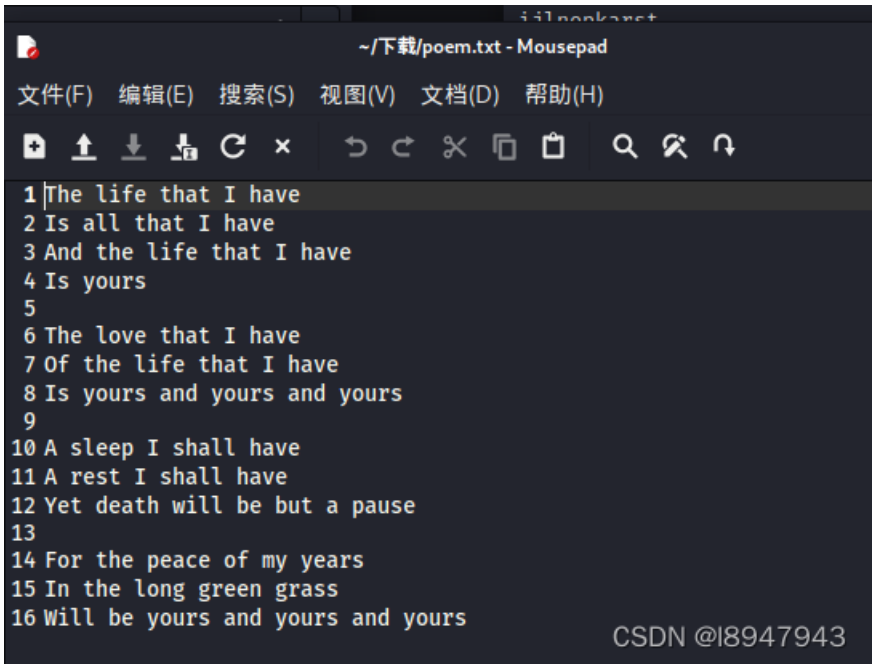
接着搞个排列：

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

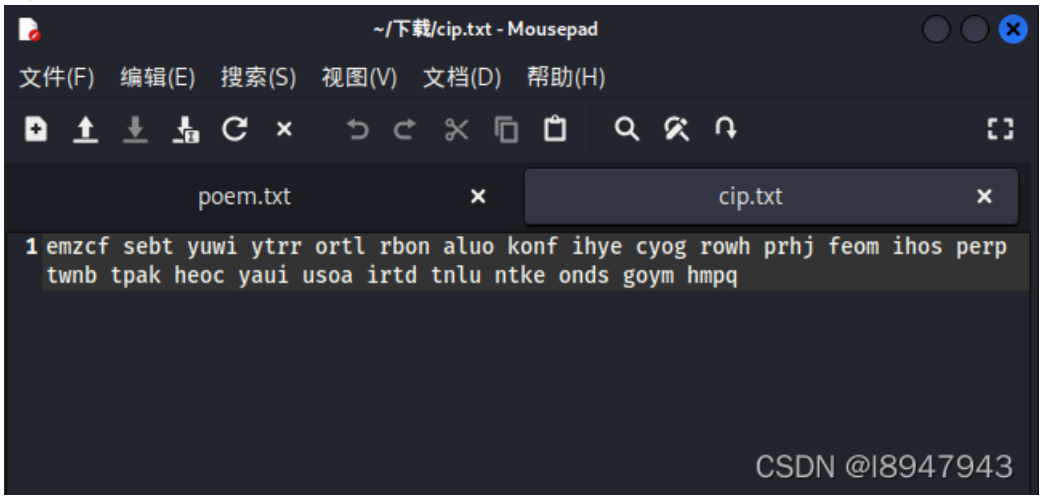
那么，诗歌片段中的第一个字母“f”；下面是6：第二个字母是“o”，下面是12。在我们的（填充的分组信息）中，第6列字母组合是“eud”，第12列字母组合是“tdk”。
以此类推，可以通过给出的关键词实现对信息的加密。

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：



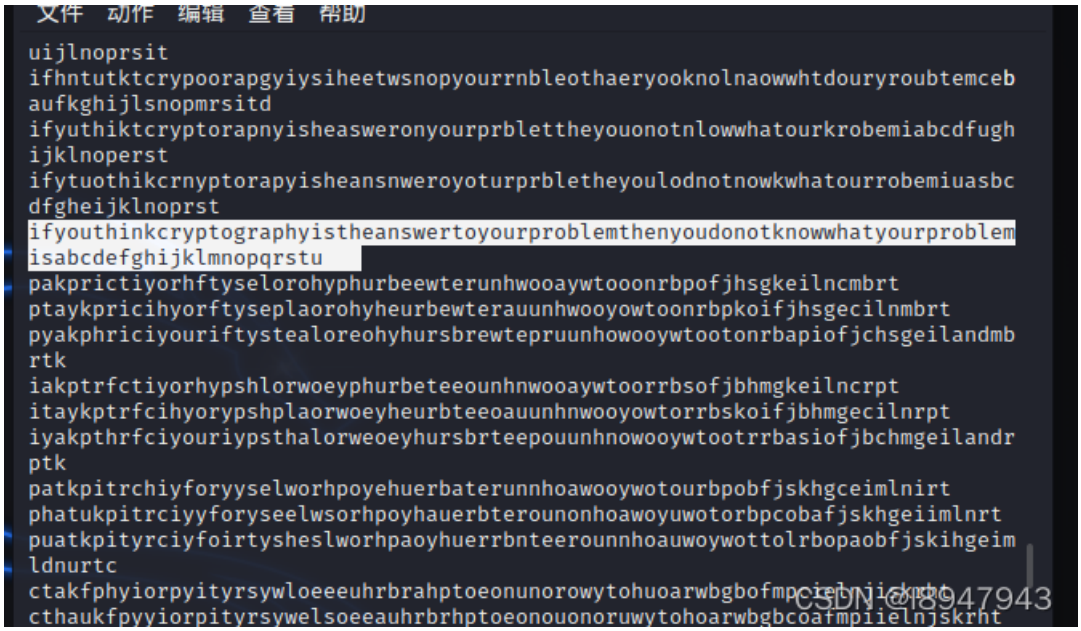
将解密信息存储成cip.txt



最后运行脚本：

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

结果如图：



最终答案为：

`ifyouthinkcryptographyistheanswertoyourproblemthenyoudonotknowwhatyourproblemisabcdefghijklmnopqrstu`