# 攻防世界crypto高手题之Decrypt-the-Message

原创

沐一 · 林 于 2021-09-12 14:59:05 发布 134 收藏

分类专栏： CTF 密码学 文章标签： ctf



本文链接：https://blog.csdn.net/xiao__1bai/article/details/120250452



CTF 同时被 2 个专栏收录

167 篇文章 6 订阅

订阅专栏

密码学

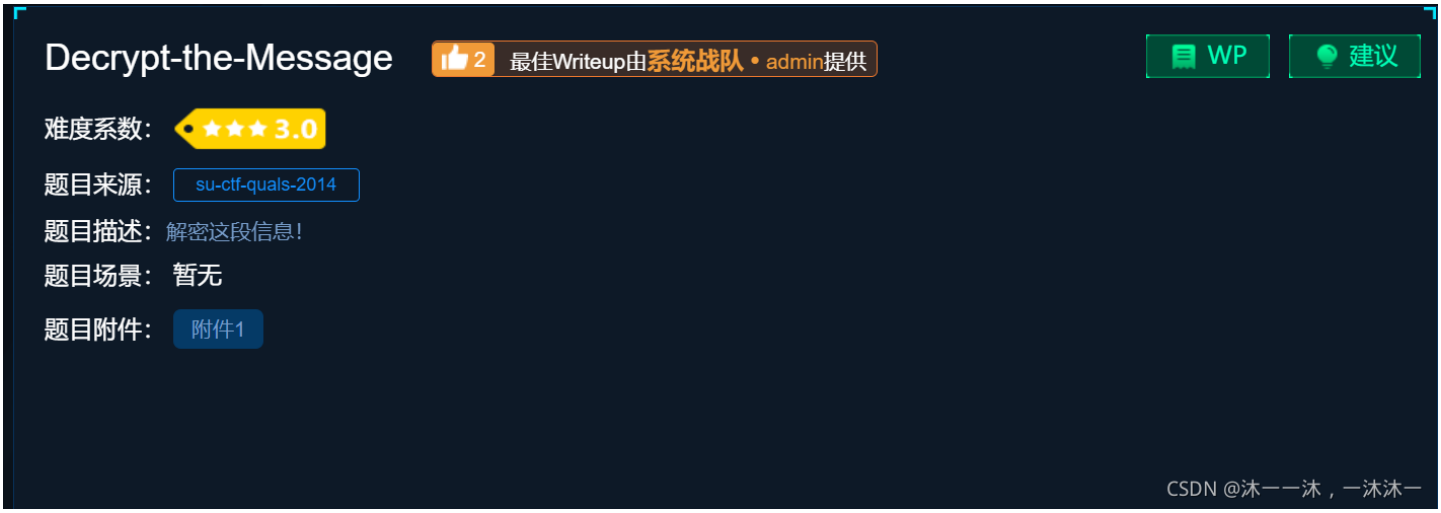
51 篇文章 1 订阅

订阅专栏

## 攻防世界crypto高手题之Decrypt-the-Message

继续开启全栈梦想之逆向之旅~

这题是攻防世界crypto高手题的Decrypt-the-Message



下载附件，是个.txt文件，内容是诗歌，下面是一行四不像的英文，后来发现是加密后的密文：

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 usoa irtd tnlu ntke onds goym hmpq



.

.

（这里积累第一个经验）

诗歌类的加密，一开始还以为是唐伯虎点秋香中句子开头组成实际内容，结果发现不是。查了查资料，是`poem codes`加密，下面给出别人梳理好的加密过程：

(内容地址出处)https://blog.csdn.net/weixin_45530599/article/details/108027293

① 给出一首诗歌

.

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

.

② 给出5个关键单词。

.

“for”, “sail”, “all”, “stars”, “die.”

.

对其进行拆散：

.

f o r s a i l a l l s t a r s d i e

.

接下来按照 字母表顺序 进行编号，若遇相同字母，则继续 +1

.

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

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 8 | 5 | | | | | | | | | | | | | | | | | |



.

③ 将要传递的消息进行加密。

.

We have run out of cigars, situation desperate。

.

先对其进行编码。因为给出的5个 关键词 ，其长度为18.所以以18为一组。

.

若一组长度 不满 18，则用abc(不要求有序)进行补充。

| 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 |

.

将排好的消息，按照之前给出的诗歌字母编号写下密文。

.

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

.

如， for --> eud tdk oek 那么得到的又可以按照5个（适当个数）为一组进行重新分组，得到最后密文。

.

.

我的看法：

其实排序逻辑挺常规的，就是 诗歌 --> 关键词 ， 原文 --> 参照顺序排列 ， 密文 --> 按诗歌关键词对原文映射取值 。

.

.

然后，我也不知道诗歌中关键词在哪，而且题目诗歌内容也太长了，所以只能用github的脚本了：(单独赋值poemcode.py是会报错的，因为文件中有其他依靠)

```
git clone git://github.com/abpolym/crypto-tools
```

.

.

(这里积累第二个经验)

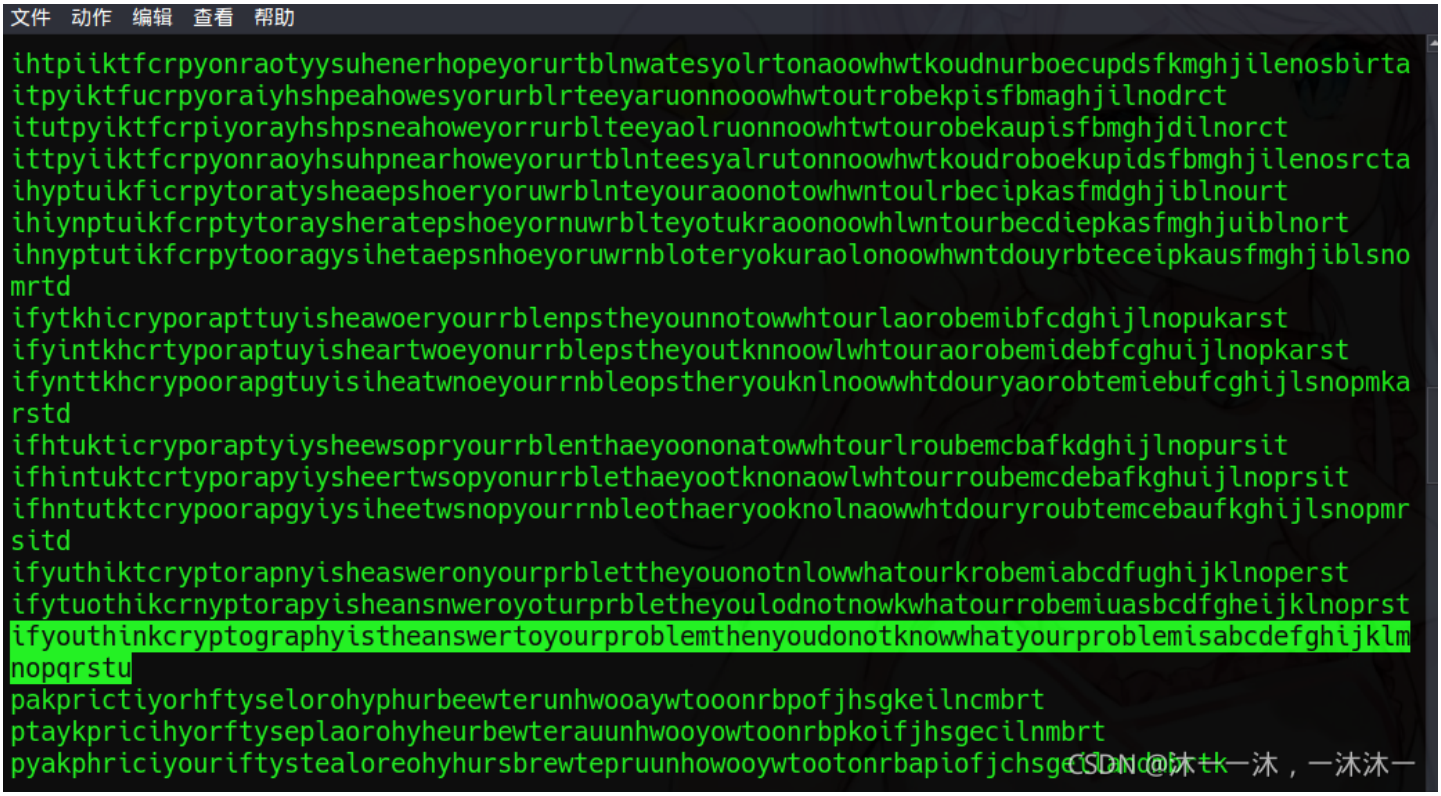
用法：(python2，ctfpoem是诗歌，ctfcip是加密密文)

```
python2 poemcode.py examples/2/ctfpoem  examples/2/ctfcip
```

.

.

结果，在众多输出中找到通顺的句子，其实后面我也不知道后面开头的单词合不合理，英语太菜了~(哭 ~)




.

.

总结：

1：

（这里积累第一个经验） 诗歌类的加密，一开始还以为是唐伯虎点秋香中句子开头组成实际内容，结果发现不是。查了查资料，是 `poem codes` 加密，下面给出别人梳理好的加密过程：

① 给出一首诗歌

.

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

.

② 给出5个关键单词。

.

“for”, “sail”, “all”, “stars”, “die.”

.

对其进行拆散：

.

f o r s a i l a l l s t a r s d i e

.

接下来按照 字母表顺序 进行编号，若遇相同字母，则继续 +1

.

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

| | | | | | | |
|---|---|---|---|---|---|---|
| i | e | | | | | |
| 8 | 5 | | | | | |



.

③ 将要传递的消息进行加密。

.

We have run out of cigars, situation desperate。

.

先对其进行编码。因为给出的5个 关键词 ，其长度为18.所以以18为一组。

.

若一组长度 不满 18，则用abc(不要求有序)进行补充。

| 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 |

.

将排好的消息，按照之前给出的诗歌字母编号写下密文。

.

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

.

如， for --> eud tdk oek 那么得到的又可以按照5个（适当个数）为一组进行重新分组，得到最后密文。

.

.

我的看法：

其实排序逻辑挺常规的，就是 诗歌 --> 关键词 ， 原文 --> 参照顺序排列 ， 密文 --> 按诗歌关键词对原文映射取值 。

2：

(这里积累第二个经验) 用法：(python2，ctfpoem是诗歌，ctfcip是加密密文)

```
python2 poemcode.py examples/2/ctfpoem examples/2/ctfcip
```

解毕！敬礼！