攻防世界crypto部分Decrypt-the-Message的writeup

原创

> 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

这是一种比较奇特的加密方式，叫做Poem Codes，详见：http://wmbriggs.com/post/1001/

加密过程如下：

（1）就其算法而言，去诗歌头一个单词，全部罗列出来，然后所有单词的字母按字母表排序并编码，如第一个a为1，第二个a为2，如果没有a了就看b，第一个b为3，第二个b为4，一直排列下去。。。

（2）将要加密的信息的字母每18个一行（不足一行的abcdef....补足）

（3）将加密的信息第一个字母对应第一步的编码数字，到第二步生成的字母表中取某列。

（4）分组即成加密信息。

解密过程非常复杂，不过，有人已经写好了解密工具，详见：https://github.com/abpolym/crypto-tools/tree/master/poemcode

具体用法如下（请注意只支持python2）：

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

猜解出一大堆消息，选择最像的那条即可，flag是：

```
ifyouthinkcryptographyistheanswertoyourproblemthenyoudonotknowwhatyourproblemisabcdefghijklmnopqrstu
```