西普实验吧密码学CTF--古典密码的安全性不高，但仍然十分美妙，请破译下面的密文

原创

Neil-Yale 于 2017-03-18 22:35:37 发布 3101 收藏 1
文章标签： 密码学 安全 破解 CTF

题目链接：http://www.shiyanbar.com/ctf/51

古典密码，说到安全性不高，则置换密码可以通过高频词分析破解

高频词手工破解思路：

单个的字母一般是a或者i，当然也有用o的

最常用的双子母单词是of，然后是to，in

最常用的三字母单词是the，然后是and

q后边基本我们常见的都是跟着u

元音字母后边最多辅音字母是n

最常见的双字母按频率依次是：ll ee oo tt ff rr nn pp cc

最常见的四字母单词是that

但是我们可以使用自动化的工具quipquip
这网站打不开了，我也谷歌找了半天找到个差不多的

这里第二个空格栏是说让我们提供些线索，也就是说我们觉得可能什么单词对应什么单词，填在此栏即可，我们认为dsln可能是flag的意思
破解结果如下

```
0    -2.768  ?l fog?vryoe?sg, e h?dhv?v?v?rl f??sao ?h e ?avsrb rc alfrb?ly dg ?s?fs ?l?vh rc ?ne?lvaiv eoa oa?nefab ??vs f??saovaiv, effrob?ly vr e oay?neo hghva?; the units may be
                single letters (the most common), pairs of letters, triplets of letters, mi?tures of the above, and so forth. The receiver deciphers the te?t by performing an inverse
                substitution. So the flag is nl_2hen-d3_hul-mi-ma_a

1    -2.816  ?l fog?vr?oe?sg, e h?dhv?v?v?rl f??sao ?h e ?avsrb rc alfrb?l? dg ?s?fs ?l?vh rc ?ne?lvaiv eoa oa?nefab ??vs f??saovaiv, effrob?l? vr e oa??neo hghva?; the units ma? be
                single letters (the most common), pairs of letters, triplets of letters, mi?tures of the above, and so forth. The receiver deciphers the te?t b? performing an inverse
                substitution. So the flag is nl_2hen-d3_hul-mi-ma_a

2    -2.818  ?l fog??ryoe?sg, e h?dh??????rl f??sao ?h e ?a?srb rc alfrb?ly dg ?s?fs ?l??h rc ?ne?l?ai? eoa oa?nefab ???s f??sao?ai?, effrob?ly ?r e oay?neo hgh?a?; the units may be
                single letters (the most common), pairs of letters, triplets of letters, mi?tures of the abo?e, and so forth. The recei?er deciphers the te?t by performing an in?erse
                substitution. So the flag is nl_2hen-d3_hul-mi-ma_a
```


逐一尝试我们觉得可行的flag，得到正确结果