


BUUCTF old-fashion

原创

宁嘉  于 2020-05-13 16:48:55 发布  2140  收藏 1

分类专栏: [BUUCTF Crypto](#) 文章标签: [密码学](#)

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/MikeCoke/article/details/106101582>

版权

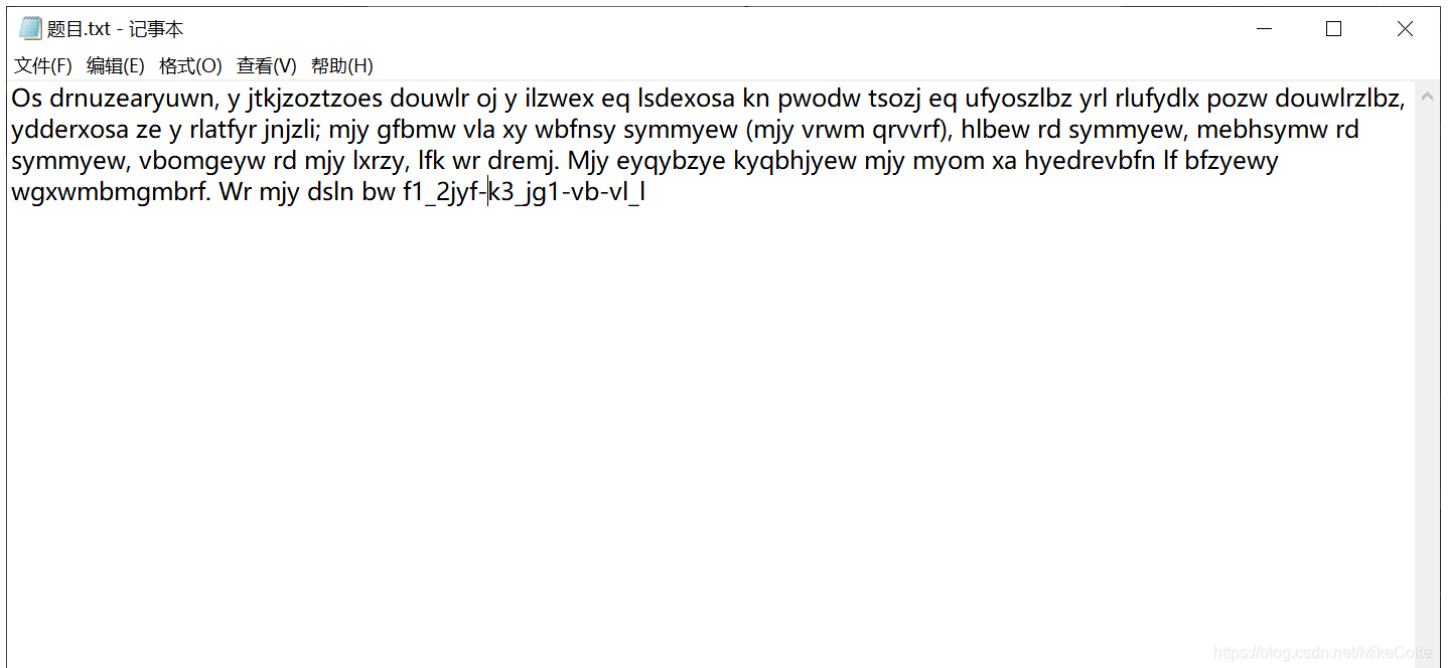


[BUUCTF Crypto](#) 专栏收录该内容

34 篇文章 2 订阅

订阅专栏

打开压缩包得到文本



词频分析，替换密码，用[爆破工具](#)

quipqiup **BETA**

quipqiup is a fast and automated cryptogram solver by [Edwin Olson](#). It can solve simple substitution ciphers often found in newspapers, including puzzles like cryptoquips (in which word boundaries are preserved) and patristocrats (inwhi chwor dboun darie saren t).

Puzzle:

Os drnuzearyuwn, y jtkjzoztzoes douwlr oj y ilzwex eq lsdexosa kn pwodw tsozj eq ufyzszlbz yrl rlufydlx pozw douwlrzlbz, ydderxosa ze y rlatfyr jnjzli; mgy gfbmw vla xy wbfnsy symmyew (mgy vrwm qrvvrf), hlbew rd symmyew, mebhsynw rd symmyew, vbomgeyw rd mgy lxrzy, lfk wr dremj. Mgy eyqybzye kyqbhgyew mgy myom xa hyedrevbfn lf bfzyewy wgxwmbmgmbrf. Wr mgy dsln bw fl_2jyf-k3_jg1-vb-vl_1

Clues: For example G=R QVW=THE

auto

Solve

<https://blog.csdn.net/MikeCoke>

| | | |
|---|--------|---|
| 0 | -2.814 | ?l fog?vryoe?sg, e h?dhv?v?v?rl f??sao ?h e ?avsrbc 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 n1_2hen-d3_hu1-mi-ma_a |
| 1 | -2.822 | Xl fogkvryoe?sg, e h?dhvxvjv?rl f?ksao xh e ?avsrbc rc alfrbxly dg wxsfs jlxvh rc knexlvaiv eoa oaknefab wxvs fxksaovaiv, effrob?ly vr e oayjneo hghvaz; the units may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth. The receiver deciphers the text by performing an inverse substitution. So the flag is n1_2hen-d3_hu1-mi-ma_a |
| 2 | -2.864 | ?l fog??ryoe?sg, e h?dh?????rl f??sao ?h e ?a?srbc 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 above, and so forth. The receiver deciphers the te?t by performing an inverse substitution. So the flag is n1_2hen-d3_hu1-mi-ma_a |
| 3 | -2.866 | ?l fog?vryoe?sg, e h??hv?v?v?rl f??sao ?h e ?avsrbc rc alfrb?ly ?g ?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 n1_2hen-?3_hu1-mi-ma_a |
| 4 | -2.866 | ?l fog?vryoe?sg, e h?ahv?v?v?rl f??s?o ?h e ??vsrbc rc ?lfrb?ly ag ?s?fs ?l?vh rc ?ne?lv?iv eo? o??nef? b ??vs f??s?ov?iv, effrob?ly vr e o?y?neo hghv??; the units may be single letters (the most common), p? |

得到flag:

flag{n1_2hen-d3_hu1-mi-ma_a}