**参考wp地址：**

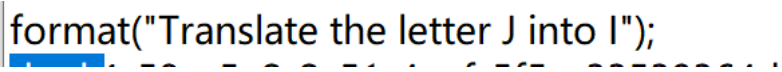
**<https://blog.csdn.net/weixin_45859850/article/details/109822044>**

**在线解密网址：**

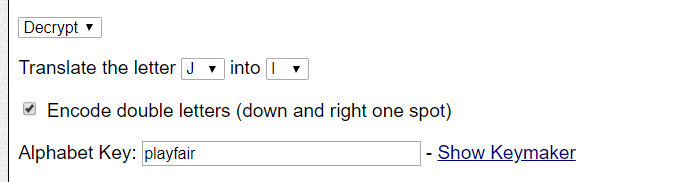
**<http://rumkin.com/tools/cipher/playfair.php>**

**另外提一下，在东华杯misc最后一题中：**

**存在关键字**



**进而可以找到这个解密网址。。。。**



**Playfair密码原理**

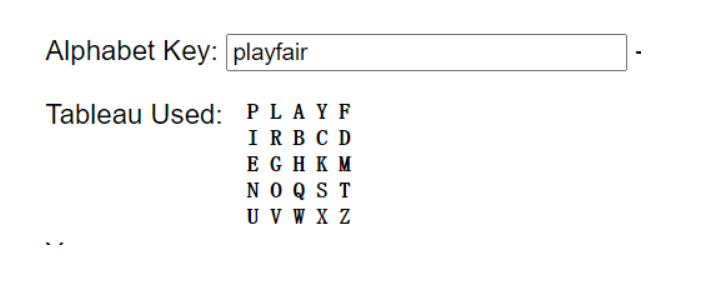
编一个5行5列的密码表。

第一列（或第一行）是密钥,其余按照字母顺序，如果密钥过长可占用第二列或行。密钥是一个单词或词组，若有重复字母，可将后面重复的字母去掉。当然也要把使用频率最少的字母去掉（它依据一个55的正方形组成的密码表来编写，密码表里排列有25个字母。如果一种语言字母超过25个，可以去掉使用频率最少的一个。如，法语一般去掉w或k，德语则是把i和j合起来当成一个字母看待，英语中z使用最少，可以去掉它）。

根据题目提示可以得到秘钥为play-fair（公平）

密钥是playfair，去掉重复的后为密码表前面字母为playfir

**playfair加解密**



整理明文/密文

整理明文/密文，将明文/密文每两个字母组成一对。如果成对后有两个相同字母紧挨或最后一个字母是单个的，就插入一个字母X（或者Q）

**加密规则：**

（1） 若c1 c2在同一行，对应明文p1 p2分别是紧靠c1 c2 左端的字母。其中最后一列被看做是第一列的左方。

（2） 若c1 c2在同一列，对应明文p1 p2分别是紧靠c1 c2 上方的字母。其中最后一行被看做是第一行的上方。

（3）若c1 c2不在同一行，不在同一列，则p1 p2是由c1 c2确定的矩形的其他两角的字母。

**解密规则:**

（1）若p1 p2在同一行，对应密文c1 c2分别是紧靠p1 p2 右端的字母。其中第一列被看做是最后一列的右方。如，按照前表，fg对应gj，mr对应om

（2） 若p1 p2在同一列，对应密文c1 c2分别是紧靠p1 p2 下方的字母。其中第一行被看做是最后一行的下方。

（3）若p1 p2不在同一行，不在同一列，则c1 c2是由p1 p2确定的矩形的其他两角的字母（至于横向替换还是纵向替换要事先约好，或自行尝试）。如，按照前表，ir对应pa或ap。

