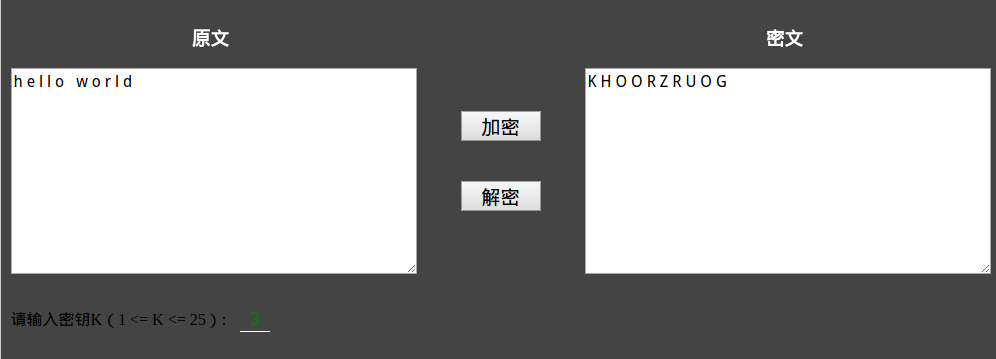
四个算法的基本展示页面如下：



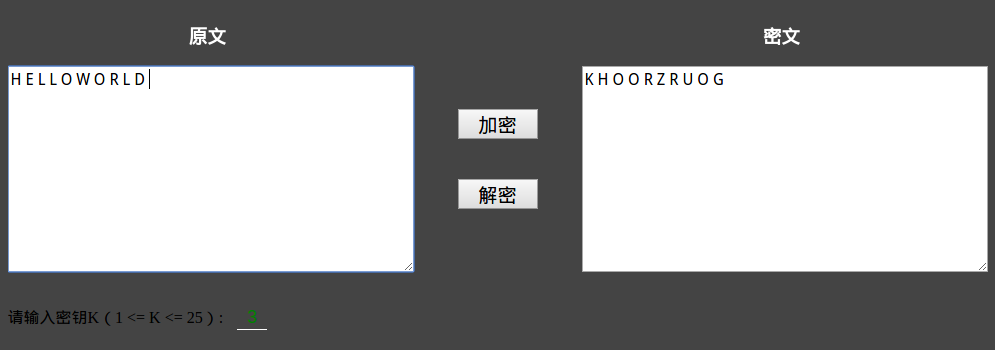
**一、Caesar算法**

默认密钥是3

输入字符串， 点击加密按钮即可进行加密获得密文信息KHOORZRUOG：



点击解密按钮，即可将密文解密获得原文输入信息HELLOWORLD：



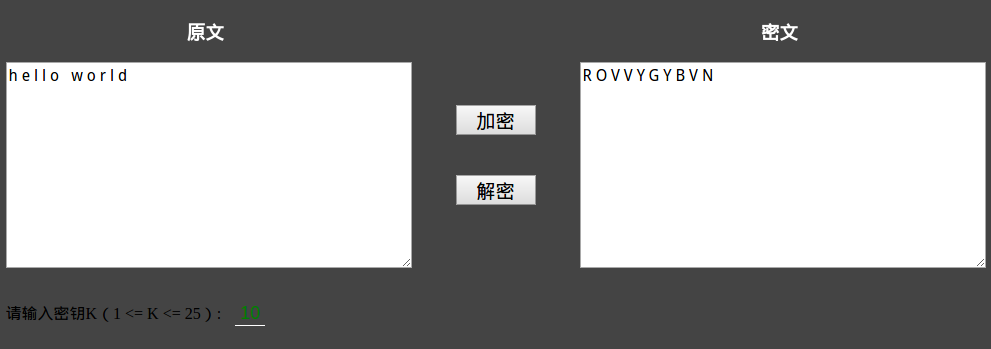
输出原文信息对比可知与原来输入的是一致的。

用户也可以自己输入密文，点击解密按钮获得对应的相应的原文信息：



用户可以随意选择密钥K进行加密或者解密，K的范围是[1, 25],

例如选择密钥K选择10，则hello world加密得到的是ROVVYGYBVN：



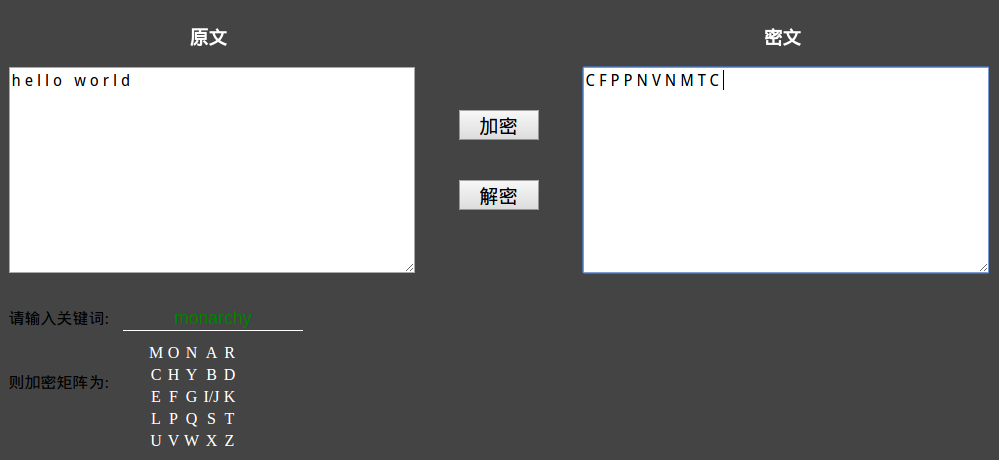
1. **Playfair算法**

默认密钥关键词是monarchy

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| M | O | N | A | R |
| C | H | Y | B | D |
| E | F | G | I/J | K |
| L | P | Q | S | T |
| U | V | W | X | Z |

则生成的加密矩阵是：

输入hello world，点击加密按钮得到密文CFPPNVNMTC：



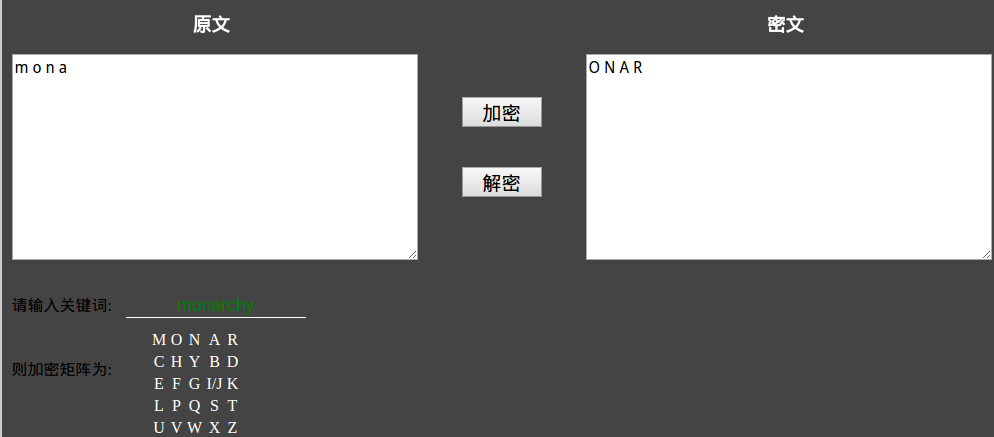
点击解密按钮可获得同样的原文信息HELLOWORLD：



考虑三种情况：

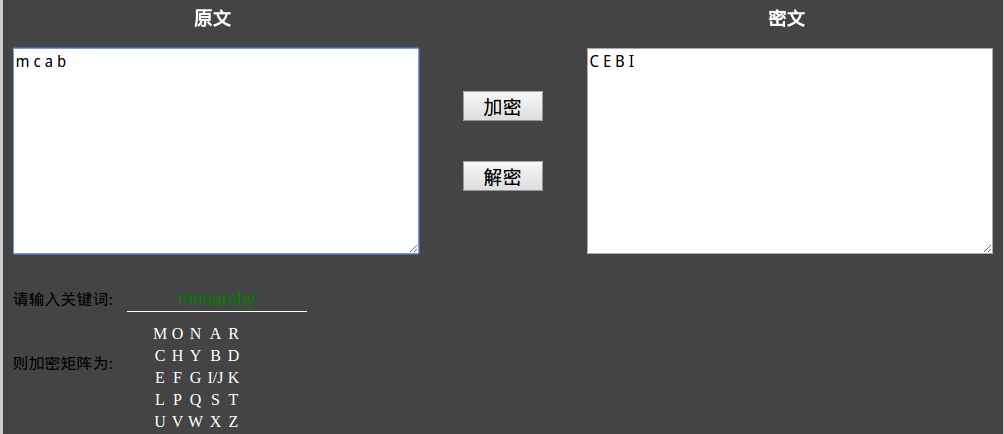
1. 当输入的字母刚好位于矩阵同一行上

例如mona加密之后是ONAR：



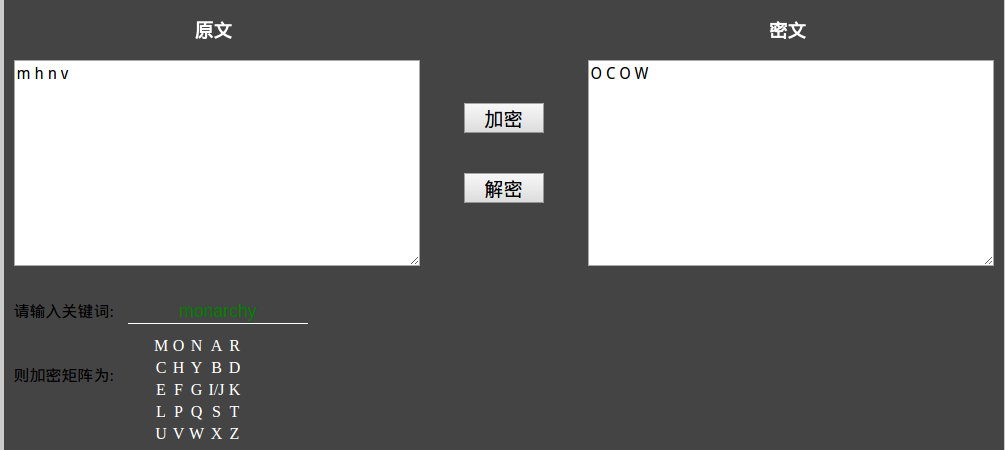
1. 当输入的字母刚好位于矩阵同一列上

例如mcab加密之后是CEBI



1. 当输入的字母不同行不同列

例如mhnv加密之后是OCOW



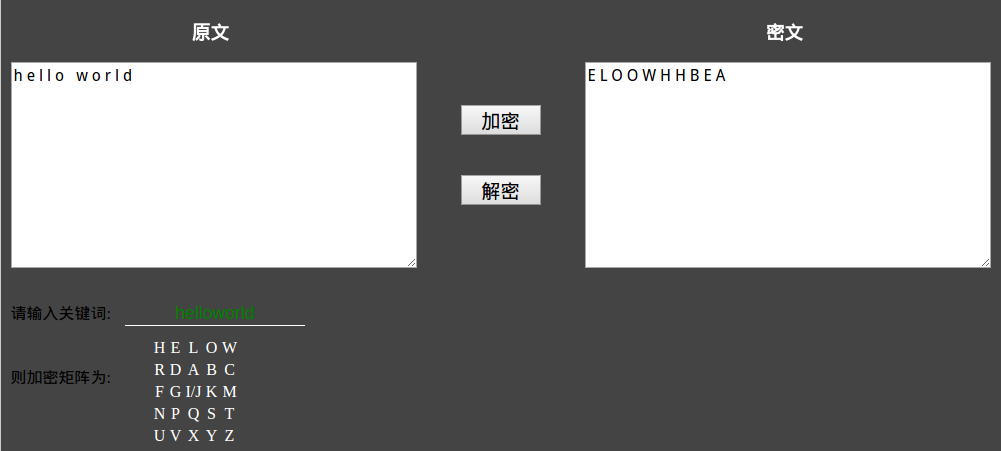
通过输入关键词，即可对应的修改加密矩阵，从而获得不同的密钥。

例如输入关键词：helloworld

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| H | E | L | O | W |
| R | D | A | B | C |
| F | G | I/J | K | M |
| N | P | Q | S | T |
| U | V | X | Y | Z |

则加密矩阵为：

同样加密hello world可获得和之前不一样的密文ELOOWHHBEA：



解密之后得到，同样可以获得原文信息HELLOWORLD：



1. **Hill算法**

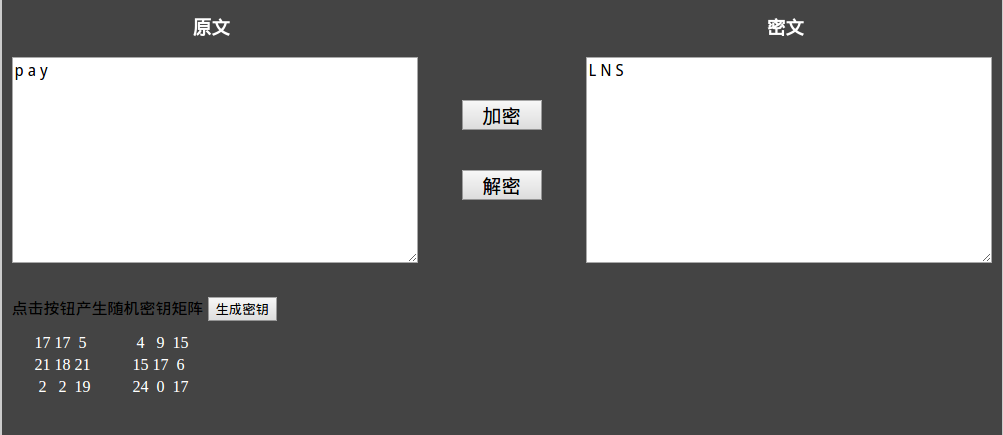
|  |  |  |
| --- | --- | --- |
| 17 | 17 | 5 |
| 21 | 18 | 21 |
| 2 | 2 | 19 |

默认随机加密矩阵是：

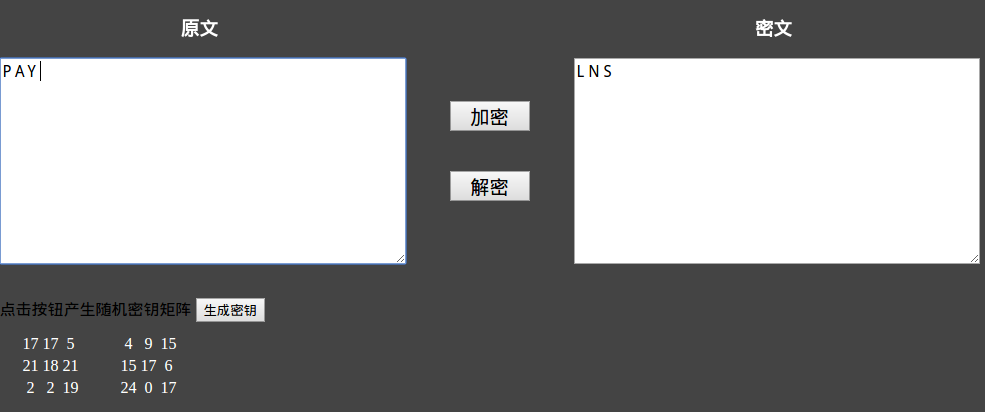
|  |  |  |
| --- | --- | --- |
| 4 | 9 | 15 |
| 15 | 17 | 6 |
| 24 | 0 | 17 |

则相应的解密矩阵是：

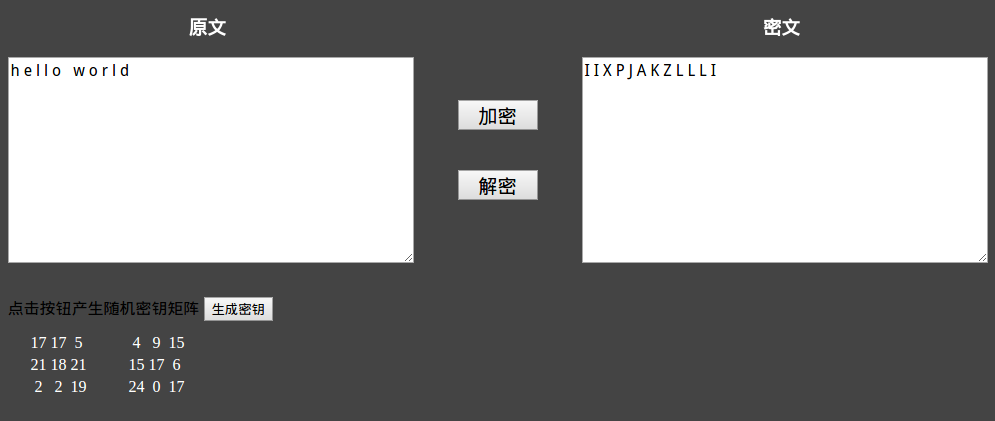
按照课本例子输入pay获得密文信息LNS：



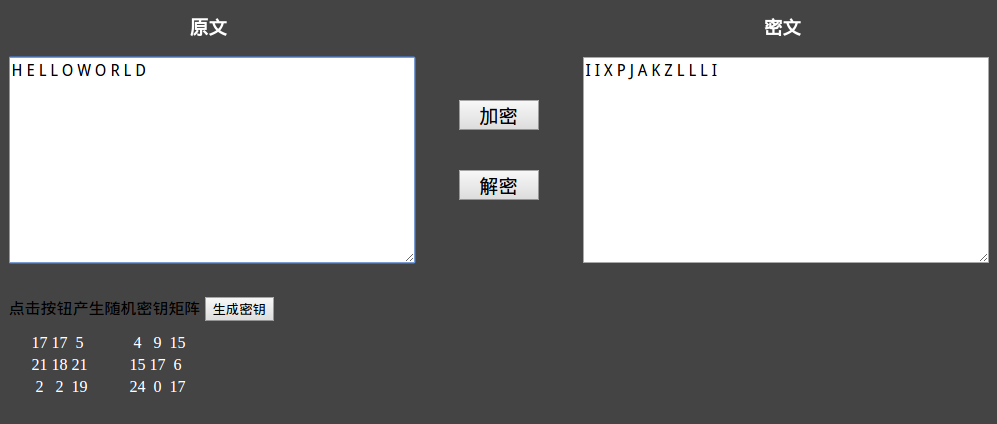
解密可以获得原文信息PAY：



输入原文hello world，点击加密按钮得到密文IIXPJAKZLLLI：



点击解密按钮，可以获得对应的原文信息HELLOWORLD：



1. **Rsa算法**

默认初始随机素数是101， 103

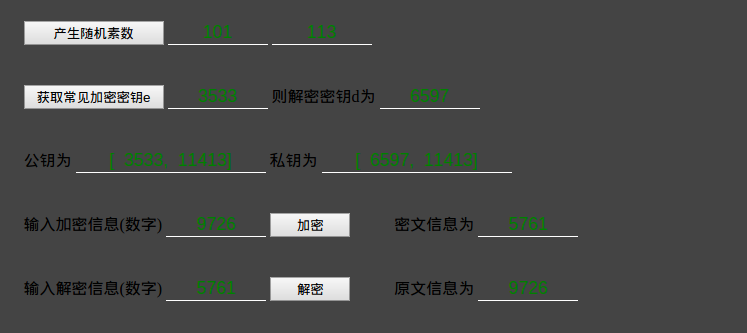
默认加密密钥e是3533，则相应的解密密钥d为6597

则公钥为[ 3533, 11413]， 私钥为[ 6597, 11413]

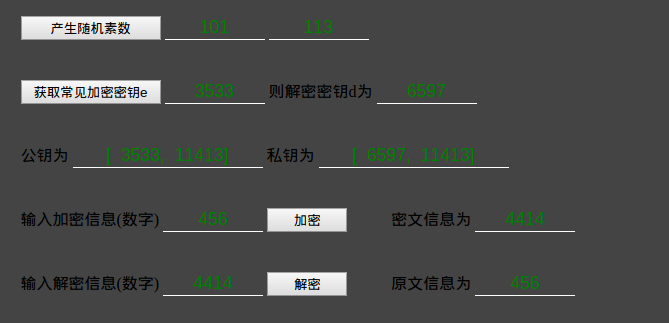
课本例子：

则输入加密信息9726，点击加密按钮，可以得到密文信息5761，

输入解密信息5761，点击解密按钮，可以得到原文信息9726



输入其他加密解密信息例子，截图如下：



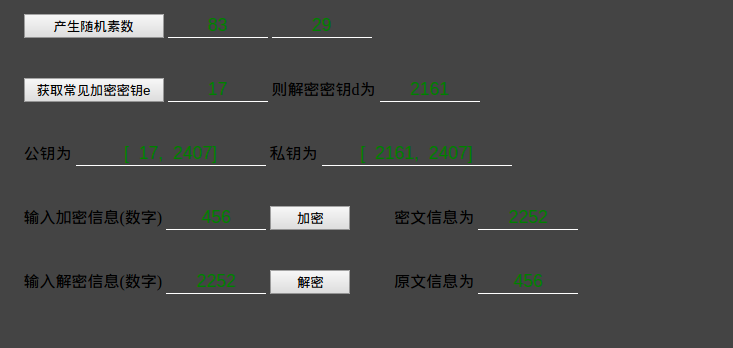
用户可以通过点击产生随机素数，来获去其他素数，再而获取常见的随机密钥e，来获得不同的公钥和私钥。

例如：点击产生随机素数之后获得素数83, 29；点击获取常见加密密钥e获得加密密钥17，则解密密钥d为2161；

因此：公钥为[ 17, 2407]，私钥为[ 2161, 2407]

输入加密信息456，点击加密按钮得到密文信息为2252；

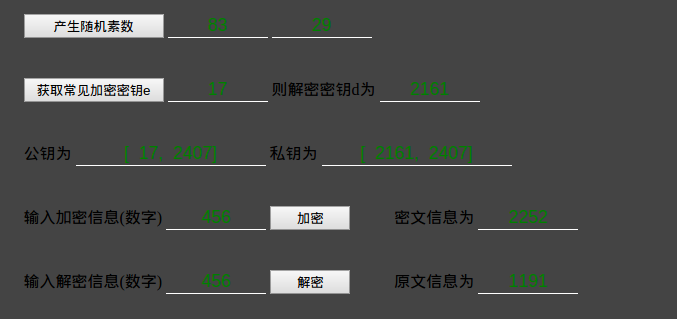
输入解密信息2252，点击解密按钮得到原文信息为456：



加密信息和加密信息是相互不影响的

例如你可以输入加密信息456，获得密文信息2252，

同时你也可以输入解密信息456，获得原文信息为1191



通过对应的输入上面的原文信息1191和密文信息2252，可以获得相应的密文信息和原文信息都是456，，则可以验证算法的准确性。

如下截图：

