我们拥有多年的区块链服务经验，为用户提供专业的服务信息。这里是换位密码和换位密码转换器。精选可以随时随地解决玩币遇到的各种问题，让你不再为职称评定的繁琐业务而烦恼。

例如，用句点e换位，将明文字母相除。

换位密码是一种早期的加密方法，它保持了与明文相同的字母，不同的是顺序是乱序的。

经典密码：

从远古时代到香农&#039；s1949年出版的《保密系统的通信理论》，这一时期人类使用的所有密码都被称为经典密码。本文主要介绍了三种经典密码，即置换密码、替换密码和轮换密码。

置换密码(也称换位密码):

是一个密码系统，它指示重新排列文本中字符的位置以获得密文。

特点：保持Ming=text中所有字符不变，但使用替换来打乱明文字符的位置和顺序。

排列的定义：有限集x上的运算:xx，是双射函数，则称为排列。

即任意xX有唯一的x&#039X，所以(X)=X&#039；

逆置换&#039；将用于解密，即任何x&#039X，并且存在唯一的xX，所以&#039；(x&#039)=x和&#039；=i.

在我们对排列有了基本的了解之后，让&#039；让我们谈谈排列密码。有两种排列密码。，一个是列替换密码，另一个是定期替换密码。

列置换密码：

列置换密码，顾名思义，按列置换，逐列读出明文序列，得到密文。具体加密步骤如下：

。

将明文p逐行写入一个nm阶矩阵，分组长度固定为m(如果不是m的倍数，会加上多余的空格)。

根据(1，2，3…m)的排列交换列的位置，其中是关键。

按照列的顺序读出新获得的矩阵，以获得密文C.

解密过程如下：

密文C写成nm阶矩阵，列长固定n

根据逆矩阵&#039；

按行依次以纯文本形式读取矩阵。

周期置换：

周期变换密码是将明文P按照固定长度m分组，然后按照置换重新排列每组字符串的位置，得到密文。

周期排列的思路和列排列的思路是一样的，只是列的排列是以矩阵的形式改变整列的位置，周期是分组后分别变换各组。知道列的排列就很容易理解周期排列。

替代密码(也称为替代密码):

就是解释在密文中每个字符被另一个字符替换，被替换的字母保持原来的位置，通过密文的反向替换可以恢复明文。

替代密码分为单表替代密码和多表替代密码。

单表替换密码我们分别介绍凯撒密码和仿射密码。

凯撒密码：

凯撒密码根据凯撒密码替换表替换26个英文字母。

经典加密算法：置换密码

排列密码算法的原理是在不改变明文字符的情况下，改变明文中字符的排列顺序，

从而实现明文信息的加密。置换密码有时也称为换位密码。

矩阵转置法是实现置换密码的常用方法。。它将文本中的字母按照给定的顺序排列成一个矩阵，然后将矩阵中的字母按照密钥提供的顺序重新组合，从而形成密文。例如，明文是攻击

从

开始于

五。，密钥是cipher，明文以每行6列的形式排列在矩阵中，形成如下形式：

a

t

t

a

g

I

n

s

a

t

f

I

v

e

根据字母表中密钥中字母的顺序，给出一个排列：

1

2

3

4

[

=

1

4

5

3

2

,第6列的顺序排列，则有下面形式：

a

a

c

t

t

k

b

I

n

g

e

s

a

I

v

f

t

e

从而得到密文：aacttkbingesaifte

加密转置密码只需要加密明文，通过密钥重新排列其中字母的位置。具体方法如下

1。基于二维数组移位的加密算法

给出二维数组的列数。即二维数组的每一行中可以存储的字符数。然后将明文串按行依次排列成二维数组。最后将二维数组中的字符按列读出，从而得到密文。

2。换位解密算法(基于二维数组移位的解密算法)

首先给定二维数组的列数，即二维数组的每一行可以存储的字符数，这个数要和加密算法中的一致。接下来，将密文串逐列排列成二维数组。最后，逐行读出二维数

组中的字符。

3。换位加密算法

首先将待加密的明文按照密钥排列顺序加密：0123456789abcdefghijklmnopkrstuvwxyz，然后列表找出对应的字母，即为密钥。。然后对它们进行转置加密，即按照密钥排列顺序对表的第二行进行排序，得到加密的密文。

扩展数据

数据加密技术的分类

1。特殊键

也称对称密钥或单密钥，加密和解密用的是同一个密钥，也就是同一个算法。单密钥是最简单的方式，通信双方必须互相交换&#039；s密钥，当他们需要互相发送消息时，他们会用自己的加密密钥对消息进行加密。在接收方接收到数据后，用对方给的密钥解密。当要对文本进行加密和传输时，用密钥对文本进行加密以形成密文，并且在信道上传输密文。收到密文后，用同一个密钥对密文进行解密，形成一个通用的样式进行读取。

2。对称密钥

对称密钥是最古老的，通常认为&quot秘密代码&quot使用对称密钥。对称密钥由于计算量小、速度快、安全性高，至今仍被广泛使用。它将数据分成64位数据块，其中8位用于奇偶校验。，剩下的56位作为密码的长度。首先替换原始文本得到一个64位的混沌数据集，然后将其分成相等的两段；第三步，用加密函数进行变换，在给定密钥参数的情况下，多次迭代，得到加密的密文。

3。公钥

也称为非对称密钥。加密和解密使用不同的密钥，即不同的算法。虽然两者之间有一定的关系，但不能简单地从一个推导出另一个。。非对称密钥由于两个密钥(加密密钥和解密密钥)不同，所以一个密钥可以公开，另一个密钥可以保密，同样可以起到加密的作用。虽然公钥加密机制提供了很好的保密性，但是很难识别发送者。也就是说，任何获得公钥的人都可以生成和发送消息。

4。非对称加密技术

数字签名一般采用非对称加密技术(如RSA)，通过对整个明文进行某种变换得到一个值作为验证签名。。接收者使用发送者&#039；的公钥来解密签名。如果结果是明文，则签名有效，证明对方&#039；的身份是真实的。数字签名不同于手写签名。数字签名随着文字的变化而变化，手写签名反映一个人&#039；的性格特点。，是一样的；数字签名和文本信息密不可分，而手写签名是附着在文本上，与文本信息分离的。

参考来源：百度百科-换位密码

相信在边肖推出换位密码和换位密码转换器之后