拥有多年的区块链服务经验，为用户提供专业的服务信息，下面介绍换位密码，以及换位密码转换器，选择可以为您随时随地解决玩币中所遇到的各种问题，让你不再为职称评级繁琐事务而烦恼。

举例：周期为e的换位将明文字母划分。

换位密码就是一种早期的加密方法，与明文的字母保持相同，区别是顺序被打乱了。

古典密码：

从远古到1949年香农发表《保密系统的通信理论》，这期间人类所使用的密码均称为古典密码，本文主要介绍三种古典密码，分别为置换密码，代换密码和轮换密码。

置换密码（又称为换位密码）：

是指明文中各字符的位置次序重新排列得到密文的一种密码体制。

特点:保持明=文中所有的字符不变，只是利用置换打乱明文字符的位置和次序。

置换定义：有限集X上的运算σ：X→X，σ是一个双射函数，那么称σ为一个置换。

即任意x∈X,存在唯一的x′ ∈X，使得σ(x)=x′ 。

解密的时候会用到逆置换σ′ ,即任意x′ ∈X,存在唯一的x∈X，使得σ′ (x′ )=x且满足σσ′ =I。

对置换有了一个基本的认识之后我们来谈一下置换密码，置换密码有两种，一种为列置换密码，一种为周期置换密码。

列置换密码：

列置换密码，顾名思义，按列换位并且按列读出明文序列得到密文，具体加密步骤如下：

将明文p以固定分组长度m按行写出nxm阶矩阵（若不m倍数，空余部分空格补充）。

按（1,2,3…m）的置换σ交换列的位置,σ为密钥。

把新得到的矩阵按列的顺序依次读出得到密文c。

解密过程如下：

将密文c以固定的长度n按列写成nxm阶矩阵。

按逆矩阵σ’ 交换列的位置。

把矩阵按着行依次读出为明文。

周期置换：

周期变换密码是将明文P按固定长度m分组，然后对每组的字符串按置换σ重新排列位置从而得到密文。

周期排列与列排列思想是一致的，只不过列排列是以矩阵的形式整列换位置，而周期是在分组以后对每组分别变换。懂得列排列就可以很容易地理解周期排列。

代换密码（又称为替代密码）：

就是讲明文中的每个字符替代成密文中的另一个字符，替代后的各个字母保持原来的位置，在对密文进行逆替换就可以恢复出明文。

代换密码有分为单表代换密码和多表代换密码。

单表代换密码我们分别介绍凯撒密码和仿射密码。

凯撒密码：

凯撒密码依据凯撒密码代换表对26个英文字母进行替换。

古典加密算法:置换密码

置换密码算法的原理是不改变明文字符，只将字符在明文中的排列顺序改变，从而实现明文信息的加密。置换密码有时又称为换位密码。

矩阵换位法是实现置换密码的一种常用方法。它将明文中的字母按照给的顺序安排

在一个矩阵中，然后用根据密钥提供的顺序重新组合矩阵中字母，从而形成密文。例如，明文为attack

begins

at

five，密钥为cipher，将明文按照每行6列的形式排在矩阵中，形成如下形式：

a

t

t

a

c

k

b

e

g

i

n

s

a

t

f

i

v

e

根据密钥cipher中各字母在字母表中出现的先后顺序，给定一个置换：

1

2

3

4

5

6

f

=

1

4

5

3

2

6

根据上面的置换，将原有矩阵中的字母按照第1列，第4列，第5列，第3列，第2列，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：aacttkbingesaivfte

加密换位密码通过密钥只需要对明文进行加密，并且重新排列里面的字母位置即可。具体方法如下

1、基于二维数组移位的加密算法

给定一个二维数组的列数，即该二维数组每行可以保存的字符个数。再将明文字符串按行依次排列到该二维数组中。最后按列读出该二维数组中的字符，这样便可得到密文。

2、换位解密算法（基于二维数组移位的解密算法）

先给定一个二维数组的列数，即该二维数组每行可以保存的字符个数，并且这个数应该和加密算法中的一致。下面将密文字符串按列一次性排列到该二维数组中。最后按行读出该二维数组中的字符即可。

3、换位加密算法

首先按照密钥排列顺序：0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZ将想要加密的明文加密，然后列出表格，找出对应的字母，就是密钥。然后对他们进行换位加密，就是将表格的第二行依据密钥排列顺序进行排序以便得到加密后的密文。

扩展资料

数据加密技术的分类

1、专用密钥

又称为对称密钥或单密钥，加密和解密时使用同一个密钥，即同一个算法。单密钥是最简单方式，通信双方必须交换彼此密钥，当需给对方发信息时，用自己的加密密钥进行加密，而在接收方收到数据后，用对方所给的密钥进行解密。当一个文本要加密传送时，该文本用密钥加密构成密文，密文在信道上传送，收到密文后用同一个密钥将密文解出来，形成普通文体供阅读。

2、对称密钥

对称密钥是最古老的，一般说“密电码”采用的就是对称密钥。由于对称密钥运算量小、速度快、安全强度高，因而如今仍广泛被采用。它将数据分成长度为64位的数据块，其中8位用作奇偶校验，剩余的56位作为密码的长度。首先将原文进行置

换，得到64位的杂乱无章的数据组，然后将其分成均等两段；第三步用加密函数进行变换，并在给定的密钥参数条件下，进行多次迭代而得到加密密文。

3、公开密钥

又称非对称密钥，加密和解密时使用不同的密钥，即不同的算法，虽然两者之间存在一定的关系，但不可能轻易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）各不相同，因而可以将一个密钥公开，而将另一个密钥保密，同样可以起到加密的作用。公开密钥的加密机制虽提供了良好的保密性，但难以鉴别发送者，即任何得到公开密钥的人都可以生成和发送报文。

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，作为核实签名。接收者使用发送者的公开密钥对签名进行解密运算，如其结果为明文，则签名有效，证明对方的身份是真实的。数字签名不同于手写签字，数字签名随文本的变化而变化，手写签字反映某个人个性特征，是不变的；数字签名与文本信息是不可分割的，而手写签字是附加在文本之后的，与文本信息是分离的。

参考资料来源:百度百科-换位密码

相信经过小编对换位密码和换位密码转换器的介绍，你对换位密码了解更加地透彻了，感谢你对我们地支持与关注！