实验 1-1 古典密码算法

一．实验原理

古典密码算法历史上曾被广泛应用，大都比较简单，使用手工和机械操作来实现加密和解密。它的主要应用对象是文字信息，利用密码算法实现文字信息的加密和解密。下面介绍两种常见的具有代表性的古典密码算法，以帮助读者对密码算法建立一个初步的印象。

1． 替代密码

替代密码算法的原理是使用替代法进行加密，就是将明文中的字符用其它字符替代后形成密文。例如：明文字母 a、b、c、d ，用 D、E、F、G 做对应替换后形成密文。

替代密码包括多种类型，如单表替代密码、多明码替代密码、多字母替代密码、多表替代密码等。下面我们介绍一种典型的单表替代密码，恺撒(caesar)密码，又叫循环移位密码。它的加密方法，就是将明文中的每个字母用此字符在字母表中后面第 k 个字母替代。它的加密过程可以表示为下面的函数：

$E(m)=(m+k) \bmod n$

其中：m 为明文字母在字母表中的位置数；n 为字母表中的字母个数；k 为密钥；E(m)为密文字母在字母表中对应的位置数。

例如，对于明文字母 H，其在字母表中的位置数为 8，设 k=4，则按照上式计算出来的密文为 L：

$E(8) = (m+k) \bmod n = (8+4) \bmod 26 = 12 = L$

2． 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：

$$f = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \\ 1\,4\,5\,3\,2\,6 \end{pmatrix}$$

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：abatgftetcnvaiikse

其解密的过程是根据密钥的字母数作为列数，将密文按照列、行的顺序写出，再根据由密钥给出的矩阵置换产生新的矩阵，从而恢复明文。

二．实验目的

通过编程实现替代密码算法和置换密码算法，加深对古典密码体制的了解，为深入学习密码学奠定基础。

三．实验环境

运行 windows 或 linux 操作系统的 PC 机，具有 gcc（linux）、VC（windows）等 C 语言编译环境。

四．实验内容和步骤

1． 根据实验原理部分对替代密码算法的介绍，自己创建明文信息，并选择一个密钥 k，编写替代密码算法的实现程序，实现加密和解密操作。

2． 根据实验原理部分对置换密码算法的介绍，自己创建明文信息，并选择一个密钥，编写置换密码算法的实现程序，实现加密和解密操作。

五．实验报告要求

要求上述密码算法最后的实现程序提供加密和解密两个接口：int encrypt ( )和 int decrypt ( )，当加密或者解密成功时返回 CRYPT_OK，失败时返回 CRYPT_ERROR。