**密码学课程实训**

**实训要求：**

1. 要求提交可执行的代码和实验报告，课程报告封面写清楚自己的姓名和学号，实验报告的具体内容包括：实验名称、实验原理、具体实现步骤、以及核心代码等。

2、编程语言不做要求，选择自己擅长的即可。

3、最终代码和课程报告提交时间：

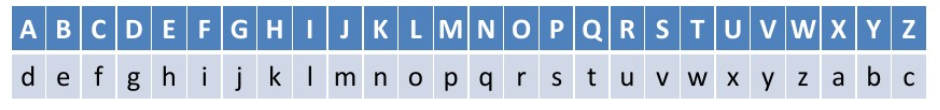
从以下题目中，每人任选两个题目完成，并写成相应的课程报告。

1. **古典密码系列（包含三个小实验）**

（1）凯撒密码

凯撒密码，又称移位密码，就是将字母表按照一定的移位个数进行移位，形成密码表，然后再按照此表进行加解密。凯撒密码的密钥是一个整数，即移位个数。

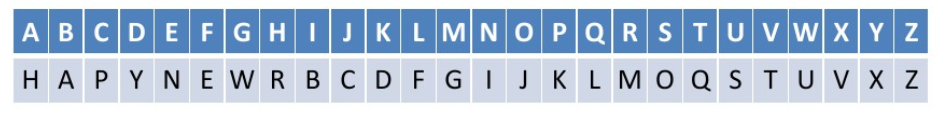
例如密钥是3，则明文、密文对照表如下：



编写一个程序，可以通过用户输入密码（一个小于26的正整数），生成密码表（即上面的那个表），然后可以对用户输入的明文进行加密，对输入的密文进行解密。

（2）密钥短语密码

凯撒密码很简单，但是通过穷举法很容易进行暴力破解。下面对凯撒密码进行进一步的改进。选一个英文短语，称其为密钥字（key word）或密钥短语（key phrase），例如HAPPY NEW YEAR， 按顺序去掉重复字母和空格得HAPYNEWR。将它依次写在明文字母表之下，而后再将明文字母表中未在短语中出现过得字母，依次写在此短语之后，就可以构造出一个代替表，如下表所示：



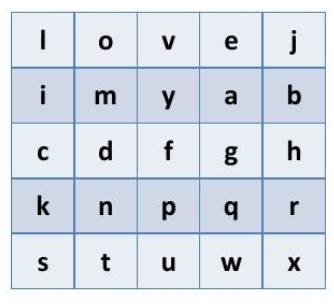
按照这个表，明文LOVE，变为密文FJTN。

编写一个程序，可以通过用户输入密码（一个字符串），生成密码表（即上面那个表），然后可以对用户输入的明文进行加密，对输入的密文进行解密。

（3）Playfair密码

前两个问题的密码表都是一维的，一维密码强度并不够。Playfair密码是二维密码的一个典型例子。Playfair密码依据一个5\*5的正方形组成的密码表来编写，密码表里排列有25个字母。如果一种语言的字母超过25个，就去掉使用频率最少的一个。例如，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。

加密描述：第一步是编制密码表。在这个5\*5的密码表中，共有5行5列字母。第一列或（第一行）是密钥，其余按照字母顺序。密钥是一个单词或词组，若有重复字母，可以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。例如，密钥是Live and learn， 去掉后则维liveandr。如果密钥过长可以占用第二行或第二列。如密钥love jimmy，可编制成：



第二步是整理明文。将明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。如communist，应成为co，mx，mu，ni，st。每对中的两个字母，可以用p1、p2代替。

最后编写密文。

1. 如果p1、p2在同一行，对应密文c1、c2分别是紧靠着p1、p2右端的字母。其中第一列被看作是最后一列的右方。按照上表，cf对应dg。
2. 如果p1、p2在同一列，对应密文c1、c2分别是紧靠p1、p2下方的字母，其中第一行被看作是最后一行的下方。例如dt对应no。
3. 若p1、p2不在同一行，也不在同一列，则c1、c2是由p1、p2确定的矩形其他两角的字母（至于是横向替换还是纵向替换可以事先约定好，或自行尝试）。例如，按照上表，mq对应an或者na（需要确定一种，并且贯彻始终）。

依照上面的密码和替换规则，假设明文为：ItIsNotEnoughToBeIndustrious，通过替换规则加密成（横向替换）：Os Ci Tm wO tm wf dX jM IA tn wt xn ml wt。

解密描述：Playfair解密算法首先将密钥填写在一个5\*5的矩阵中（去除重复字母和字母z），矩阵中其他未用到的字母按顺序填在矩阵剩余位置中，根据替换矩阵由密文得到明文。解密过程：

1. 若c1c2在同一行，对应明文p1p2分别是紧靠c1c2左端的字母。其中最后一列被看做是第一列的左方。
2. 若c1c2在同一列，对应明文p1p2分别是紧靠c1c2上方的字母。其中最后一行被看作是第一行的上方。
3. 若c1c2不在同一行，不在同一列，则p1p2是由c1c2确定的矩形的其他两角的字母。

这一过程和加密正好相反。

编写一个程序，可以通过用户输入密码（一个字符串），生成密码表（即上面那个表），然后可以对用户输入的明文进行加密，对输入的密文进行解密。

1. **DES密码**

DES是一种分组加密算法，每次加密或解密的分组大小均为64位，所以DES没有密文的扩充。对于大于64位的明文只要按每64位一组进行切割，而对于小于64位的明文，只要在后面补“0”即可。另一方面，DES所用的加密或解密密钥也是64位大小，但因其中有8个奇偶校验位，所以有效密钥长度是56位。

编程实现：采用56位密钥加密64位数据。然后可以对用户输入的明文进行加密，对输入的密文进行解密。

1. **RSA算法实现**

RSA算法是典型的公钥密码算法。公钥和私钥的生成和加解密过程可以参考教材。可以自己选定大素数p和q，编程实现对用户输入的明文进行加密，对输入的密文进行解密。

**4、基于混沌的图像加密算法**

数字图像是最流行的多媒体形式之一，在政治、经济、国防、教育等方面均有广泛应用。对于某些特殊领域，如军事、商业和医疗，数字图像还有较高的保密要求。

为了实现数字图像保密，实际操作中一般先将二维图像转换成一维数据，再采用传统加密算法进行加密。与普通的文本信息不同，图像和视频具有时间性、空间性、视觉可感知性，还可进行有损压缩，这些特性使得为图像设计更加高效、安全的加密算法成为可能。

混沌图像加密，是图像加密技术中较为简单的一种。其中典型的方法是Logistic混沌序列加密。

学习混沌图像加密的原理，编程实现Logistic混沌序列加密，能够对输入的数字图像进行加密，实现环境和编程语言不限。