实验一随机全排列生成程序及其应用开发

一、实验目的

该实验为设计性实验。通过本实验，使学生掌握一种以上产生今后在密码学中经常用到的随机全排列（可用以作为“代替表”或“置换”）的方法，并引导学生充分发挥想象和创造力、开发出它的更多的应用情形。

二、实验内容

1. 编制生成 0~n（n≤255）的一个全排列的程序，可选择下列两个方法之一或

自行设计另外方法：

方法 1：从一个随机文件读取 n+1 字节数据 d0, d1, dn。由预先取定的一个 0~n 的全排列 P（比如，可为 0~n 的自然排列）开始，依次对 i=n, n-1,1，计算：j=di-1+di (mod i)交换 P 的第 i 项第 j 项（在此注意我们假定 P 从第 0 项开始）。

方法 2：用一个随机函数产生 m（m>n）字节数据 d1, d2,dm。d1(mod对(n+1)), d2(mod (n+1)),dm(mod (n+1))依次考察，把后面出现的与前相同者去掉；在最后剩下的数据中，把没有出现的 0~n 依序补写于后面。

2. 对第一步生成随机全排列的程序，自己设计一种应用并予以实现。

三、实验要求

1. 程序须对不超过 255 的正整数 n 都容易生成 0~n 的一个全排列；

2. 对较小的 n，抓图显示随机全排列生成程序的计算结果（附页），数据不能出现明显错误；

3. 每位同学设计的“一种对于随机全排列生成程序的应用”须有个性化特点、不与别人雷同。

四、实验原理（提示）

（一）关于“随机全排列生成程序”应用的设计

“一个 0~n 随机全排列”中的随机性是指：某种相应的生成方法可以做到“让0~n 中任意数等可能地出现在任一位置”。生活中应用“一个 0~n 随机全排列”的例子随处可见，比如“编排考试等一个场所中的随机座位号”“模拟抽取某种福，利或体育彩票中的一组中奖号码”“模拟分发固定人数参与游戏的一付扑克牌”等等。要求每位学生把自己的这部分设计完完整整地写清楚，包括介绍你所设想的具体应用场合、这种应用遵循的原则或规则、如何进行相应模拟计算（给出实例）等。

（二）主要参考程序

……

五、思考题

“生成一个 0~n 随机全排列”是否同于“生成一组 0~n 中随机数”？

题目，涉及到书上什么内容，测试数据和测试结果，结果简单分析，思考题