

“众妙之门” ——数学原理在电子门禁系统上的应用

谭知微 曾学为 / 澳门特别行政区培正中学
指导教师 王灿霖

◎ 概述

➤ 摘要

本项目主要是初等数学原理在电子密码锁上应用的研究，利用“3个不同点确定唯一的一元二次函数”这一数学原理，来设计电子门禁装置，使得至少3位有效密码持有者同时在场才可开启门禁电子锁。同时，应用数论中的算术基本定理——每个大于1的正整数都可以唯一地表示成质数的乘积——来管理使用者的开门权限。实践方面，我们使用 Visual Basic 来编写该系统的软件部分，并利用“USB 多功能 I/O 开发板”、“S70 射频卡”和自制电子门实现硬件部分。当门禁系统通过 USB 接口同时读取3张不同的有效射频卡时，电子门方可自动打开。所谓三人为众，再加上本原理巧妙地利用了一些数学原理，所以我们引用老子的《道德经》中的“众妙之门”来命名该门禁装置。

➤ 问题提出

学期开学之初，老师告诉我们，为了更好地利用数学实验室，所以希望每次进入数学实验室的同学至少3位或更多。鉴于传统门禁锁的使用难以满足至少3人才可进入实验室的条件，而且每个学期又都要有新的同学进入实验室，电子密码也需要不断更新……所以我们便有了设计一个专门的门禁装置的想法。

➤ 研究假设

可不可以利用所学的数学知识来设计满足老师要求的密码锁呢？如果可以，那么它要具有以下功能：

- ◆ 门禁系统要具备管理弹性，

因为每个学期数学班同学的人数和人员组成都不一样；

- ◆ 任意3位持有有效密码的数学班的同学同时在场，均可以打开该门禁系统；
- ◆ 密码应当不容易破解又可以在每个学期支持更新；
- ◆ 门禁系统的使用过程中，不需要修改内置程序。

◎ 密码原理

➤ 密码的产生

密码由管理班级的老师制作并派发。老师首先在心中想定一个形如

表 1

学号 x	$y=f(x)$	密码		学号 x	$y=f(x)$	密码
001	003	001003		007	063	007063
002	008	002008		008	080	008080
003	015	003015		009	099	009099
004	024	004024		010	120	010120
005	035	005035		011	143	011143
006	048	006048		012	168	012168



图1 射频卡及读写机
左上方的是射频卡读写机，学生可以利用读写机将射频卡上的资料读进系统内。

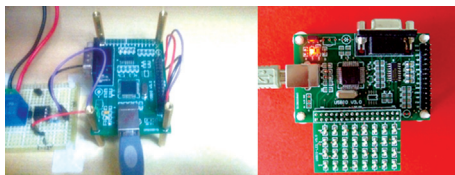


图2 I/O（输入/输出）开发板
中间绿色的是 USB I/O（输入/输出）开发板，当接到系统确认 3 个有效密码的信号后，开发板激活继电器使电磁铁通电。

$f(x)=Ax^2+Bx$ 的二次函数式， A 与 B 两个系数由老师选定。例如令 $A=1$ ， $B=2$ 。每个学生各派发给一个密码。为方便阐明原理，我们令密码由 2 组数字（每组 3 位）组成，第一组数字是他在数学班的学号并记为 x ，第 2 组数字就是 $f(x)$ 并记为 y 。设一班有 12 人，则学号（密码前 3 位）就是 001 至 012，后 3 位也易算得。12 位同学使用的最终密码如表 1。

密码锁的使用

假如学号是 001、002 及 003 共 3 位同学要进入数学实验室，则当 2 位同学正确地输入他们的密码后，密码锁就能求出老师用来产生密码的系数 A 和 B 。假如 002 及 003 两位同学输入密码后，密码锁就知道老师想定的二次函数经过 $(0, 0)$ 、 $(2, 8)$ 和 $(3, 15)$ 3 点，因而这个二次函数是唯一的。解方程组

$$4A+2B=8$$

$$9A+3B=15$$

就可求出 A 和 B 的值即是 1 和 2。

所以

$$f(x) = x^2 + 2x$$

最后 001 同学输入他的密码，密码锁就利用所求得的二次函数验证所输入密码是否由该函数产生。如果是，就开锁；否则，保持上锁状态。如果 002 及 003 同学输入错误的密码，解出来的 A

和 B 就不会是 1 和 2。所以当 001 同学输入他的密码后，当系统检测到此密码并不是由它求得的函数产生时，密码锁也会保持上锁状态。

这个锁有一个很大的优点，就是 A 和 B 不会留在锁上，这使得它十分安全。等到下学时，老师就可以更新 A 和 B ，大家开始使用新的密码。而密码锁内的程序设置，一点都不必改变或更新。

实际操作中，计算机无须每次都解方程，而是利用拉格朗日函数的特点直接算出 A 和 B 。

系统权限管理

在权限管理方面，我们应用了算术基本定理，它又称为质数的唯一分解定理，即：

每个大于 1 的自然数均可写为质数因子的积，而且这些质因子按大小排列之后，写法仅有一种方式。

于是系统将第 i 个学号对应为第 i 个质数来存储，即序号为 004 和 005 的同学对应第 4 和第 5 个质数 7 和 11。当管理老师要禁止这 2 位同学进入实验室时，门禁系统会存储 7 和 11 的乘积（77），若 77 可以被学号对应的质数整除时，则系统不接受开门请求。

系统功能实现

硬件部分

电子门禁系统使用 Visual Basic 来编写该系统的应用程序的主要功能，而此程序由一台笔记本电脑执行。该电脑的一个 USB 接口连接射频卡的读写机（见图 1），而另一 USB 接口连接一个多功能 I/O（输入/输出）开发板（见图 2）。开发板接收到控制电脑传来的开门信号后，电磁铁通电后吸起门闩，就可以开门。

软件部分

系统的应用程序是在 Windows XP 环境下执行，主要分为卡片注册、卡片管理和卡片读取等 3 个功能。管理操作界面如图 3 所示。

◆ 卡片注册。模块主要依据密码设计原理，由老师自定 KEY A 和 KEY B 来生成注册学生的注册密码，并输入注册学生的组号、组别和设定的有效期限。然后系统利用读写机将密码及其他资料写在该生的射频卡上，其功能的操作界面如图 4 所示。

◆ 其中 Channel 及 Baud 都是连接读写机的 USB 设定，每部电脑都可能不一样，要正确填写，读写机才可正常工作。而 Card ID 代表卡片的唯一序号。管理老师可以在该界面的密码参数设定区域输入有效期限和所设定的一元二次函数



图3 系统操作主界面



图4 注册界面



图5 密码读取



图6 权限管理

的系数A (KEY A)和B (KEY B)的值,然后点击“生成密码”键生成该卡的密码,然后点击“写入密码”将所生成的密码写入对应的卡片。这个界面还同时提供“回首页”按键,以供管理老师返回首页进行相应操作。

◆ 卡片读取。当3个或3个以上的学生请求进入实验室时,可以通过读卡功能将所持有的密码卡储存的密码提供给门禁系统,由门禁系统根据所读入的密码的正误情况选择打开和继续保持锁定。具体操作如下:

第1步:读入前两位学生的密码。

第2步:应用拉格朗日函数计算出注册生成这2个密码的二次函数系数的A和B的值,从而得到该一元二次函数。

第3步:读入第3位同学的密码,满足第2步所得到的函数则打

开门禁;否则,保持锁定,并将储存的函数清除,并返回第1步。

第4步:结束。

具体操作界面如图5所示。

◆ 卡片管理。管理老师可利用此功能以通过整组或单个组员进行权限管理。权限管理具有两个功能:删除权限和恢复权限,如图6所示。当管理老师要对整组成员进行管理时,只需将该组组号输入对话框内,即可进行删除和恢复权限的操作。同理,需要对单个组员进行管理时,可以在对话框内输入该成员的组号和卡号,即可进行删除和恢复权限的操作。

◎ 结论

此项目原理设计简单,性能安全,管理富有弹性,同时便于实践。稍加改动便可扩展到N人开门系统。与此同时,此原理的应用可以延伸至系统备份、计算机安全和审核认证等研究领域。在日

常的学习中,只要我们多吸收、多观察、多思考,很多知识就都可以应用在我们的生活中。在这里用到的二次函数性质和方法,想来在其他领域,如计算机安全上一定也会很有用。

该项目获得第26届全国青少年科技创新大赛创新成果竞赛项目中学组数学一等奖。

专家评语

本项目巧妙地利用“一元二次函数曲线被三个点所决定”的原理,设计了一种持有密码的人群中三个人输入密码才能打开的密码锁。选题新颖、恰当,是一项优秀的初中生科研实践。■