高等学校自动识别技术系列教材

应用密码学基础

李益发 赵亚群 张习勇 张铎／编著

AUTOMATIC
IDENTIFY
TECHNOLOGY

WUHAN UNIVERSITY PRESS
武汉大学出版社

北京华信恒远信息技术研究院 策划
高等学校自动识别技术系列教材

应用密码学基础

李益发 赵亚群 张习勇 张铎 / 编著

WUHAN UNIVERSITY PRESS
武汉大学出版社

图书在版编目(CIP)数据

应用密码学基础/李益发,赵亚群,张习勇,张铎编著. —武汉:武汉大学出版社,2009.11
高等学校自动识别技术系列教材
ISBN 978-7-307-07321-0

Ⅰ.应… Ⅱ.①李… ②赵… ③张… ④张… Ⅲ.密码—理论—高等学校—教材 Ⅳ.TN918.1

中国版本图书馆 CIP 数据核字(2009)第 163328 号

责任编辑:黄汉平　　责任校对:刘　欣　　版式设计:詹锦玲

出版发行:**武汉大学出版社**　(430072　武昌　珞珈山)
(电子邮件:cbs22@whu.edu.cn　网址:www.wdp.com.cn)
印刷:武汉中远印务有限公司
开本:720×1000　1/16　印张:20.5　字数:355 千字　插页:1
版次:2009 年 11 月第 1 版　2009 年 11 月第 1 次印刷
ISBN 978-7-307-07321-0/TN·39　定价:32.00 元

内容简介

本书简要介绍了密码学基础理论和基本技术，内容分为三个部分：基础的密码算法、基本的应用技术和必要的数学基础知识。密码算法部分包括：对称分组密码算法、非对称密码算法、散列算法和数字签名算法；基本应用技术包括：密钥管理的基本技术、基本认证技术和在防伪识别中的简单应用技术；数学基础知识部分包括：初等数论、代数学基础、有限域和椭圆曲线基础、计算复杂性理论基础。

本书不同于其他密码学教材之处有二：一是包含了较多的密钥管理和认证技术，二是包含了密码学在自动识别中的保密和防伪应用。本书可供自动识别技术专业的专科生、本科生作为密码学的教材使用，也可供计算机专业的专科生和本科生作为了解密码学的参考资料。

丛书序言

今天，随着国民经济和科学技术的快速发展，条码已经成为全球通用的商务语言，无线射频技术正在应用于铁路、物流、邮政、公共安全、资产管理、物品追踪与定位等多个领域，以指纹识别技术为代表的生物识别技术开始在金融、公共安全等领域得到逐步推广，这一切都预示着自动识别技术的应用将大大促进我国各领域信息化水平的进一步提高。

20世纪80年代末期，条码技术开始在我国得到普及和推广。作为一种数据采集的标准化手段，通过对供应链中的制造商、批发商、分销商、零售商的信息进行统一编码和标识，为实现全球贸易及电子商务、现代物流、产品质量追溯等起到了重要作用。随着2003年中国“条码推进工程计划纲要”的提出和实施，条码技术已经开始涉及国民经济的各个领域。

二十多年后的今天，以条码技术、射频识别技术、生物特征识别技术为主要代表的自动识别技术，在与计算机技术、通信技术、光电技术、互联网技术等高新技术集成的基础上，已经发展成为21世纪提高我国信息化建设水平，促进国际贸易流通，推进国民经济效益增长，改变人们生活品质，提高人们工作效率，获得舒适便利服务的有利工具和手段。

为推动中国自动识别技术产业的持续性发展，培养和造就服务于自动识别产业和相关产业的专业人才，中国自动识别技术协会作为国家级的行业组织，经过充分的市场调研和反复的需求论证，从2006年夏季开始，在国内部分高等院校推动自动识别技术专业方向的学历教育。这是国内首次将自动识别技术教育以专业教育的形

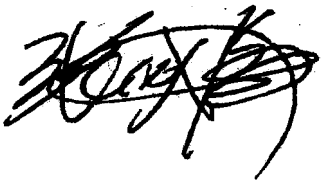
式引入高等学历教育领域的尝试和突破。

为配合自动识别专业人才的培养教育，中国自动识别技术协会组织有关专家、学者、高级工程技术人员，共同设计了国内第一套自动识别技术教育大纲，并组织撰写了与之配套的自动识别技术高等学历教育教材，以满足教学需要。

全套教材将涉及自动识别技术导论、条码技术、射频识别技术、生物识别技术、电子数据交换技术与规范、图像处理与识别技术、密码原理、自动识别产品设计等内容，从2007年5月起陆续分册出版发行。

技术的发展没有止境，知识的进步没有边际。在我们试图总结自动识别产业专家学者和技术人员的知识和经验时，我们也意识到这套教材只是我们的初次探索，是推动中国自动识别产业人才战略的第一步。我们希望这套教材能够为广大学子奠定行业知识的基础，真心祝愿学子们成为自动识别产业坚实的后备力量。

最后，真诚欢迎国内外各界人士和自动识别产业界的朋友对全套教材提出批评和指正。



2007年1月

前　言

本书是在中国自动识别技术协会的组织下，为适应自动识别技术专业的教学需要编写的密码学基础教材。

自动识别这个名词可能不一定为大家所熟悉，但其产品及应用绝对称得上是家喻户晓。如果你跟一个家庭主妇打听自动识别，她可能根本不知道你在说什么，但几乎每个家庭主妇对日用品上的一维条码都不陌生。我们都会记得，在商店购买商品的过程中，营业员用条码扫描器扫描每一件商品上的一维条码，然后打印出清单付费。条码作为自动识别的主要应用之一，随处可见。当然，信用卡上的磁条、手机里的 SIM 卡、打开保险柜的指纹、高速公路收费口的远距离射频卡等，这些都是我们能够亲身接触到的自动识别。

随着社会自动化和信息化程度越来越高，对自动识别的要求也越来越多，特别是对识别标签提出了保密和防伪的功能要求。这使得密码学与自动识别产生了联系，成为保密与防伪识别的理论和技术基础，也成为自动识别专业的一门必修课程。

自动识别中的保密和防伪，从密码学的角度看，就是保密与认证。换言之，就是将密码学中的保密与认证技术用于自动识别。保密自然要用到加、解密算法，而认证更是一项复杂的技术，需要用到许多密码学的基础知识——密码体制、单向函数、数字签名等。因此，即使是为了弄清认证在自动识别中的一个小小应用，也不得不较为系统地介绍密码学的许多基础理论和基本技术。

根据自动识别技术专业教学计划的要求，本书意在面向防伪识别的需要，写成适合自动识别专业本、专科生学习密码学的入门教材。因此在内容选择上，侧重介绍基本概念、基本算法、基本技术，

力求使读者通过本书快速了解基本的密码学知识及其在防伪识别中的简单应用。

本书的内容分为三个部分：基础的密码算法、基本的应用技术和必要的数学基础知识。

密码算法部分包括：对称分组密码算法、非对称密码算法、散列算法和数字签名算法。在每种算法中，我们只介绍了最基本的几个，例如对称分组算法只介绍了 DES 和 AES；非对称算法只介绍了 RSA、ElGamal、ECC 和 IBC，并且 ECC 和 IBC 还作为选修内容；Hash 函数只介绍了 MD5 和 SHA-1；数字签名算法主要介绍了几个基本的签名方案，特殊签名只介绍了盲签名，并且也是作为选修内容。之所以要介绍盲签名，一则是想展示一下如何构造针对特殊需要的签名方案，二是作者觉得特殊签名特别是盲签名也有可能用于防伪识别。

基本应用技术包括：密钥管理的基本技术、基本认证技术和在防伪识别中的简单应用技术。密钥管理是算法走向应用的基础，面向应用，这部分内容是不可缺少的。防伪主要是通过认证实现的，因此认证技术是本书的核心内容。但认证技术是灵活的，实际上可根据环境及需求来定制。因此，我们给出的认证方案主要是介绍认证的基本思想和手段，只具有参考性，不能作为认证的标准。

数学基础知识部分包括：初等数论、代数学基础、有限域和椭圆曲线基础、计算复杂性理论基础。这部分内容本是密码学的理论基础，但我们把它放在最后，因为不清楚读者在使用本教材之前具备哪些数学基础。这要求老师在授课时，要根据学生的具体情况对这部分教学内容及教学时机有所选择。

本书既然针对防伪识别的需要而编著，则命名为“防伪识别的密码学基础”似乎更为贴切。但一则书名早就与出版社商定，涉及出版社的出版计划与新书预告，不便更改；二则从内容上看，主要介绍的仍是应用密码学的基础知识，可供读者作为了解应用密码学的入门教材，因此仍使用原定的书名。当然，在介绍具体应用时，由于删去了密码学在网络安全、电子商务、电子政务等方面的许多应用，只保留了在防伪识别方面的应用，虽说可能更为适合自动识别专

业，但在“应用”上难免显得单薄，颇有些顾此失彼，望读者见谅。

密码学以数论、代数学、椭圆曲线、计算复杂性理论等许多深奥的数学理论为基础，这使得密码学的学习对许多非数学专业的学生来说都比较困难。建议读者先不要深究数学本身，而是承认那些要用到的数学结论，重点了解结论的含义，并关注这些结论在密码学中的应用。这样可能使学习变得轻松一些。对于许多复杂的密码算法，如果一下子不容易弄明白算法的细节，建议先忽略它，重点关注算法的基本特性，以及如何应用算法实现保密和认证。

本书第11章由赵亚群教授编写，3.4节与13.2节关于椭圆曲线的部分由张习勇副教授编写，第10章防伪应用部分由北京华信恒远信息技术研究院张铎院长参与编写。张铎院长还对全书的内容选择提出了许多建设性意见。其他部分由李益发编写，并做最后统稿。

韩文报教授、范淑琴教授、王政博士等共同审阅了全书。赵远、马宇驰、元彦斌、邓帆、邓少锋等几位硕士研究生也参与了部分内容的录入和校对。作者对他们的辛勤付出表示衷心的感谢！

作者能写作此书，得益于沈世镔先生的大力推荐。武汉大学出版社任翔副编审为本书的出版耗费了大量心血，北京华信恒远信息技术研究院的邵慧欣女士也为本书的出版多方联系。作者谨致以诚挚的谢意！

此书在写作过程中，还得到了信息工程大学信息工程学院信息研究系领导李华政委、索敏杰主任、国立杰副主任，以及信息研究系密码理论教研室戚文峰主任和陈卫红副主任的热忱关心和大力支持。此外，邓依群副教授、夏英华副教授和毛艳教员也给予了极大的帮助。在此一并致以深深的谢意！

限于水平，错漏之处在所难免，敬请读者批评指正。

作　者

2009年7月27日

目　录