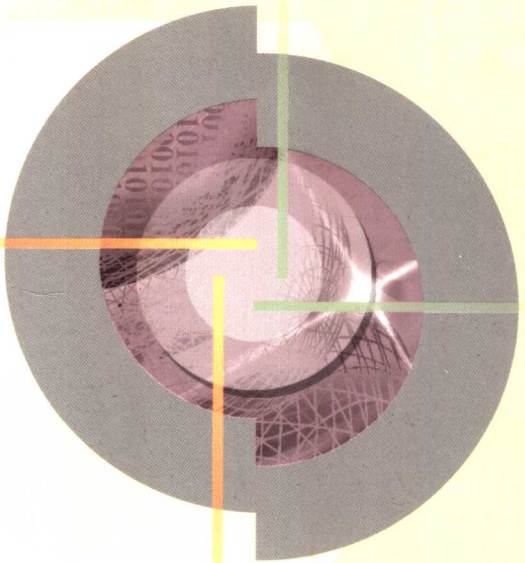
普通高等教育“十五”国家级规划教材

信息安全专业系列教材

现代密码学基础

XIANDAI MIMAXUE JICHU



章照止 主编

北京邮电大学出版社
www.buptpress.com

普通高等教育“十五”国家级规划教材

现代密码学基础

章照止　主编

北京邮电大学出版社
·北京·

内 容 简 介

本书全面深入地介绍了现代密码学的基础理论。全书共分 15 章和 1 个附录。内容包括密码学研究的基本问题、古典密码学、密码学的信息论基础和计算复杂性理论基础、单向函数和伪随机序列生成器的严格理论、序列密码、分组密码和公钥密码、数字签名、杂凑函数、身份识别、认证码、密钥管理和零知识证明,附录的内容包括本书用到的代数学和初等数论方面的基础知识,每章还包括注记和习题。本书注意了严格理论和直观描述的配合,在介绍经典密码体制的同时,注意从中总结出一般的原则和方法及基本工具,并注重介绍一些新的密码体制。

本书是为信息安全专业编写的专业基础课教材,适用于高等院校信息安全本科专业的学生以及计算机应用、信息工程、应用数学等相关本科专业的学生,同时也可供从事信息安全工作的科技人员以及相关专业的研究生参考。

图书在版编目(CIP)数据

现代密码学基础/章照止主编. —北京:北京邮电大学出版社,2004
ISBN 7-5635-0651-9

Ⅰ.现… Ⅱ.章… 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(2004)第 014350 号

书　　名:现代密码学基础
主　　编:章照止
责任编辑:王琴秋
出版发行:北京邮电大学出版社
社　　址:北京市海淀区西土城路 10 号(邮编:100876)
电话传真:010-62282185(发行部) 010-62283578(FAX)
电子信箱:publish@bupt.edu.cn
经　　销:各地新华书店
印　　刷:北京皇家印刷厂
开　　本:787 mm×1 092 mm 1/16
印　　张:18.5
字　　数:401 千字
印　　数:1—5 000 册
版　　次:2004 年 4 月第 1 版 2004 年 4 月第 1 次印刷

ISBN 7-5635-0651-9/TP·83　　定　价:29.00 元

信息安全专业系列教材

编　委　会

总　序

办好信息安全本科专业的第一要素是拥有高质量的教材。由于各方面的原因，我国开办信息安全本科专业的历史很短，刚刚起步，但是，当前以各种形式开办信息安全本科专业的高等院校却非常多，学生总数也相当可观，而且其中大部分学生已经学完基础课程，即将进入专业课的学习阶段。

与信息安全本科专业招生的火爆场面形成鲜明对比的是，到目前为止，我国还没有一套自己的信息安全本科专业系列教材。为了保证信息安全本科专业学生的培养质量，2001 年，北京市教委以“精品教材立项”的形式委托我们北京邮电大学信息安全中心负责编写《现代密码学基础》、《信息安全概论》、《网络安全》、《信息隐藏与数字水印》、《入侵检测》、《计算机病毒原理及防治》等 6 本教材，随后，教育部又将此套系列教材列入了“普通高等教育‘十五’国家级教材规划”。由此可见，此套教材的编写确实受到了各级教育主管部门的高度重视。

北京邮电大学信息安全中心是一专门从事信息安全的教学、科研和成果转化的重点实验室。该实验室已经培养出了我国第一位密码学博士，而且在“信息安全”和“密码学”两个专业领域内健全了博士后、博士、硕士和本科的培养教育体系，已经培养出了数以百计的信息安全研究生。

在接受了北京市教委和教育部的编写信息安全本科系列教材的任务之后，我们立即组织了最强的师资队伍投入到教材的编写工作之中。经过两年多的不懈努力，数易其稿，反复研讨，按照教育目标和大学生基本素质培养的要求，本着推进理工融合及学科交叉的思想，经过优化课程体系和精选课程内容，我们终于完成了信息安全本科专业系列教材的第一批教材（共 6 本）。现在我们正在着手规划信息安全本科专业的第二批教材，它们的暂定名分别是《安全操作系统》、《安全数据库》、《安全访问控制》、《安全检测与监控》、《数字证书与管理》、《安全备份与灾难恢复》、《安全隔离技术》、《安全服务技术》、《安

全系统工程》、《安全规范与标准》等。我们诚意邀请国内所有高等院校的权威安全专家加入第二批教材的编写工作(有意者请与我们直接联系。地址:100876,北京邮电大学信息安全中心126信箱)。我们希望这套信息安全本科专业系列教材最终完成之后能够基本满足国内各类高校信息安全本科专业的普遍需求。

虽然我们的目标是编写一套适合信息安全专业本科生使用的精品教材,但是,由于水平有限,时间仓促,且信息安全本科专业刚刚开始,我们还没有足够的实践机会,不足之处和错误在所难免,恳请读者和同行专家多提意见,以便我们再版时充分修改,不断完善。

衷心感谢北京邮电大学胡正名教授对本套教材的大力支持,感谢北京邮电大学信息安全中心二百余位成员的支持与配合。本套教材也是国家自然科学基金项目(90204017, 60372094, 60373059)和国家"973"项目(G1999035804)资助的成果,在此一并表示感谢。

杨义先 教授、博士生导师、全国政协委员
2004年1月于北京邮电大学信息安全中心

前　言

本书是为信息安全专业编写的专业基础课教材，其选材及内容的组织安排是在参考了国内外已出版的若干同类教材的基础上，根据现代密码学的特点以及对信息安全专业学生的培养目标确定的。编入本教材的内容都是相对成熟的、公认的理论与方法。与国内已出版的这类教材相比，本教材还具有以下一些特点：

(1) 由于密码学是在密码设计者和密码分析者之间的不断斗争中发展起来的。密码分析方法的奏效将促使密码设计方法的改进，这又迫使密码分析者研究新的分析方法。因此设计一个密码体制不仅要考虑已知的分析方法，而且要考虑密码体制设计出来后可能出现的新的分析方法。故密码体制的安全性必须建立在严格的理论基础上，单凭直观和显然是不行的。为了培养学生掌握严格的信息安全理论基础，本书对现代密码学的基础——计算复杂性理论——作了比较深入的介绍，并介绍了现代密码学的源头概念——单向函数——的严格定义。本书还介绍了基于计算复杂性理论的伪随机序列生成器的严格理论，应用这种生成器输出的伪随机序列作密钥所设计的密码系统，其安全性在理论上是可证明的。关于密码学协议的主要工具——Hash 函数和零知识证明系统——的介绍，本书采用严格和直观相配合的方法，使学生更易理解和掌握。

(2) 为了培养学生的灵活思维方法，并具有一定的研究、开发和创新能力。本书的某些较难的章节可以作为选学内容，某些定理被略去的证明可以让学生自己补上。本书在各章的注记中还提供了补充阅读的文献，可以作为学生的自学内容，以扩大知识面。本书每章还提供了一些习题，其中有一些较容易的旨在巩固学习内容或锻炼计算能力的题，也有一些较难的旨在培养研究和创新能力的题。

(3) 为了适应通信技术和计算技术迅速发展对密码学提出的新的要求，本书在介绍经典的密码体制时，注意了从中总结出一般的原则和方法以及基本工具，并注重介绍一些新提出的密码体制，如 AES。

量子密码是一个新方向，但这方面的技术还处于实验室阶段，要达到应用还有较长时间，因此本书不介绍量子密码学的内容。本书参考文献[33]6.3节对量子密码学作了简短介绍，想了解此方面内容的读者可参看该文献及其所引文献。

密码学要用到的数学知识很多，特别是概率论、代数学和数论方面的基础知识。学习本书要求学生具有一定的概率论基础知识。本书附录简要地介绍了书中用到的有关代数学和初等数论方面的基础知识，其他数学知识(如纠错码、素性检验、椭圆曲线、图论等)只能在有关章节中作简短的介绍和说明。学习一些这方面的数学知识对学习本书是有帮助的；但是，没有学过这些数学知识也不会使本书的学习受到影响。

本书共分15章和一个附录。第1～4章介绍密码学的基础知识，主要包括密码学研究的基本问题、古典密码学、密码学的信息论基础和计算复杂性理论基础；第5,6,11和15章介绍设计密码体制和安全协议的主要工具，包括单向函数和伪随机序列生成器、杂凑(Hash)函数和零知识证明；第7～9章介绍各类密码体制及其攻击(分析)方法，包括序列(流)密码、分组密码和公钥密码；第10,12和13章分别介绍了数字签名、身份识别、认证码；第14章介绍了密钥管理；附录中介绍了代数和数论的若干基础知识。

目前，密码学教材和文献中所用的术语和符号还很不统一，本书各章之间所引用的术语和符号也没有完全统一。为了避免混淆，必要时通过在括号中对术语加注英语符号加以说明。此外，本书未列出所有参考文献，只在书的最后列出了本书各章所用的主要参考文献。

本书的编写工作由杨义先和温巧燕负责组织，由温巧燕草拟了本书的编写原则和章节目录。章照止编写了书稿的第1,4,5,6,11,13和15章，周世祥编写了书稿的第2,3,12和14章以及附录，并对温巧燕准备的书稿第7,8两章的素材进行了整理和补充，邓玉峰根据徐国爱的意见编写了书稿的第9,10两章，章照止对全书作了一些必要的修改。此外，周世祥和邓玉峰还在本书的电子版及书稿打印方面做了许多工作；张龙在校对书稿等方面做了许多工作；张劼帮助作者回答了书稿中的一个疑问。作者对他们表示衷心的感谢。

作　者

2004年1月

目　录

第 1 章　引 论

1.1　密码学研究的基本问题 …… 1
1.1.1　密码体制 …… 1
1.1.2　单向函数与伪随机序列生成器 …… 3
1.1.3　数字签名与杂凑(Hash)函数 …… 3
1.1.4　消息认证和身份识别 …… 4
1.1.5　抗欺骗协议和零知识证明 …… 5
1.2　密码学的广泛应用 …… 6
1.3　本书选材的组织与安排 …… 7
习题一 …… 8

第 2 章　古典密码学

2.1　古典密码体制 …… 9
2.1.1　定义和分类 …… 9
2.1.2　代换密码(Substitution Cipher) …… 11
2.1.3　置换密码(Permutation Cipher) …… 17
2.2　古典密码体制分析 …… 18
2.2.1　单表代换密码分析 …… 20
2.2.2　多表代换密码分析 …… 20
2.2.3　对 Hill 密码的已知明文分析 …… 26
习题二 …… 27

第 3 章　密码学的信息论基础

3.1　保密系统的数学模型 …… 29
3.2　信息量和熵 …… 31
3.3　完善保密性 …… 34
3.4　理论安全性和实际安全性 …… 36

习题三 …… 40

第 4 章　密码学的计算复杂性理论基础

4.1　问题与算法的复杂性…… 42
4.1.1　问题与语言…… 42
4.1.2　算法与图灵机…… 44
4.2　问题的计算复杂性分类…… 47
4.2.1　P、NP、NP 完全类问题 …… 47
4.2.2　概率算法与 BPP 类问题 …… 49
习题四 …… 51

第 5 章　单向函数

5.1　一般单向函数…… 53
5.1.1　单向函数的定义…… 53
5.1.2　候选单向函数…… 55
5.2　单向函数族…… 56
5.2.1　单向函数族的定义…… 56
5.2.2　候选单向函数族…… 57
5.3　单向函数族的其他性质…… 59
5.3.1　单向陷门置换族…… 59
5.3.2　单向无爪函数族…… 59
5.4　单向函数的硬核…… 60
5.4.1　单向函数的硬核谓词…… 61
5.4.2　单向函数的硬核函数…… 62
习题五 …… 63

第 6 章　伪随机序列生成器

6.1　计算不可区分性…… 65
6.2　伪随机序列生成器的定义和性质…… 67
6.3　伪随机序列生成器的构造…… 69
6.3.1　用一般单向置换构造伪随机序列生成器…… 69
6.3.2　用单向置换族构造伪随机序列生成器…… 69
6.4　用伪随机序列生成器构造伪随机函数…… 71
6.5　伪随机置换的构造…… 72
习题六 …… 74

第7章 序列密码

7.1 布尔函数…… 75
7.1.1 布尔函数的表示…… 76
7.1.2 布尔函数的非线性…… 78
7.1.3 布尔函数的相关免疫性…… 79
7.1.4 布尔函数不同性质之间的关系…… 79
7.1.5 多输出布尔函数…… 79
7.2 序列密码的原理…… 81
7.3 序列的伪随机性…… 82
7.4 序列密码对密钥流的要求…… 83
7.5 密钥流生成器…… 84
7.6 线性移位寄存器…… 85
7.7 非线性序列…… 91
7.7.1 非线性移位寄存器序列…… 91
7.7.2 非线性前馈序列…… 92
7.7.3 非线性组合序列…… 93
7.8 序列密码分析…… 94
7.8.1 二元加法非线性组合流密码的相关攻击…… 94
7.8.2 二元加法非线性组合流密码的线性逼近攻击…… 96
习题七 …… 99

第8章 分组密码

8.1 分组密码概述 …… 100
8.2 分组密码的设计原则 …… 101
8.3 分组密码的结构 …… 102
8.4 分组密码的安全性 …… 103
8.4.1 安全需求 …… 104
8.4.2 安全模型 …… 104
8.4.3 分组密码作为一个伪随机置换 …… 105
8.4.4 攻击的分类 …… 106
8.5 典型的分组密码算法——DES …… 106
8.5.1 算法描述 …… 107
8.5.2 DES的设计思想和特点 …… 113
8.5.3 DES的工作模式(对其他分组密码也适用) …… 114

8.5.4 DES的实现 …… 117
8.5.5 DES的安全性 …… 117
8.6 典型的分组密码的分析方法 …… 119
8.6.1 差分分析法 …… 119
8.6.2 线性密码分析 …… 126
8.7 美国高级数据加密标准——AES …… 129
8.7.1 AES的评估准则 …… 130
8.7.2 高级加密标准算法AES——Rijndael …… 131
8.8 欧洲21世纪数据加密标准 …… 136
8.8.1 NESSIE建议 …… 138
8.8.2 Camellia算法简介 …… 138
8.9 其他分组密码算法综述 …… 144
8.9.1 IDEA算法 …… 144
8.9.2 RC6算法 …… 147
习题八 …… 150

第9章 公钥密码学

9.1 公钥密码学思想 …… 152
9.2 RSA公钥密码体制 …… 154
9.2.1 RSA体制 …… 154
9.2.2 RSA的参数选择 …… 154
9.2.3 概率素性检测 …… 156
9.2.4 RSA的攻击 …… 159
9.3 ELGamal公钥密码体制和离散对数问题 …… 160
9.4 基于纠错码的公钥密码体制 …… 162
9.5 椭圆曲线公钥体制 …… 166
9.5.1 椭圆曲线 …… 166
9.5.2 椭圆曲线密码体制 …… 167
9.6 其他公开密钥密码体制 …… 168
9.6.1 Goldwasser-Micali概率公开密钥密码系统 …… 168
9.6.2 Merkle-Hellman背包公钥密码体制 …… 170
9.6.3 有限自动机公开密钥密码体制 …… 171
习题九 …… 171

第 10 章 数字签名

10.1 基于 RSA 和离散对数的签名体制 …… 174
10.1.1 RSA 签名方案 …… 174
10.1.2 ELGamal 签名方案及其一般化的模型 …… 175
10.1.3 DSS …… 177
10.1.4 Lamport 签名方案 …… 179
10.1.5 不可否认签名方案 …… 179
10.1.6 故障停止式签名方案 …… 181
10.1.7 Schnorr 数字签名方案 …… 183
10.2 群签名 …… 184
10.3 多重数字签名方案 …… 185
10.4 代理数字签名体制 …… 188
10.5 基于纠错码的数字签名体制 …… 190
10.6 批验证协议 …… 193
习题十 …… 194

第 11 章 杂凑(Hash)函数

11.1 杂凑函数的定义 …… 195
11.2 无碰撞杂凑函数的构造方法 …… 198
11.2.1 用单向压缩函数构造无碰撞杂凑函数的一般方法 …… 198
11.2.2 用分组加密函数构造杂凑函数 …… 199
11.2.3 用候选单向函数构造杂凑函数 …… 200
11.2.4 软件杂凑算法 MD4 和 MD5 …… 201
11.2.5 安全 Hash 标准(SHS) …… 204
11.3 杂凑函数的攻击方法与安全性 …… 204
11.3.1 生日攻击 …… 204
11.3.2 特殊攻击 …… 206
11.4 时戳 …… 207
习题十一 …… 208

第 12 章 身份识别方案

12.1 Schnorr 身份识别方案 …… 210
12.2 Okamoto 身份识别方案 …… 212
12.3 Guillou-Quisquater 身份识别方案 …… 213

12.4 基于身份的身份识别方案…… 214
12.4.1 Shamir 的基于身份的密码方案的基本思想 …… 214
12.4.2 Guillou-Quisquater 的基于身份的识别协议…… 216
12.5 转换身份识别为签名方案…… 217
习题十二…… 218

第 13 章 认证码

13.1 认证理论与认证码…… 219
13.2 计算欺骗概率…… 220
13.3 组合界…… 222
13.4 用正交矩阵构造认证码…… 223
习题十三…… 225

第 14 章 密钥管理

14.1 密钥管理概述…… 227
14.2 密钥分配协议…… 230
14.3 密钥共享…… 236
14.4 密钥托管…… 240
14.4.1 密钥托管体制的基本组成…… 241
14.4.2 密钥托管体制实例…… 241
习题十四…… 243

第 15 章 零知识证明

15.1 交互零知识证明系统的定义…… 244
15.2 交互零知识证明系统的构造…… 249
15.3 非交互零知识证明系统理论…… 253
习题十五…… 257

附录 数学基础…… 259

参考文献…… 277

第1章 引 论

1.1 密码学研究的基本问题

在历史上(1975年以前),为了通过公开的通信媒体(如电话)进行秘密通信,密码学研究的问题仅限于设计和分析密码体制(通称密码系统)。但从1975年以来,构造不能伪造的数字签名问题和设计抗欺骗协议(fault-tolerant protocol)问题也被包括在现代密码学的研究范围内。总之,设计和分析任何安全协议(为抗拒参与者各方内部或外部可能有不诚实者为了达到种种目的而进行的恶意破坏)的问题都被认为是现代密码学研究的领域。因此,如何度量或评价一个密码系统(包括协议)的安全性则成为密码学研究的一个重要问题。现有两种定义"安全性"的方法:一种是基于信息论的方法(经典方法);另一种是基于计算复杂性理论的方法(现代方法)。为了构造安全的密码系统,有几个基本工具是非常有用的,它们是单向函数、伪随机序列生成器、零知识证明和杂凑函数(Hash function)。对于上述问题和涉及的有关概念,在给出它们的正式定义之前,先给出一个简短的基于直观的说明,以使读者对密码学要研究的问题有一个直观的了解。

1.1.1 密码体制

通过不安全的通信媒介进行安全通信问题是密码学研究的最基本的问题。它的背景是两个参与者通过一个信道(如电话)进行通信,可能被第三者(称为搭线者)搭线窃听。通信双方希望相互交换信息而让搭线者对信息内容尽可能无知。不严格地说,一个密码体制(有时也称加密方案)是一个使通信双方能进行秘密通信的协议。一个典型的加密方案包括两个算法:一个称为加密算法,由发方用来发送消息;另一个称为解密算法,由收方用来接收消息。因此,为了发送一个消息,发方首先用加密算法处理消息,发送处理结果,称为密文。收到密文后,收方用解密算法将密文恢复为原始消息,称为明文。为使这一方案能提供秘密通信,通信双方(至少收方)必须知道某些搭线者不知道的东西,否则搭线者也能像收方一样地恢复消息。这个外加知识的形式,可以是解密算法本身或它的某些参数和(或)辅助输入,称这个外加知识为解密密钥。不失一般性,可设搭线者知道加密算法

和解密算法,解密算法需要两个输入,即密文和解密密钥。要注意的是,存在一个搭线者不知道的解密密钥只是提供秘密通信的一个必要条件。

如何估价一个密码体制的安全性是件要仔细推敲的事。前面已提到现有两种定义"安全性"的方法。基于信息论的定义是用密文中是否蕴含明文的信息作为标准。不严格地说,若密文中不含明文的任何信息,则认为该密码体制是安全的,否则就认为是不安全的。已经证明,达到这样高等级(完善)的安全性,仅当所用密钥的长度不短于加密的发送消息的总长度才有可能。这种安全性称为无条件安全性,即无论搭线者有多少计算资源,他也不能从截取到的密文恢复出明文。但这种密码体制的应用受到严重的限制,特别是需要发送大量秘密信息的情形。

基于计算复杂性理论的安全性定义则不考虑密文中是否蕴含明文的信息,而是考虑这些信息是否能有效地被提取出来。换句话说,把搭线者提取明文信息的可能性改为搭线者提取明文信息的可行性,这种安全性称为有条件安全性,即搭线者在一定的计算资源条件下,不能从密文恢复出明文。已经证明,为达到基于计算复杂性理论定义的安全性,所用密钥长度可以比加密的发送消息的总长度短得多。例如,可用伪随机序列生成器将短的随机密钥扩展为较长的伪随机密钥,用它构造的密码体制具有与用长度相当的随机密钥构造的密码体制同样的安全性。

更有意思的是,用基于计算复杂性理论的方法可以引入一些新的概念和源头,这些概念和源头在信息论方法下是不可能存在的,典型的例子是公钥密码体制。前面集中讨论了解密算法和解密密钥。可以证明,加密算法除了输入发送消息外,还必须有一个辅助输入(依赖于解密密钥),这个辅助输入称为加密密钥。在经典的密码体制中,特别是在1980年以前所用的所有密码体制中,加密密钥与解密密钥是相同的,称这类密码体制为私钥(对称)密码体制。在这类密码体制中,搭线者必须不知道加密密钥,从而产生密钥分发问题,即如何使通信双方得到同样的加解密密钥。传统的方法是用比公开信道代价高得多的安全信道交换密钥。在公钥密码体制中,加密密钥可以公开让大家知道而并不损害密码体制的安全性。当然,加密密钥与解密密钥是不同的,且要求从加密密钥计算解密密钥是不可行的,这就自然地解决了密钥分发问题。

密码分析是研究密码体制的破译问题,即试图在不知道密钥的情况下,从截取到的密文恢复出明文消息或密钥,这正好是搭线者想做的事情。同时,密码体制的设计者和用户也应关心密码分析问题,因为对一个具体的密码体制的分析结果是评价这一体制安全性的一种检验。根据密码分析者可能取得的分析资料的不同,密码分析(或称攻击)可分为下列四类:

(1) 唯密文分析(攻击),密码分析者取得一个或多个用同一密钥加密的密文;

(2) 已知明文分析(攻击),除要破译的密文外,密码分析者还取得一些用同一密钥加密的明密文对;

(3) 选择明文分析(攻击),密码分析者可取得他所选择的任何明文所对应的密文(当

然,不包括他要恢复的明文),这些明密文对和要破译的密文是用同一密钥加密的;

(4) 选择密文分析(攻击),密码分析者可取得他所选择的任何密文所对应的明文(要破译的密文除外),这些密文和明文和要破译的密文是用同一解密密钥解密的,它主要应用于公钥密码体制。

1.1.2 单向函数与伪随机序列生成器

单向函数是基于计算复杂性理论的方法引入的一个最基本的新概念。不严格地说,一个单向函数是一个函数 $y=f(x)$,由 x 计算函数值 y 是容易的,但由 y 计算函数的逆 $x=f^{-1}(y)$ 是困难的(在某种平均意义下)。"容易"和"困难"的确切含意由计算复杂性理论定义。单向函数是现代密码学的一个基本工具,大部分安全的密码系统(包括协议)的构造依赖于"单向函数存在"这一假设,但单向函数的存在性至今没有证明。虽然如此,密码学界还是普遍相信单向函数是存在的,而且还给出了一些经过分析、检验的被认为是单向函数的例子。

伪随机序列生成器也是密码学的一个基本工具,在构造密码系统中起着重要作用,特别是它可构造简单的私钥密码体制(流密码)。在实际应用中,伪随机序列生成器虽然不是计算复杂性理论方法引入的新概念,在密码学文献及更广的概率计算文献中却早有研究和应用,但很少给出确切的定义,这对密码学应用是很不安全的。应用计算复杂性理论方法可给出伪随机序列生成器的一个确切定义。直观地说,一个伪随机序列生成器是一个确定算法,它把短的随机比特(种子)扩展为长得多的貌似随机的比特序列。换句话说,伪随机序列生成器的输出虽然不是真正的随机序列,但在计算资源一定的条件下,要判别这个输出与等长的真随机序列的不同是不可行的。可以证明,伪随机性与计算困难性有密切联系,因为可用单向函数来构造伪随机序列生成器。事实上,可证伪随机序列生成器的存在性和单向函数的存在性是等价的。

1.1.3 数字签名与杂凑(Hash)函数

数字签名是一个在全球计算机网发展以前不存在的概念。它是在计算机通信网上从事商贸和有关事务的环境下提出和需要研究的问题。某些参与者需要在他们发送的电子文件上签名以示承担责任。当然,不能伪造的签名在几个世纪以前就有讨论,但讨论的只是手写签名而不是数字签名,而且看不出这种讨论与密码学有什么关系。

加密和签名数字化了,并引入了安全性的计算复杂性理论方法,这使它们之间可能建立起一定的关系。不严格地说,对一个不能伪造的数字签名方案有下列要求:

(1) 每个用户能有效(容易)地在他选择的文件上产生他自己的签名;

(2) 每个用户能有效(容易)地验证一给定的数字串是否是另一特定用户在某特定文件上的签名;

(3) 没人能在其他用户没签名的文件上有效(容易)地产生他们的签名。