国外计算机科学教材系列

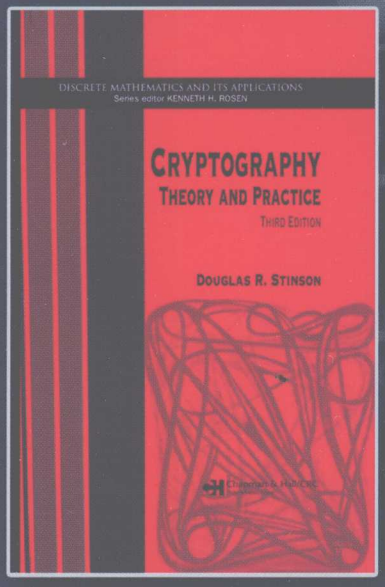
CHAPMAN&HALL/CRC

密码学原理与实践

（第三版）

Cryptography Theory and Practice

Third Edition



[加] Douglas R. Stinson 著

冯登国 等译

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

国外计算机科学教材系列

密码学原理与实践

（第三版）

Cryptography Theory and Practice

Third Edition

[加] Douglas R. Stinson 著

冯登国 等译

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 简 介

本书是密码学领域的经典著作，被世界上的多所大学用做指定教科书。本书在第二版的基础上增加了7章内容，不仅包括一些典型的密码算法，而且还包括一些典型的密码协议和密码应用。全书共分 14 章，从古典密码学开始，继而介绍了Shannon信息论在密码学中的应用，然后进入现代密码学部分，先后介绍了分组密码的一般原理、数据加密标准(DES)和高级加密标准(AES)、Hash 函数和MAC算法、公钥密码算法和数字签名、伪随机数生成器、身份识别方案、密钥分配和密钥协商协议、秘密共享方案，同时也关注了密码应用与实践方面的一些进展，包括公开密钥基础设施、组播安全和版权保护等。在内容的选择上，全书既突出了广泛性，又注重对要点的深入探讨。书中每一章后都附有大量的习题，这既利于读者对书中内容的总结和应用，又是对兴趣、思维和智力的挑战。

本书适合于作为计算机科学、数学等相关学科的密码学课程的教材或教学参考书，同时也是密码学研究的必备参考书。

版权贸易合同登记号　图字：01-2009-2867

图书在版编目(CIP)数据

密码学原理与实践：第 3 版/(加)斯廷森(Stinson, D. R.)著；冯登国等译. —北京：电子工业出版社，2009.7
(国外计算机科学教材系列)

书名原文：Cryptography:Theory And Practice，Third Edition

ISBN 978-7-121-09028-8

I. 密… II. ①斯…②冯… III. 密码－理论－教材 IV. TN918.1

中国版本图书馆 CIP 数据核字(2009)第 093828 号

策划编辑：马　岚
责任编辑：李秦华
印　　刷：北京天宇星印刷厂
装　　订：三河市皇庄路通装订厂
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：787×1092　1/16　印张：29.25　字数：749 千字
印　　次：2009 年 7 月第 1 次印刷
印　　数：4000 册　　定价：55.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：(010) 88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：(010) 88258888。

出 版 说 明

21世纪初的5至10年是我国国民经济和社会发展的重要时期，也是信息产业快速发展的关键时期。在我国加入WTO后的今天，培养一支适应国际化竞争的一流IT人才队伍是我国高等教育的重要任务之一。信息科学和技术方面人才的优劣与多寡，是我国面对国际竞争时成败的关键因素。

当前，正值我国高等教育特别是信息科学领域的教育调整、变革的重大时期，为使我国教育体制与国际化接轨，有条件的高等院校正在为某些信息学科和技术课程使用国外优秀教材和优秀原版教材，以使我国在计算机教学上尽快赶上国际先进水平。

电子工业出版社秉承多年来引进国外优秀图书的经验，翻译出版了“国外计算机科学教材系列”丛书，这套教材覆盖学科范围广、领域宽、层次多，既有本科专业课程教材，也有研究生课程教材，以适应不同院系、不同专业、不同层次的师生对教材的需求，广大师生可自由选择和自由组合使用。这些教材涉及的学科方向包括网络与通信、操作系统、计算机组织与结构、算法与数据结构、数据库与信息处理、编程语言、图形图像与多媒体、软件工程等。同时，我们也适当引进了一些优秀英文原版教材，本着翻译版本和英文原版并重的原则，对重点图书既提供英文原版又提供相应的翻译版本。

在图书选题上，我们大都选择国外著名出版公司出版的高校教材，如Pearson Education培生教育出版集团、麦格劳－希尔教育出版集团、麻省理工学院出版社、剑桥大学出版社等。撰写教材的许多作者都是蜚声世界的教授、学者，如道格拉斯·科默（Douglas E. Comer）、威廉·斯托林斯（William Stallings）、哈维·戴特尔（Harvey M. Deitel）、尤利斯·布莱克（Uyless Black）等。

为确保教材的选题质量和翻译质量，我们约请了清华大学、北京大学、北京航空航天大学、复旦大学、上海交通大学、南京大学、浙江大学、哈尔滨工业大学、华中科技大学、西安交通大学、国防科学技术大学、解放军理工大学等著名高校的教授和骨干教师参与了本系列教材的选题、翻译和审校工作。他们中既有讲授同类教材的骨干教师、博士，也有积累了几十年教学经验的老教授和博士生导师。

在该系列教材的选题、翻译和编辑加工过程中，为提高教材质量，我们做了大量细致的工作，包括对所选教材进行全面论证；选择编辑时力求达到专业对口；对排版、印制质量进行严格把关。对于英文教材中出现的错误，我们通过与作者联络和网上下载勘误表等方式，逐一进行了修订。

此外，我们还将与国外著名出版公司合作，提供一些教材的教学支持资料，希望能为授课老师提供帮助。今后，我们将继续加强与各高校教师的密切联系，为广大师生引进更多的国外优秀教材和参考书，为我国计算机科学教学体系与国际教学体系的接轨做出努力。

电子工业出版社

教材出版委员会

译 者 序

2002 年我组织相关专家翻译了 Douglas R. Stinson 所著的《密码学原理与实践》一书的第二版，本书翻译出版后在国内密码学界产生了很大的影响，反应很好。凭我自己的学习经验，要掌握好一门课程，必须精读一两本好书，我认为本书是值得精读的一本。2008 年年初，电子工业出版社委托我翻译 Douglas R. Stinson 所著的《密码学原理与实践》一书的第三版，我通读了一遍本书，发现本书的前 7 章与第二版的几乎一样，只有细微差异，但新增加了 7 章内容，这些内容都很基础也很新颖，我受益匪浅，于是我花了大量时间翻译了本书，以供密码学爱好者参考。

本书是一本很有特色的教科书，具体表现在以下 6 个方面：

1．表述清楚。书中所描述的问题浅显易懂，如分组密码的差分分析和线性分析本是很难描述的问题，本书中以代替置换网络(SPN)作为数学模型表述得很清楚。

2．论证严谨。书中对很多密码问题如唯一解距离、Hash 函数的延拓准则等进行了严格的数学证明，有一种美感。

3．内容新颖。书中从可证明安全的角度对很多密码问题特别是公钥密码问题进行了清楚的论述，使用了谕示器(Oracle)这一术语，通过阅读本书可使读者能够掌握这一术语的灵魂。书中对一些最新领域，如组播安全、数字版权保护等也做了相应的介绍。

4．选材精良。书中选择一些典型的、相对成熟的素材进行重点介绍，对一些正在发展的方向或需要大量篇幅介绍的内容以综述或解释的方式进行处理，特别适合于各种层次的教学使用。

5．覆盖面广。几乎覆盖了密码学的所有核心领域以及部分前沿内容，通过阅读本书可以了解密码学的全貌。

6．习题丰富。书中布置了大量的习题，通过演练这些习题可以熟练掌握密码学的基本技巧。

本书在翻译过程中，得到了很多老师的协助，张斌副研究员协助翻译了第 8 章、徐静副教授协助翻译了第 9 章、张振峰副研究员协助翻译了第10章、陈华副研究员协助翻译了第11章、张立武副研究员协助翻译了第12章、林东岱研究员协助翻译了第13章、赵险峰副研究员协助翻译了第 14 章，全书由我统一统稿。没有他们的鼎力相助，本书决不会这么快问世，在此对他们表示衷心的感谢。

本书的出版得到了国家 973 项目(编号：2007CB311202)和国家自然科学基金(编号：60673083)的支持，在此表示感谢。

冯登国

2008 年夏于北京

前　言

本书的第一版出版于1995年，共包含13章内容。第一版的编写目标是编写一本关于密码学所有核心领域以及部分前沿内容的通用教材。在编写过程中，我尽力使本书的内容能够适应密码学相关各种课程的要求，使其可用于数学、计算机和各工程专业的大学生和研究生课程。

本书的第二版出版于2002年，内容集中于更适合在课程中介绍的密码学核心领域的内容。与第一版相反，第二版只包含7章。我当时的目的是编写一本随身手册，包含第一版各章节更新后的内容，也有介绍新内容的章节。

然而，在撰写第三版时，我改变了计划，决定编写一本扩充内容的第三版。第三版内容的广度和范围更类似于第一版，不过大部分内容都经过完全重写。这个版本适当更新了第二版7章中的内容，并新加入了另外7章的内容。下面是这本《密码学原理与实践》第三版总共14章的简要大纲：

- 第1章对简单的“经典”密码体制做了基本的介绍。这一章也介绍了本书中使用的基本数学知识。
- 第2章介绍了Shannon对密码学研究的主要内容。包括完善保密性和熵的概念，以及信息论在密码学中的应用。
- 第3章关注的是分组密码。使用了代替置换网络(SPN)作为数学模型来介绍现代分组密码设计和分析的很多概念，包括差分和线性分析，并侧重于介绍基本原理。使用两个典型的分组密码(DES和AES)来阐述这些基本原理。
- 第4章统一介绍了带密钥和不带密钥的Hash函数，以及它们在构造消息认证码方面的应用，侧重于数学分析和安全性验证。本章还包括了安全Hash算法(SHA)的介绍。
- 第5章是关于RSA密码体制，以及大量数论背景知识的介绍，如素性检测和因子分解。
- 第6章讨论了公钥密码体制，如基于离散对数问题的ElGamal密码体制。另外还有一些关于计算离散对数、椭圆曲线和Diffie-Hellman问题的内容。
- 第7章介绍的是数字签名方案。介绍了很多具体方案，如数字签名算法(DSA)，还包括了一些特殊类型的签名方案，如不可否认、fail-stop签名方案等。
- 第8章包含了密码学中的伪随机比特生成器。本章基于第一版的相关章节。
- 第9章是关于身份识别(实体认证)。本章第一部分讨论了从简单的密码本原(primitive)，如数字签名方案或消息认证码构造的方案。第二部分在第一版内容的基础上介绍了特殊目的的“零知识”方案。
- 第10章和第11章讨论了各种不同的密钥建立方法。第10章是关于密钥分配，第11章介绍了密钥协商协议。这两章的内容比第一版内容丰富了很多(第二版不包含密钥建立的内容)。这两章比以前更加侧重于安全模型和证明。

- 第 12 章对公钥基础设施(PKI)做了总体的介绍，同时也讨论了与 PKI 拥有同样作用的基于身份的密码学。这是一个全新的章节。
- 第 13 章的主题是秘密共享方案。本章内容基于第一版的相应章节。
- 第 14 章是一个全新的章节，讨论了组播安全。包括广播加密和版权保护。

下面是本书所有版本的特点：

- 所有需要相应数学背景知识的地方都有很及时的介绍。
- 对密码体制非正式的描述都附带伪代码。
- 使用了很多例子来阐述本书中大多数的算法。
- 各算法和密码体制的数学基础都有很严格、很仔细的解释。
- 本书包含了很多习题，其中一些相当具有挑战性。

我相信这些特点使得本书用于课堂讲授和自学都更加有用。

在本书中，尽量按照符合逻辑的、自然的顺序安排书中的内容。有时读者有可能为了集中了解后面的某一内容而跳过前面的章节。不过有几章的内容确实非常依赖前面的章节。下面是一些重要的依赖关系：

- 第 9 章使用了第 4 章(消息认证码)和第 7 章的内容(数字签名方案)。
- 第 13 章的 13.3.2 节使用了第 2 章关于熵的结论。
- 第 14 章使用了第 10 章(密钥预分配)和第 13 章(秘密共享)的内容。

还有很多地方，前面章节介绍的数学工具会用到后面的章节里，但是应该不会造成课堂讲授的困难。

决定介绍多少数学基础知识，是编写任何一本密码学书籍最困难的事情之一。密码学是一个涉及面广的学科，需要若干数学领域的知识，如数论、群环域理论、线性代数、概率论和信息论。同样也需要熟悉计算复杂度、算法和 NP 问题。在我看来，数学知识不够是很多学生在刚开始学习密码学时遇到困难的原因。

本书中尽量介绍遇到的数学背景知识，在大多数时候，都会详细介绍用到的数学工具。但是如果读者对基本的线性代数和模运算有一定了解的话，是非常有帮助的。

很多人指出了第二版和第三版草稿中的错误，并对加入的新内容的选择和内容的广度提出了有用的建议。特别要感谢 Carlisle Adams，Eike Best，Dameng Deng，Shuhong Gao，K.Gopalakrishnan，Pascal Junod，Torleiv Kløve，Jooyoung Lee，Vaclav Matyas，Michael Monagan，James Muir，Phil Rose，Tamir Tassa 和 Rebecca Wright。与往常一样，希望大家能够用勘误表的方式通知我，我会把它们放在一个网页上。

Douglas R. Stinson

于加拿大安大略省滑铁卢市

目　录

第 1 章　古典密码学

本章主要对密码学和密码分析做一简要介绍，并给出一些简单的古典密码体制，以及对这些体制的破译方法。同时，本章对本书中要用到的各种数学知识也做了介绍。

1.1　几个简单的密码体制

密码学的基本目的是使得两个在不安全信道中通信的人，通常称为 Alice 和 Bob，以一种使他们的敌手 Oscar 不能明白和理解通信内容的方式进行通信。这样的不安全信道在实际中是普遍存在的，例如电话线或计算机网络。Alice 发送给 Bob 的信息，通常称为明文(plaintext)，例如英文单词、数据或符号。Alice 使用预先商量好的密钥(key)对明文进行加密，加密过的明文称为密文(ciphertext)，Alice 将密文通过信道发送给 Bob。对于敌手 Oscar 来说，他可以窃听到信道中 Alice 发送的密文，但是却无法知道其所对应的明文；而对于接收者 Bob，由于知道密钥，可以对密文进行解密，从而获得明文。

上述观点可用数学方式描述为定义 1.1。

定义 1.1　一个密码体制是满足以下条件的五元组 $(\mathcal{P},\mathcal{C},\mathcal{K},\mathcal{E},\mathcal{D})$：

1. $\mathcal{P}$ 表示所有可能的明文组成的有限集。
2. $\mathcal{C}$ 表示所有可能的密文组成的有限集。
3. $\mathcal{K}$ 代表密钥空间，由所有可能的密钥组成的有限集。
4. 对每一个 $K\in\mathcal{K}$，都存在一个加密规则 $e_K\in\mathcal{E}$ 和相应的解密规则 $d_K\in\mathcal{D}$。并且对每对 $e_K:\mathcal{P}\to\mathcal{C}$，$d_K:\mathcal{C}\to\mathcal{P}$，满足条件：对每一个明文 $x\in\mathcal{P}$，均有 $d_K(e_K(x))=x$。

定义 1.1 中，最关键的是性质 4。它主要保证了如果使用 e_K 对明文 x 进行加密，则可使用相应的 d_K 对密文进行解密，从而得到明文 x。

Alice 和 Bob 通过下列流程使用一个特定的密码体制。首先，他们随机选择一个密钥 $K\in\mathcal{K}$，这一步必须在安全的环境下进行，不能被敌手 Oscar 知道，例如，两人可在同一地点协商密钥，或者使用安全信道传输密钥。完成密钥协商后，假如 Alice 想通过不安全信道发送消息串给 Bob，不妨设此消息串为

$$x=x_1x_2\cdots x_n$$

n 为正整数，$x_i\in\mathcal{P}$，$i=1,2,\cdots,n$。对每一个 x_i，使用加密规则 e_K 对其进行加密，K 是预先协商好的密钥。Alice 计算 $y_i=e_K(x_i)$，$1\leqslant i\leqslant n$。然后将密文串

$$y=y_1y_2\cdots y_n$$

通过信道发送给 Bob。当 Bob 接收到密文串 $y_1y_2\cdots y_n$ 时，他使用解密规则 d_K 对其进行解密，就可得到明文串 $x_1x_2\cdots x_n$。图 1.1 具体描述了这一加解密过程。

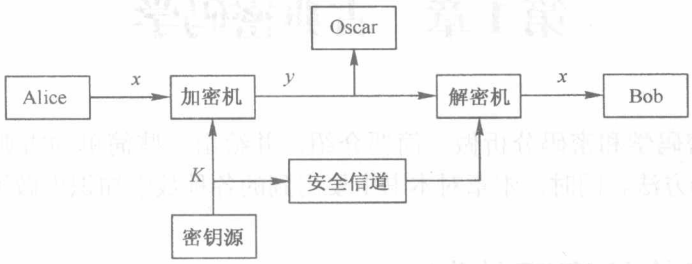


图 1.1 通信信道

显然，用来加密的加密函数 e_K 必须是一个单射函数(例如，一对一映射)，否则将给解密工作带来麻烦，例如，如果

$$y=e_K(x_1)=e_K(x_2)$$

且 $x_1\neq x_2$，则 Bob 就无法判断 y 究竟该对应于 x_1 还是 x_2。如果 $\mathcal{P}=\mathcal{C}$，即明文空间等于密文空间，则具体的加密函数就是一个置换。这就是说，如果明文空间等于密文空间，则每个加密函数仅仅是对明文空间的元素的一个重新排列(置换)。

1.1.1 移位密码

本小节介绍移位密码(Shift Cipher)，其基础是数论中的模运算。这里首先给出一些模运算的基本定义。

定义 1.2 假设 a 和 b 均为整数，m 是一正整数。若 m 整除 $b-a$，则可将其表示为 $a\equiv b(\mathrm{mod}\,m)$。式 $a\equiv b(\mathrm{mod}\,m)$ 读作“a 与 b 模 m 同余”，正整数 m 称为模数。

假如用 m 分别除 a 与 b，可得相应的商和余数，余数是在 0 与 $m-1$ 之间。即可将 a 与 b 分别表示为 $a=q_1m+r_1$，$b=q_2m+r_2$，$0\leqslant r_1\leqslant m-1$，$0\leqslant r_2\leqslant m-1$。这样，易看出 $a\equiv b(\mathrm{mod}\,m)$ 当且仅当 $r_1=r_2$。我们将用记号 $a\bmod m$ 来表示 a 除以 m 所得的余数。因此 $a\equiv b(\mathrm{mod}\,m)$ 当且仅当 $a\bmod m=b\bmod m$。如果用 $a\bmod m$ 来代替 a，我们就说 a 被模 m 约化了。

我们给出两个例子，计算 $101\bmod 7$，$101=7\times 14+3$，因为 $0\leqslant 3\leqslant 6$，故 $101\bmod 7=3$。再如计算 $(-101)\bmod 7$，因为 $-101=7\times(-15)+4$，故 $(-101)\bmod 7=4$。

注：许多计算机编程语言定义 $a\bmod m$ 的取值在 $-m+1,\cdots,m-1$ 之间，并要求取值和 a 的正负号相同。在此定义下，(−101)mod 7 应为−3。但在这里，为了方便起见，我们要求 $a\bmod m$ 恒为一非负值。

我们现在定义模 m 上的算术运算：令 $\mathbb{Z}_m$ 表示集合 $\{0,1,\cdots,m-1\}$，在其上定义两个运算，加法(+)和乘法(×)，其运算类似于普通的实数域上的加法和乘法，所不同的只是所得的值是取模以后的余数。