Springer

安全技术经典译丛

深入浅出密码学

——常用加密技术原理与应用

Understanding Cryptography:
A Textbook for Students and Practitioners

[美] Christof Paar, Jan Pelzl 著

马小婷 译

- 著名密码学专家打造的力作
- 作者长期教学经验的浓缩和结晶
- 通透讲解绝大多数实际使用的加密算法
- 指导您深入理解现代加密方案的工作原理

清华大学出版社

安全技术经典译丛

深入浅出密码学

——常用加密技术原理与应用

[美] Christof Paar 著
Jan Pelzl
马小婷 译

清华大学出版社
北 京

北京市版权局著作权合同登记号　图字：01-2011-6699

图书在版编目(CIP)数据

深入浅出密码学——常用加密技术原理与应用/(美)帕尔(Paar, C.)，(美)佩尔茨尔(Pelzl, J.) 著；马小婷 译. —北京：清华大学出版社，2012.9

(安全技术经典译丛)

书名原文：Understanding Cryptography: A Textbook for Students and Practitioners

ISBN 978-7-302-29609-6

Ⅰ. ①深… Ⅱ. ①帕… ②佩… ③马… Ⅲ. ①密码—理论 Ⅳ. ①TN918.1

中国版本图书馆 CIP 数据核字(2012)第 178347 号

责任编辑：王　军　韩宏志

装帧设计：康　博

责任校对：蔡　娟

责任印制：宋　林

出版发行：清华大学出版社

网　　址：http://www.tup.com.cn，http://www.wqbook.com

地　　址：北京清华大学学研大厦 A 座　　**邮　　编**：100084

社 总 机：010-62770175　　**邮　　购**：010-62786544

投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn

质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn

印 刷 者：清华大学印刷厂

装 订 者：北京市密云县京文制本装订厂

经　　销：全国新华书店

开　　本：185mm×230mm　　**印　　张**：22.75　　**字　　数**：468 千字

版　　次：2012 年 9 月第 1 版　　**印　　次**：2012 年 9 月第1 次印刷

印　　数：1～3000

定　　价：59.00 元

产品编号：041528-01

致谢

如果没有多位人士的支持和帮助，我们不可能完成这本书的撰写。我期望我们的感谢没有遗漏任何人士。

首先要感谢 Daehyun Strobel 和 Pascal WiBmann 出色的工作，他们提供了本书中绝大多数插图，并毫无怨言地接受我们提出的多次修改。Axel Poschmann 提供了本文中最新的主题，即当前的分组密钥的内容，非常感谢他对本书的贡献。而提供技术性问题的解决方案有 Frederick Armknecht(序列密码)、Roberto Avanzi(有限域和椭圆曲线)、Alex May(数论)、Alfred Menezes 和 Neal Koblitz(椭圆密码学的发展历史)、Matt Robshaw(AES)和 Damian Weber(离散对数)。

非常感谢波鸿大学嵌入式安全组织的成员们——Andrey Bogdanov、Benedikt Driessen、Thomas Eisenbarth、Tim Güneysu、Stefan Heyse、Markus Kasper、Timo Kasper、Amir Moradi 和 Daehyun Strobel——他们在本书的技术校对方面做了大量工作，并在改进素材的编排方式上提出了很有用的建议。尤其要感谢 Daehyun 和 Markus，谢谢他们分别在实例与一些高级 LATEX 工作方面与课后问题方面的帮助！我们还要感谢 Olga Paustjan 在插图和排版方面的帮助。

我们组中上一届的博士生帮助创建了本书在线课程，他们是 Sandeep Kumar、Kerstin Lemke-Rust、Andy Rupp、Kai Schramm 和 Marko Wolf。他们的工作十分出色，令我们深受鼓舞。

我们感到非常荣幸地邀请到 Bart Preneel 为本书写序。在此，我们再次向他表示我们的深切谢意。最后也非常感谢 Springer 给予的支持和鼓励，尤其是本书的编辑 Ronan Nugent 和 Alfred Hofmann，非常感谢你们！

序言

密码学的学术研究始于20世纪70年代中期。如今，密码学已经发展成为一门成熟的研究学科，拥有不少成立多年的专业组织(如国际密码安全协会)、数以万计的研究员和几十个国际会议。在密码学及其应用领域，每年都有数以千计的学术论文发表。

20世纪70年代，密码学仅应用于外交、军事和政府等领域；而到了20世纪80年代，金融和通信产业都已使用了硬件加密设备。20世纪80年代末的数字手机系统标志着密码学第一次在大众市场的大规模应用。如今，基本上每个人每天都会用到密码学，比如使用远程控制设备打开车门或车库门、连接到无线LAN、用信用卡在零售店或网上购物、安装一个软件更新、拨打IP语音电话或在公共交通系统中购票。毋庸置疑，诸如电子健康、汽车远程信息处理系统和智能建筑等新兴应用领域的涌现会促使密码学的应用更趋普及。

密码学是一门非常有趣的学科，它与计算机科学、数学以及电子工程都存在交叉。随着密码学日新月异地取得发展，人们现在已经很难跟上它的发展步伐。密码学领域的理论基础在过去的25年里已经得到加强和巩固；现在，人们对安全的定义和证明结构安全的方法有了更深入的认识。同时，我们也见证了应用密码学的快速发展：旧算法不断地被破解和抛弃，同时，新算法和协议也在不断涌现。

在过去几十年里，已有不少密码学方面的优秀教材出版，这些教材主要面向拥有扎实数学背景的读者。此外，一些具有吸引力的新进展和高级协议也为此增加了很多有趣的素材。本书的最大价值在于重点讨论了密码学研究人员所关心的主题。而且，本书对数学背景知识和公式的使用加以严格限制——只有在必要的情况下才会在适当的地方介绍这些数学知识和公式。对密码学领域的新手而言，这种“少即是多”的方法足以满足他们的需求，因为本书将带领他们一步一步地学习基本概念和各种精心选择的算法与协议。对于想要深入学习和拓展知识的读者而言，本书每个章节都提供了非常有用的扩展阅读素材。

总体而言，本书作者成功地介绍了应用密码学主题相关的内容，这些内容具有极高的价值，对此我感到非常高兴。我希望这本书可以对密码学相关的从业人员有一定的指导作用，帮助他们构建更安全的基于密码学的系统；也希望本书能成为未来研究学者发现密码学及其应用方面更精彩方面的阶梯。

Bart Preneel
2009 年 8 月

前言

密码学已经渗透到我们生活的方方面面，从 Web 浏览器和电子邮件程序，到手机、银行卡、汽车，甚至包括器官移植。在不久的将来，我们将看到密码学更多令人激动不已的新应用，比如防伪的射频识别(RFID)标签，或车对车的通信(已经有人在为保证这两种应用的安全而努力)。过去，密码学总是被传统地限制在十分特殊的应用领域，尤其是政务信息和银行系统。时至今日，这种情况已经发生了很大的改变。由于加密算法的普遍性，越来越多的人必须理解加密算法的工作原理，以及怎样将它们应用到实践中；本书全面介绍当前应用的密码学，为读者释疑解惑，堪称读者的良师益友。本书面向学生和密码行业的从业者。

本书可以帮助读者深入地理解现代加密方案的工作原理。本书在对大学级别微积分背景要求最少的情况下，以最通俗易懂的方式介绍了必要的数学概念。所以，对本科生或即将开始学习研究生课程的学生而言，本书是一本非常合适的教科书；而对期望更深入理解现代密码学的职业工程师或计算机科学家而言，本书则是极具价值的参考书。

本书拥有的诸多特征使得它成为密码学从业者和学生独一无二的资源——本书介绍了绝大多数实际应用中使用的加密算法，并重点突出了它们的实用性。对于每种加密模式，我们都给出了最新的安全评估和推荐使用的密钥长度。同时，本书也探讨了每种算法在软件实现和硬件实现中的一些重要问题。除加密算法外，本书还介绍了很多其他重要主题，比如加密协议、运作模式、安全服务和密钥建立技术等。此外，本书还包含了许多非常新的主题，比如针对受限的应用而优化的轻量级加密(例如 RFID 标签或智能卡)，或新的操作模式。

每章末尾的讨论单元都给出了许多注明出处的参考文献，为读者提供了大量扩展阅读的材料。对于课堂使用的读者而言，这些讨论单元提供了很好的课程项目资源。对于将本书当作教科书的读者，强烈推荐阅读本书的配套学习资源网站：

www.crypto-textbook.com

读者在这里可以找到许多关于课程项目的观点、开源软件的链接、测试向量和现代密码学的相关信息。此外，本书还提供了对应的视频教程的链接。

如何使用本书

本书提供的实例和相关材料在过去几十年经过了不断完善和改进，在课堂教学中也得到了广大师生的认可。我们也曾将本书作为初级研究生教程和高级本科生教程；同时，它也曾单独地用于 IT 安全工程专业本科生的课程。实践发现，两个学期内，每周 90 分钟的讲课时间加上 45 分钟的习题解答环节时间(总计 10 个 ECTS 学分)基本上可以完成本书绝大多数章节的教学。对典型的美国风格的三学分制的课程，或一学期欧洲学校的课程而言，本书的某些章节可以忽略。以下是两种针对一学期课程的合理选择：

课程选择 1：将重点放在密码学应用上，比如在计算机科学或电子工程项目中的应用。本书中的加密内容对计算机网络或高级安全课程有很好的辅助作用：第 1 章，第 2.1 到 2.2 节、第 4 章、第 5 章的 5.1 节、第 6 章、第 7 章的 7.1 节~ 7.3 节、第 8 章的 8.1 节~8.4 节、第 10 章的 10.1～10.2 节、第 11 章、第 12 章和第 13 章。

课程选择 2：将重点放在密码学算法及对应的数学背景上，比如可以把本书作为计算机科学专业、电子工程专业或数学系研究生的应用密码学课程。本书可以作为深入学习更理论化密码学研究生课程的先导教程。涉及的章节主要包括：第 1 章、第 2 章、第 3 章、第 4 章、第 6 章、第 7 章、第 8 章的 8.1 节~ 8.4 节、第 9 章、第 10 章和第 11 章的 11.1 节~11.2 节。

作为科班出生的工程师，我们已经在应用密码学和安全领域工作了 15 年以上，我们真诚地希望读者也能和我们一样，在这个奇妙的领域发现很多乐趣。

目 录

第 1 章

密码学和数据安全导论

本章将介绍现代密码学中一些非常重要的术语，并给出了专有算法与公开的已知算法的相关内容。本章还将介绍在公钥密码学中占有重要地位的运算，即模运算。

本章主要内容包括

- 密码学的通用准则
- 短期、中期及长期安全性所需要的合适密码长度
- 针对密码发起的各种攻击的区别
- 一些经典密码，并进一步介绍在现代密码学中占有重要地位的模运算
- 使用完善的加密算法的原因

1.1 密码学及本书内容概述

每当听到“密码学”这个词时，首先映入我们脑海的可能是电子邮件加密、网站的安全访问、银行应用程序使用的智能卡或第二次世界大战中的密码破译，比如针对德国的Enigma 加密机(如图 1-1 所示)的破译。

从表面上看，密码学与现代电子通信似乎有着密不可分的关系；实际上，密码学其实是一个非常古老的应用——最早使用密码学的例子可以追溯到公元前 2000 年，当古埃及还在使用没有标准密码规则的象形文字时。自埃及时代起，在几乎所有发明了文字的文化圈中，密码学总是以各种形式存在其中。例如，据相关文献记载，在古希腊时代就已经有将文字写成密文的事例，叫斯巴达密码棒(Scytale of Sparta)(图 1-2)，或下一章将要介绍的非

常出名的古罗马的凯撒密码(Caesar Cipher)。然而，本书主要侧重于现代密码学方法的研究，同时也阐述了许多数据安全问题及其与密码学的关系。

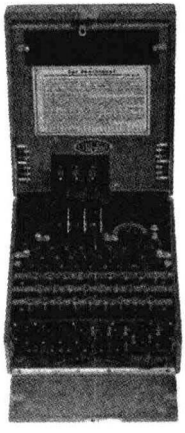

图 1-1　德国的 Enigma 加密机(由慕尼黑德意志博物馆授权复制)

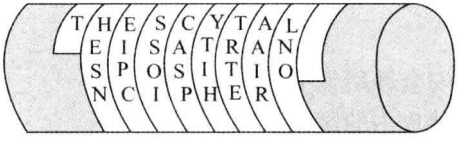

图 1-2　斯巴达密码棒

下面将介绍密码学领域(如图 1-3 所示)。首先要说明的一件事情是，最常用的术语是密码编码学(cryptology)，而不是密码使用学(cryptography)。密码编码学有两个主要分支：

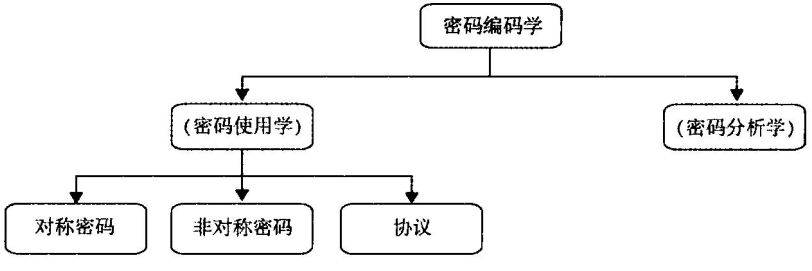

图 1-3　密码术领域概览

密码使用学指的是一种为了达到隐藏消息含义目的而使用的密文书写的科学。

密码分析学本身就是一种科学，在某些情况下也指一种破译密码体制的技巧。不少人

也许会认为密码破译应该只是那些情报部门或犯罪团伙所为，而不应该包括在严肃的自然学科分类中。然而，绝大多数的密码分析都是由当今学术界中赫赫有名的研究学者完成的。密码分析在现代密码体制中发挥着至关重要的作用：如果没有人试图破译我们的加密方法，我们永远也不知道这个系统是否安全。关于这个问题的更多讨论可以参阅第 1.3 节。

由于密码分析是确保密码体制安全的唯一方法，所以它是密码学中一个不可缺少的部分。然而，本书的重点在于密码使用学：将详细介绍最重要的实用加密算法。这些实用的加密算法已经在相当长的时间内抵御各种密码分析，有的加密算法甚至需要几十年的时间才能破译。在密码分析方面，本文将只提供破解已介绍的加密算法的最新结果，比如破译 RSA 方案的因式分解方法的记录。

现在回顾一下图 1-3。密码使用学本身可以分为以下三个主要分支：

对称算法(Symmetric Algorithm)：该算法是基于这样的假设：

双方共享一个密钥，并使用相同的加密方法和解密方法。1976 年以前的加密算法毫无例外地全部基于对称算法。如今对称密码仍广泛应用于各个领域，尤其是在数据加密和消息完整性检查方面。

非对称算法(Asymmetric Algorithm)或公钥算法(Public-Key Algorithm)：Whitfield Diffie、Martin Hellman 和 Ralph Merkle 在 1976 年提出了一个完全不同的密码类型。与对称密码学一样，在公钥密码学中用户也拥有一个密钥；但不同的是，他同时还拥有一个公钥。非对称算法既可以用在诸如数字签名和密钥建立的应用中，也可用于传统的数据加密中。

密码协议(Cryptographic Protocol)：粗略地讲，密码协议主要针对是密码学算法的应用。对称算法和非对称算法可以看作是实现安全 Internet 通信的基础。密码协议的一个典型示例就是传输层安全(TLS)方案，现在所有的 Web 浏览器都已使用这个方案。

严格来讲，将在第 11 章中介绍的哈希函数是除了对称算法和非对称算法外的第三种算法，但同时哈希函数与对称加密也存在一些相同的属性。

绝大多数实际系统中的加密应用都是同时使用对称算法和非对称算法(同时还包括哈希函数)。这种方案有时候也叫混合方案。同时使用这两种类型算法的原因在于，每类算法都有各自的优缺点。

本书重点讨论对称算法与非对称算法以及哈希函数，但也会介绍一些基本安全协议，尤其是几种密钥建立协议和使用加密协议的作用：数据保密性、数据完整性、数据认证和用户标识等。

1.2　对称密码学

本节主要介绍对称密码的概念和传统的替换密码。我们将以替换密码为例，介绍蛮力

攻击与分析攻击的区别。

1.2.1 基础知识

对称加密方案也称为对称密钥(Symmetric-key)、秘密密钥(secret-key)和单密钥(Single-key)方案(或算法)。我们先通过一个非常简单的问题来介绍对称密码学：假设两个用户——Alice和Bob——想通过一个不安全的信道进行通信(如图1-4所示)。“信道”这个术语看上去有点抽象，但它却是通信链路中最常见的术语：信道可以是Internet、手机使用的空气中的信道或无线LAN通信，或其他任何你可以想到的通信媒介。实际问题来自于一个名叫Oscar[1]的坏蛋，他试图通过侵入Internet路由器或监听Wi-Fi通信的无线电信号来访问Alice和Bob的通信信道。这种未授权的监听就称为窃听。显而易见，在很多情况下Alice和Bob都更愿意避开Oscar的监听进行通信。例如，如果Alice和Bob分别代表了一个汽车制造厂的两个办事员，他们想传输一些关于公司未来几年计划发展的新汽车模型商业战略方面的文档，同时这些文档不能落入竞争公司或关注此事的外国情报机构的手里。

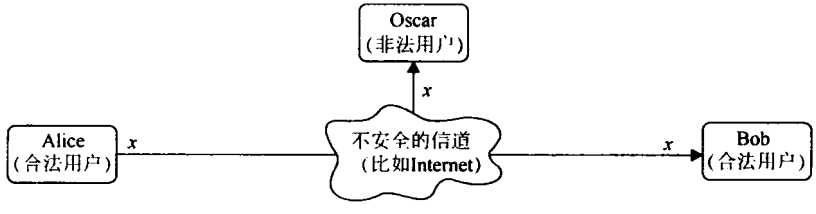

图1-4 不安全信道上的通信

在这种情况下，对称密码学提供了非常强大的解决方案：Alice使用对称算法加密她的消息x，得到密文y；Bob接收并解密该密文。解密过程与加密过程正好相反(如图1-5所示)。这种方法的优势在哪呢？如果选择的加密算法非常强壮，则Oscar监听到的密文看上去将是杂乱无章且没有任何意义的。

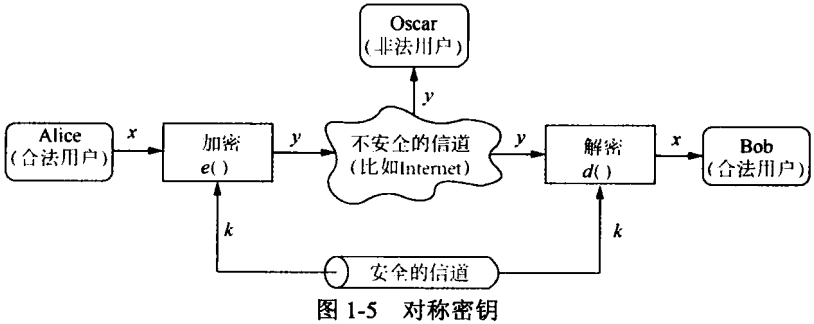

图1-5 对称密钥

1. 选择名字Oscar的原因是为了提醒我们世界的敌人。

变量 x、y 和 k 在密码学中非常重要，它们都有特殊的称谓：

- x 称为明文(*plaintext* 或 *cleartext*)
- y 称为密文(*ciphertext*)
- k 称为密钥(*key*)
- 所有可能密钥组成的集合称为密钥空间(*key space*)

这个系统通常需要一个安全的信道用于在 Alice 和 Bob 之间分配密钥。图 1-5 所示的安全信道有多种选择，它可以是一个人将该密钥装在钱夹里在 Alice 和 Bob 之间传输。当然，这种方法相对而言比较累赘。这种方法非常合适的一个例子就是无线 LAN 中 Wi-Fi 保护访问(Wi-Fi Protected Access，WPA)加密所使用的预共享密钥(pre-share key)的分配。后面的章节将介绍如何在不安全信道上建立密钥。在所有这些情况中，密钥只需要在 Alice 和 Bob 之间传送一次，就能用于保护后续多个通信的安全。

这个情况中有一个非常重要且令人匪夷所思的事实就是，它所使用的加密算法和解密算法都是公开且已知的。看上去，如果将加密算法保密应该会使得这个系统更难破译。但有一点值得注意的是：保密的算法也可能是未测试的算法。而证明某个加密方法是否强壮(即不能被顽固的攻击者破解)的唯一方法就是将其公开，让更多其他的密码员对其进行分析。关于此主题的更多讨论请阅读第 1.3 节。在一个可靠的密码体制中唯一需要保密的就是密钥。

注意：

(1) 如果 Oscar 得到了密钥，他理所当然可以很轻松地解密该消息，因为此加密算法是公开的。因此，需要注意的是：安全地传输消息的问题最后可以归结为安全地传输和存储密钥的问题。

(2) 在这个场景中，我们只考虑了保密性的问题，即防止消息被人窃听。后面的章节还将介绍密码学相关的其他内容，比如防止 Oscar 在 Alice 和 Bob 不知情的情况下篡改消息(消息完整性)，或确定消息真的来自于 Alice(发件人身份认证)。

1.2.2　简单对称加密：替换密码

现在我们将学习一种最简单的加密文本的方法，即替代密码或替换密码。这种类型的密码已被使用了无数次，而且它也是对基础密码学最好的解释。我们将使用替换密码作为学习密钥长度和破译密码的不同方式等重要方面的例子。

替换密码的目标就是加密文本(与现代数字系统中的位相反)，其思路非常简单：将字母表中的一个字符用另一个字符替换。

示例 1.1

```
A → k
B → d
```