信息安全国家重点实验室

信息安全丛书

Applied Cryptography

应用密码学

林东岱　曹天杰　编著

科学出版社
www.sciencep.com

信息安全国家重点实验室信息安全丛书

应用密码学

林东岱　曹天杰　编著

科学出版社
北京

内 容 简 介

本书是在作者多年从事应用密码学教学和科研工作基础上撰写而成，书中全面、系统、准确地讲述了现代密码学的基本概念、理论和算法。全书共分 11 章，内容包括：密码学概述、经典密码学、密码学的信息论基础、序列密码、分组密码、Hash 函数、消息认证码、公钥密码、数字签名、侧信道攻击以及密码协议。每章均配有习题，以帮助读者掌握本章重要知识点并加以巩固。

本书语言精炼，概念准确，内容全面，讲述的算法既包括密码学的经典算法，也包括了密码学领域的最新标准化算法。

本书可作为高等院校信息安全、信息对抗、计算机科学与技术、数学等专业的本科生及研究生教材，也可供信息安全领域的工程技术人员参考。

图书在版编目(CIP)数据

应用密码学/林东岱，曹天杰编著．—北京：科学出版社，2009
（信息安全国家重点实验室信息安全丛书）
ISBN 978-7-03-025841-0

Ⅰ．应… Ⅱ．①林…②曹… Ⅲ．密码-理论 Ⅳ．TN918.1

中国版本图书馆 CIP 数据核字（2009）第 190340 号

责任编辑：鞠丽娜/责任校对：王万红
责任印制：吕春珉/封面设计：三函设计

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

铭浩彩色印装有限公司 印刷

科学出版社发行 各地新华书店经销

*

2009 年 11 月第 一 版 开本：B5（720×1000）
2009 年 11 月第一次印刷 印张：14 1/2
印数：1—3 000 字数：290 000

定价：28.00 元

（如有印装质量问题，我社负责调换〈环伟〉）
销售部电话 010-62134988 编辑部电话 010-62138978-8002

序　言

人类的进步得益于科学研究的突破、生产力的发展和社会的进步。

计算机、通信、半导体科学技术的突破，形成了巨大的新型生产力。数字化的生存方式席卷全球。农业革命、工业革命、信息革命成为人类历史生产力发展的三座丰碑。古老的中华大地，也正在以信息化带动工业化的国策下焕发着青春。电子政务、电子商务等各种信息化应用之花，如雨后春笋，在华夏沃土上竞相开放，炎黄子孙们在经历了几百年的苦难历程后，在国家崛起中又迎来了一个运用勤劳和智慧富国强民的新契机。

科学规律的掌握，非一朝一夕之功。治水、训火、利用核能都曾经经历了多么漫长的时日。不掌握好科学技术造福人类的一面，就会不经意地释放出它危害人类的一面。

生产力的发展，为社会创造出许多新的使用价值。但是，工具的不完善，会限制这些使用价值的真正发挥。信息化工具也和农业革命、工业革命中人们曾创造的许多工具一样，由于人类认识真理和实践真理的客观局限性，存在许多不完善的地方，从而形成信息系统的漏洞，造成系统的脆弱性，在人们驾驭技能不足的情况下，损害着人们自身的利益。

世界未到大同时，社会上和国际间存在着竞争、斗争、战争和犯罪。传统社会存在的不文明、暴力，在信息空间也同样存在。在这个空间频频发生的有些人利用系统存在的脆弱性，运用其“暴智”来散布计算机病毒，制造拒绝服务的事端，甚至侵入他人的系统，盗窃资源、资产，以达到其贪婪的目的。人类运用智慧开拓的信息疆土正在被这些暴行蚕食破坏着。

随着信息化的发展，信息安全成为全社会的需求，信息安全保障成为国际社会关注的焦点。因为信息安全不但关系国家的政治安全、经济安全、军事安全、社会稳定，也关系到社会中每一个人的数字化生存的质量。

信息革命给人类带来的高效率和高效益是否真正实现，取决于信息安全是否得以保障。什么是信息安全？怎样才能保障信息安全？这些问题都是严肃的科学和技术问题。面对人机结合，非线性、智能化的复杂信息巨系统，我们还有许多科学技术问题需要认真的研究。我们不能在研究尚处肤浅的时候，就盲目乐观地向世人宣称，我们拥有了全面的解决方案；我们也不能因为面对各种麻烦，就灰头土脸，自暴自弃，我们需要的是具有革命的乐观主义精神，坚忍不拔的奋勇攀登科学技术高峰的坚定信念。

人是有能力认识真理的，今天对信息安全的认识，就经历了一个从保密到保护，又发展到保障的趋近真理的发展过程。因为信息安全的问题不仅仅是因为技术原因引起的，它涉及到人、社会和技术，因此，仅仅靠技术是不能有效地实施信息安全保障的。从社会学的观点来看，只有依靠有信息安全觉悟和技能的人及科学有效的管理来实施综合的技术保障手段，才能取得良好的效果。

为了推动我国信息化发展的进程，信息安全国家重点实验室组织编写了《信息安全国家重点实验室信息安全丛书》。在本丛书的编写过程中，我们既注重学术水平，又注意其实用价值。本丛书从信息安全保障体系，操作系统安全，数据库安全，网络安全，无线网络安全，网络攻击，密码技术，PKI 技术，信息隐藏，安全协议，安全事件应急响应，量子密码通信等多个角度，分析和总结信息安全的科学问题以及信息安全保障的理论与技术，因此，这套丛书有较大的适用范围。我们将努力把国内外信息安全的最新研究成果写进书中，以使一些读者阅读本丛书后在理论、方法、技术上有新的启发和收获，从而切实解决工作中的实际问题。

本丛书的组织方式是开放式的，今后将根据学科发展陆续组织出版信息安全领域的优秀图书。

信息安全只能是相对而言，它是动态发展的。任何人都不能宣称自己终极了对信息安全的认识。让我们一起努力，不断地深化自己的研究，借鉴国外先进的科学技术，结合国情，与时俱进地推出信息安全保障的新理论、新办法和新手段，用我们的智慧保卫我们的信息疆土，使我们的信息家园尽量祥和安宁。

限于作者的水平，本丛书难免存在不足之处，敬请读者批评指正。

《信息安全国家重点实验室信息安全丛书》编委会

前　言

密码学是信息安全的核心，应用密码学技术是实现安全系统的核心技术。应用密码学研究如何实现信息的机密性、完整性和不可否认性。随着信息系统及网络系统的爆炸性增长，形形色色的安全威胁严重阻碍了当前的信息化进程，因此，亟待使用密码学来增强系统的安全性。

本书的主要特色是：可读性强、内容全面、选材新颖，力求使学生能够较快掌握应用密码学的的核心内容。

（1）可读性强。学习应用密码学，重点在于掌握基本概念、理论与算法，因此在内容安排上由浅入深、循序渐进、逻辑严密，如先介绍经典密码学，后介绍现代密码学；在语言表达上力求言简意赅，概念准确，如可证明安全、计算上安全等概念。通过必要的实例和算法图示为读者快速地掌握应用密码学的基本知识提供了便利。

（2）内容全面。本书不仅介绍了密码学的经典算法，也介绍了密码学领域的最新标准化算法。例如，在公钥密码体制中，已有的教材仅仅介绍经典的 RSA 算法，这种经典算法存在许多缺陷，不能在实际应用中使用，本书在分析经典的 RSA 的缺陷之后，介绍了 RSA-OAEP 加密标准和 RSA 签名标准 PSS。

（3）选材新颖。本书选材上注意到了密码学领域的最新研究成果，如在分组密码中对我国官方公布的第一个商用密码算法 SMS4 进行了讨论，介绍了线性与差分密码分析，在公钥密码中介绍了基于身份的密码学，此外，第 10 章重点讨论了密码学侧信道攻击的概念和一些攻击模式，此前的国内教材都没有涉及这些内容。

全书共分 11 章。第 1 章主要介绍了密码学的基本概念、密码体制、密码系统的攻击方法及其安全性。第 2 章介绍了几种经典的密码体制，包括替换密码体制、置换密码体制，并对这些密码体制进行了分析。第 3 章介绍了密码学的信息论基础，覆盖了概率论、信息熵、伪密钥、乘积密码体制等内容。第 4 章介绍了序列密码的基本概念、密钥流与密钥生成器、线性反馈移位寄存器序列、线性移位寄存器的一元多项式表示以及随机性伪随机性。第 5 章介绍了 DES、AES、IDEA、SMS4 等分组密码算法的特点、设计原理、实现方法和安全强度，以及分组密码在实际应用中的工作模式。第 6 章与第 7 章介绍了 Hash 函数与消息认证码的需求、特点、一般结构以及相关的安全问题等。第 8 章介绍了公开密钥体制的原理和基本概念、RSA 与 ElGamal 算法原理、计算问题与安全性、椭圆曲

线密码体制的基本原理以及基于身份的密码体制等。第 9 章介绍了数字签名的基本概念和典型的数字签名方案，如 RSA 数字签名和数字签名标准 DSS 的原理与实现，并对离散对数签名体制和椭圆曲线实现的数字签名算法、基于身份的签名方案进行了介绍。第 10 章介绍了侧信道攻击的基本概念和攻击方法，如入侵型攻击、错误攻击、时间攻击、能量攻击、电磁攻击等。第 11 章是密码技术的应用，介绍了身份认证协议、秘密共享、阈下信道、比特承诺以及零知识证明等内容。为贴近教学实际，帮助读者对本章重要知识点的掌握和巩固，每章后面附有相应的习题。

本书可作为高等院校信息安全、信息对抗、计算机科学与技术、数学等专业的本科生及研究生教材，也可供信息安全领域的工程技术人员参考。

由于作者水平有限，书中疏漏与错误之处在所难免，恳请广大同行和读者批评指正。联系方式为：tjcao@cumt. edu. cn，请随时联系获取课程资料。

作　者

2009 年 10 月

目　录

第1章　密码学概述

密码技术是一门古老的技术，大概自人类社会出现战争便产生了密码，它用于保护军事和外交通信可以追溯到几千年以前。但自从密码技术诞生至第二次世界大战结束，对于公众而言，密码技术始终处于一种未知的保密状态，常与军事、机要、间谍等工作联系在一起，让人在感到神秘之余，又有几分畏惧。信息技术的发展迅速改变了这一切，随着计算机和通信技术的迅猛发展，大量的敏感信息通过公共通信设施或计算机网络进行交换。特别是 Internet 的广泛应用、电子商务和电子政务的迅速发展，越来越多的信息需要严格保密，如：银行账号、个人隐私等。正是这种对信息的机密性和真实性的需求，密码学才逐渐揭去了神秘的面纱。

密码学的发展历史大致可分为四个阶段：

第一个阶段是从古代到 1949 年。这一时期通常称为古典密码时期，这时期的密码技术可以说是一种艺术，而不是一种科学，密码学家通常凭直觉和信念来进行密码设计和分析，没有科学的理论基础和推理证明。

第二个阶段是从 1949 年到 1976 年。1949 年 Shannon（香农）发表的“保密系统的信息理论”一文产生了信息论，信息论为对称密码系统建立了理论基础，从此密码学成为了一门科学。但密码学并没有因为科学理论的产生而丧失艺术的一面，一直到今天，密码学仍是一门具有艺术学的科学。

第三个阶段是从 1976 年到 1984 年。1976 年 Diffie 和 Hellman 发表了《密码学新方向》一文，从而导致了密码学上的一场革命。他们首次证明了在发送端和接收端无密钥传输的保密通信是可能的，从而开创了公钥密码学的新纪元。

第四个阶段是从 1984 年至今。1984 年 Goldwasser 和 Micali 首次提出了可证明安全的思想。他们将概率引入了密码学，强调多项式时间和可忽略的成功概率等，认为在公认的计算复杂度理论假设下，安全性是可以证明的。随着对可证明安全性的进一步研究，密码学界意识到它不但对密码学的理论影响重大，且对密码学实践也有重要的意义，目前已成为国内外密码学界最为关注的问题之一，同时可证明安全性也已成为设计密码协议的公认要求。

1.1　密码学的基本概念

研究密码编制的科学称为密码编码学（cryptography），研究密码破译的科学称为密码分析学（cryptanalysis），密码编码学和密码分析学共同组成密码

学(cryptology)。

密码技术的基本思想是伪装信息,使未授权者不能理解它的真实含义。所谓伪装就是对数据进行一组可逆的数学变换。伪装前的原始数据称为明文,伪装后的数据称为密文,伪装的过程称为加密。加密在加密密钥的控制下进行。用于对数据加密的一组数学变换称为加密算法。发送者将明文数据加密成密文,然后将密文数据送入通信网络传输或存入计算机文件,而且只给合法接收者分配密钥。合法接收者接收到密文后,施行与加密变换相逆的变换,去掉密文的伪装恢复出明文,这一过程称为解密。解密在解密密钥的控制下进行。用于解密的一组数学变换称为解密算法。加密算法和解密算法通常都是在一组密钥的控制下进行的,分别称为加密密钥和解密密钥。

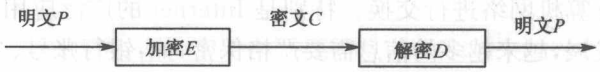

图 1.1 加密和解密

图 1.1 是加密和解密的示意图,通常明文用 P 或 M 表示,密文用 C 表示。加密函数 E 作用于 P 得到密文 C,可以表示为

$$E(P) = C$$

相反的,解密函数 D 作用于 C 产生 P

$$D(C) = P$$

先加密后再解密消息,原始的明文将恢复出来,故有

$$D(E(P)) = P$$

加密时可以使用一个参数 k,称此参数 k 为加密密钥。k 可以是很多数值里的任意值。密钥 k 的可能值的范围叫做密钥空间。如果加密和解密运算都使用这个密钥(即运算都依赖于密钥,并用 k 作为下标表示),如图 1.2 所示。这样,加/解密函数现在变成

$$E_k(P) = C$$

$$D_k(C) = P$$

这些函数具有下面的特性:

$$D_k(E_k(P)) = P$$

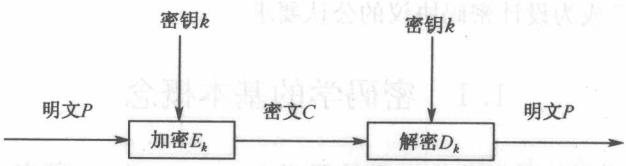

图 1.2 使用一个密钥的加/解密

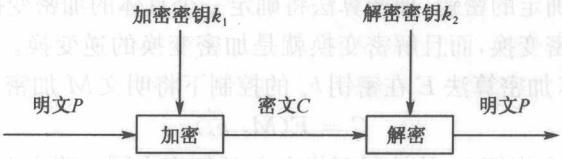

图 1.3　使用两个密钥的加/解密

有些算法使用不同的加密密钥和解密密钥(见图 1.3),即加密密钥 k_1 与解密密钥 k_2 不同,在这种情况下有

$$E_{k_1}(P) = C$$
$$D_{k_2}(C) = P$$
$$D_{k_2}(E_{k_1}(P)) = P$$

1.2　密码体制

一个密码系统,通常简称为密码体制(cryptosystem),由五部分组成(如图 1.4 所示):

1) 明文空间 M,它是全体明文的集合;

2) 密文空间 C,它是全体密文的集合;

3) 密钥空间 K,它是全体密钥的集合,其中每一个密钥 k 均由加密密钥 k_e 和解密密钥 k_d 组成,即 $K=\langle k_e, k_d\rangle$;

4) 加密算法 E,它是一族由 M 到 C 的加密变换;

5) 解密算法 D,它是一族由 C 到 M 的解密变换。

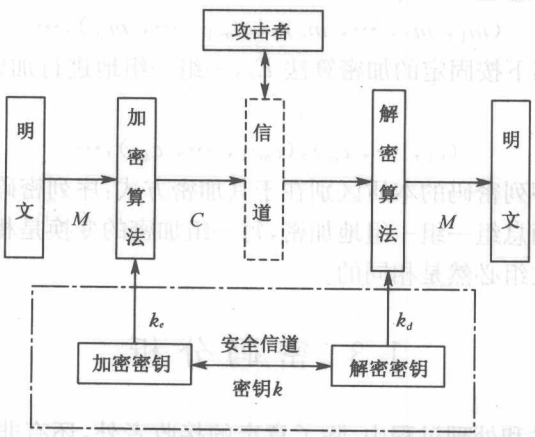

图 1.4　密码体制

对于每一个确定的密钥，加密算法将确定一个具体的加密变换，解密算法将确定一个具体的解密变换，而且解密变换就是加密变换的逆变换。对于明文空间中的每一个明文 M，加密算法 E 在密钥 k_e 的控制下将明文 M 加密成密文 C：

$$C = E(M, k_e)$$

解密算法 D 在密钥 k_d 的控制下将密文 C 解密出同一明文 M：

$$M = D(C, k_d) = D(E(M, k_e), k_d)$$

如果一个密码体制的 $k_d = k_e$，或由其中一个很容易推出另一个，则称为单密钥密码体制或对称密码体制或传统密码体制，否则称为双密钥密码体制。如果在计算上 k_d 不能由 k_e 推出，这样将 k_e 公开也不会损害 k_d 的安全，于是便可将 k_e 公开，这种密码体制称为公开密钥密码体制。公开密钥密码体制的概念于 1976 年由 Diffie 和 Hellman 提出，它的出现是密码发展史上的一个里程碑。

根据对明文和密文的处理方式和密钥的使用不同，可将密码体制分为分组密码和序列密码体制。

序列密码又称为流密码，是将明文消息字符串逐位的加密成密文字符。以二元加法序列密码为例。设

$m_1, m_2, \cdots, m_k, \cdots$是明文字符；

$z_1, z_2, \cdots, z_k, \cdots$是密钥流；

那么

$c_k = m_k \oplus z_k$ 是加密变换；

$c_0, c_1, \cdots, c_k, \cdots$是密文字符序列。

分组密码就是将明文消息序列：

$$m_1, m_2, \cdots, m_k, \cdots$$

分成等长的消息组：

$$(m_1, m_2, \cdots, m_n), (m_{n+1}, \cdots, m_{2n}), \cdots$$

在密钥的控制下按固定的加密算法 E_k，一组一组地进行加密。加密后输出等长的密文组：

$$(c_1, \cdots, c_m), (c_{m+1}, \cdots, c_{2m}), \cdots$$

分组密码和序列密码的本质区别在于其加密方式：序列密码是逐比特加密，而分组密码是按照消息组一组一组地加密，每一组加密的变换是相同的，因而相同的明文组对应的密文组必然是相同的。

1.3 密码分析

在信息的传输和处理过程中，除了意定的接收者外，还有非授权接收者，他们通过各种办法（如搭线窃听、电磁窃听、声音窃听等）来窃取信息。他们虽然不知道