高等学校网络空间安全专业“十三五”规划教材

新编密码学

范九伦　张雪锋　侯红霞　编著

西安电子科技大学出版社
http://www.xduph.com

高等学校网络空间安全专业“十三五”规划教材

新编密码学

范九伦　张雪锋　侯红霞　编著

西安电子科技大学出版社

内 容 简 介

本书系统地介绍了密码学的基本原理、基本算法，并对其安全性进行了相应的分析。全书主要内容包括绪论、基础知识、古典密码、分组密码、序列密码、Hash 函数、公钥密码、数字签名与身份认证、密钥管理和现代密码学发展前沿及应用等。

本书主要作为信息安全、网络工程、计算机科学与技术、通信工程等专业本科高年级学生的教材，也可供相关专业的科技人员参考。

图书在版编目(CIP)数据

新编密码学/范九伦，张雪锋，侯红霞编著. —西安：西安电子科技大学出版社，2018.10
ISBN 978-7-5606-5011-1

Ⅰ. ① 新… Ⅱ. ① 范… ② 张… ③ 侯 Ⅲ. ① 密码学 Ⅳ. ① TN918.1

中国版本图书馆 CIP 数据核字(2018)第 179612 号

策划编辑 陈 婷
责任编辑 曹 锦 陈 婷
出版发行 西安电子科技大学出版社(西安市太白南路 2 号)
电 话 (029)88242885 88201467 邮 编 710071
网 址 www.xduph.com 电子邮箱 xdupfxb001@163.com
经 销 新华书店
印刷单位 陕西天意印务有限责任公司
版 次 2018 年 10 月第 1 版 2018 年 10 月第 1 次印刷
开 本 787 毫米×1092 毫米 1/16 印张 14.5
字 数 338 千字
印 数 1～3000 册
定 价 35.00 元
ISBN 978-7-5606-5011-1/TN
XDUP 5313001-1

高等学校网络空间安全专业“十三五”规划教材

编审专家委员会名单

前言

QIANYAN

密码学有着悠久而神秘的历史，最早的密码技术可以追溯到古罗马时代。1949 年，Claude Shannon 在《Bell System Technical Journal》上发表的论文《Communication Theory of Secrecy Systems》，标志着密码学研究进入了崭新的时代。20 世纪 70 年代以来，分组密码和公钥密码技术得到了迅速发展，取得了丰硕的研究成果，也被广泛应用于信息安全的各个领域。随着互联网技术和计算机技术的发展和普及，越来越多的人认识到密码学的重要性。为了给在校本科生学习密码学提供内容较新、论述较系统的教材，也为了给从事相关领域研究工作的科研人员提供一本内容充实并且具有一定实用性的参考书，我们编写了本书。

本书系统地介绍了密码学的基本原理，在此基础上详细介绍了密码学中的基本算法及其应用。其中内容以当前被广泛应用的密码技术为主，重点放在密码学研究的核心问题上，既突出了广泛性，又注重对主要知识内容的深入讨论。书中对当前被广泛应用的密码算法及其理论基础进行了详细介绍，并对其安全性进行了相应的分析。本书的每一章最后都附有相应的习题，便于读者对书中的内容进行总结和应用。

本书计划教学课时为 48～64 学时，建议根据课时量和授课对象来选择和组织相关内容。学习“密码学”课程的学生需要具备高等数学和线性代数的基础知识，同时应该掌握基本的编程技术和数据结构的基本知识。为了便于读者学习和理解，书中同时介绍了学习密码学需要具备的数论基础知识。对于已经具备相关数论知识的读者，这一部分内容可以作为了解；对于不具备相应数论基础知识的读者，这一部分内容可以作为自学部分。

全书共分 10 章，第 1 章由范九伦编写，第 2、3、4 章由张雪锋编写，第 5、6、7、8、9、10 章由侯红霞编写。全书由范九伦负责整理和统稿。

衷心感谢本书的编审专家，他们提出了许多宝贵的意见和建议，使我们受益匪浅。衷心感谢西安电子科技大学出版社的编辑老师，是他们的辛勤劳动，使本书得以顺利出版。为了使本书既包含密码学的基础知识，又能反映这些基础知识涉及的最新研究

成果，本书在编写过程中参考了国内外许多同行的论文和著作，引用了其中的观点、数据与结论，在此一并表示谢忱。

由于作者学识有限，书中难免有不当之处，敬请广大读者批评、指正。

作者

2018 年 5 月 31 日于西安

目录

MULU

第1章 绪 论

全球信息化的飞速发展，特别是计算机技术与通信技术相结合而诞生的计算机互联网的发展和广泛应用，打破了传统的时间和空间的限制，极大地改变了人们的工作方式和生活方式，促进了经济和社会的发展，提高了人们的工作水平和生活质量。

在信息化日益普及的今天，伴随着信息技术的广泛应用，信息资源不仅成为人们日常工作、学习、生活中的基础资源，而且日益成为国家和社会发展的重要战略资源。国际上围绕信息的获取、使用和控制的竞争愈演愈烈，信息安全已成为维护国家安全和社会稳定的一个焦点，各国都给予极大的关注和投入。在我国，与信息技术被广泛应用形成鲜明对比的是信息安全问题日益突出，目前，我国已经成为信息安全事件的主要受害国之一。中国互联网络信息中心(CNNIC)发布的《2016 年中国手机网民网络安全状况研究报告》表明，虽然多年来我国不断加强信息安全的治理工作，但所面临的信息安全问题仍然十分严重，新型的信息安全事件不断出现，且迅速向更多网民蔓延，导致信息安全事件的情境日益多样和复杂化，信息安全所引起的直接经济损失已达到很大规模，发起信息安全事件的因素已从此前的好奇心理升级为明显的逐利性，经济利益链条已然形成，信息安全事件中所涉及的信息类型、危害类型越来越多，且日益深入涉及网民的隐私，潜在的后果更严重。与此同时，我国广大网民缺乏关于信息安全的知识，对信息安全的危害性并不清楚，采取的信息安全保护措施还未达到较高的水平，很多人尚不具备处理信息安全事件的能力。

目前信息安全已成为亟待解决、影响国家大局和长远利益的重大关键问题之一，它不但是发挥信息革命带来的高效率、高效益的有力保证，而且是抵御信息侵略的重要屏障。信息安全保障能力是 21 世纪综合国力、经济竞争实力和生存能力的重要组成部分，是世界各国都在奋力攀登的制高点。从大的方面来说，信息安全问题已威胁到国家的政治、经济和国防等领域；从小的方面来说，信息安全问题已威胁到个人的隐私等。因此，信息安全已成为社会稳定与安全的必要前提条件。

信息安全不仅要保证信息的保密性、完整性，也就是关注信息自身的安全，防止偶然的或未授权者对信息的恶意泄露、修改和破坏，从而导致信息的泄密或被非法使用等问题，而且还要保证信息的可用性、可控性，保证人们对信息资源的有效使用和管理。

密码技术是信息安全的核心技术，它的发展有着悠久而神秘的历史。当前，掌握核心密码技术是关系到国家信息安全战略成败的关键之一。为了对密码技术的发展和基本概念有一个概要认识，本章将简要介绍密码技术的发展历程，并给出密码技术涉及的相关基本概念和模型。

1.1 概　　述

密码学有着悠久而神秘的历史，人们很难对密码学的起始时间给出准确的定义。一般认为人类对密码学的研究与应用已经有几千年的历史，它最早应用在军事和外交领域，随着科技的发展而逐渐进入人们的生活中。密码学研究的是密码编码和破译的技术与方法，其中通过研究密码变化的客观规律，并将其应用于编制密码，实现保密通信的技术被称为编码学；通过研究密码变化的客观规律，并将其应用于破译密码，实现获取通信信息的技术被称为破译学。编码学和破译学统称为密码学。David Kahn 在他的被称为“密码学圣经”的著作《Kahn on Codes：Secrets of the New Cryptology》中这样定义密码学：“Cryptology，the science of communication secrecy”。

密码学研究的是，对通信双方要传输的信息进行何种保密变换，才能防止未被授权的第三方对信息的窃取。此外，密码技术还可以被用来进行信息鉴别、数据完整性检验、数字签名等。密码学作为保护信息的手段，其发展主要经历了三个阶段。

第一阶段，从古代到 1949 年。这一阶段的加密技术根据实现方式分为手工密码和机器/电子时代两个时期。

在手工密码时期，人们只需通过纸和笔对字符进行加密。密码学的历史源远流长，人类对密码的使用可以追溯到古巴比伦时代。图 1－1 所示的 Phaistos 圆盘是一种直径约为 160 mm 的黏土圆盘，表面有明显的象形文字。该圆盘于 1930 年在克里特岛被人们发现，但一直无法破译那些象形文字。近年有研究学家认为它记录着某种古代天文历法，但真相仍是个谜，只能大致推算出其出现的时间(大约在公元前 1700—公元前 1600 年)。这一时期还产生了另一种著名的加密方式——凯撒密码。为了避免重要信息落入敌军手中而导致泄密，凯撒发明了一种单字替代密码，把明文中的每个字母用密文中的对应字母替代，明文字符集与密文字符集是一一对应的关系，通过替代操作，凯撒密码实现了对字符信息的加密。

图 1－1　Phaistos 圆盘

随着工业革命的兴起，密码学也进入了机器/电子时代。与手工密码操作相比，电子密码机使用了更优秀、更复杂的加密手段，同时也拥有更高的加密与解密效率。其中最具有代表性的就是图 1－2 所示的 ENIGMA 密码机。

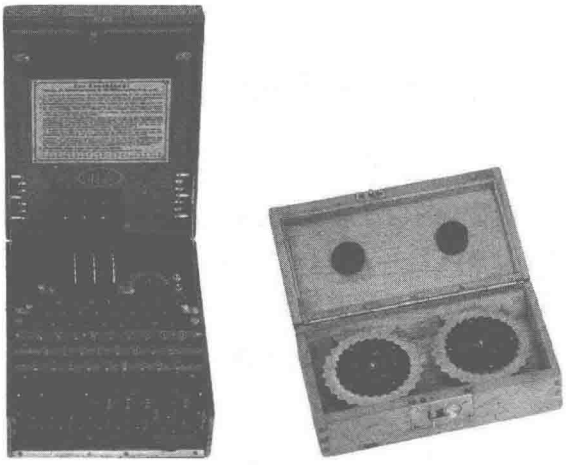

图 1-2 ENIGMA 密码机

ENIGMA 密码机是德国在 1919 年发明的一种加密电子器，它表面看上去就像常用的打字机，但在功能上却与打字机有着天壤之别。其键盘与电流驱动的转子相连，可以多次改变每次敲击的数字；相应信息以摩斯密码输出，同时还需要密钥，而密钥每天都会修改。ENIGMA 密码机被证明是有史以来最可靠的加密系统之一，第二次世界大战期间它开始被德军大量用于铁路、企业领域，令德军保密通信技术处于领先地位。

这个时期的密码技术所使用的加密设备虽然有了很大的进步，但是密码学的理论却没有多大的改变，加密的主要手段仍是简单的替代和换位，而且实现信息加密的过程过于简单，安全性能很差。伴随着高性能计算机的出现，古典密码体制逐渐退出了历史舞台。

第二阶段，从 1949 年到 1975 年。密码学正式作为一门科学的理论基础应该首推 1949 年美国科学家 Shannon 的一篇文章《Communication Theory of Secrecy Systems》。Shannon 在研究保密机的基础上，提出的将密码建立在求解某个已知数学难题的基础上的观点，为近代密码学的研究奠定了理论基础。这一时期有关密码学研究的科技文献难得一见，密码学的研究成果几乎专门服务于军事领域，大量的资源被用来研究如何进行信息保密和破译对方的保密技术，所以大量研究成果不能公开，导致公开的研究文献近乎空白。

第三阶段，从 1976 年至今。这一时期，高性能计算机的出现，使得密码算法进行高度复杂的运算成为可能。20 世纪 70 年代，以公钥密码体制(非对称密码体制，Asymmetric Cryptography System)的提出和数据加密标准 DES 的问世为标志，密码学才在真正意义上取得了重大突破，进入现代密码学阶段。其中，1976 年 Diffie 和 Hellman 发表了研究论文《New Directions in Cryptography》，导致了密码学上的一场革命。在这篇论文中，Diffie 和 Hellman 首先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。现代密码学改变了古典密码学单一的加密手法，融入了大量的数论、几何、代数等专业知识，使密码学得到进一步蓬勃发展。

直到现在，世界各国仍然对密码学的研究高度重视，密码技术已经发展到了现代密码学时期。密码学已经成为结合物理、量子力学、电子学、语言学等多个专业的综合科学，出现了如“量子密码”、“混沌密码”等先进理论。随着计算机技术和网络技术的发展，以及互联网的普及和网上业务的大量开展，人们更加关注密码学，在工作和生活中更加依赖密码

技术，密码技术在信息安全中起着越来越重要的作用。

1.2 保密通信的基本模型

保密是密码学的核心目的。密码学的基本目的是面对攻击者 Oscar，在被称为 Alice 和 Bob 的通信双方之间应用不安全的信道进行通信时，保证通信安全。图 1-3 给出了保密通信的基本模型。

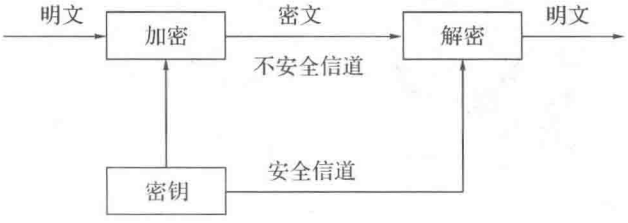

图 1-3 保密通信的基本模型

在保密通信过程中，Alice 和 Bob 也分别被称为信息的发送方和接收方；Alice 要发送给 Bob 的信息称为明文(Plaintext)。为了保证信息不被未经授权的 Oscar 识别，Alice 需要使用密钥(Key)对明文进行加密(Encryption)，加密得到的结果称为密文(Ciphertext)。密文一般是不可理解的。Alice 将密文通过不安全的信道发送给 Bob，同时通过安全的通信方式将密钥发送给 Bob。Bob 在接收到密文和密钥的基础上，可以对密文进行解密(Decryption)，从而获得明文。对于 Oscar 来说，他可能会窃听到信道中的密文，但因为得不到加密密钥，所以无法知道相应的明文。

1.3 密码学的基本概念

在图 1-3 给出的保密通信的基本模型中，根据加密和解密过程所采用密钥的特点可以将加密算法分为两类：对称密码算法(单钥密码算法，Symmetric Cryptography Algorithm)和非对称密码算法(公钥密码算法，Asymmetric Cryptography Algorithm)。

对称密码算法也称为传统密码算法，是指解密密钥与加密密钥相同或者能够从加密密钥中直接推算出解密密钥的加密算法。通常在大多数对称密码算法中解密密钥与加密密钥是相同的，所以这类加密算法要求 Alice 和 Bob 在进行保密通信前，需要通过安全的方式商定一个密钥。对称密码算法的安全性依赖于密钥的管理。

非对称密码算法也称为公钥密码算法，是指用来解密的密钥不同于进行加密的密钥，也不能够通过加密密钥直接推算出解密密钥。一般情况下，加密密钥是可以公开的，任何人都可以应用加密密钥来对信息进行加密，但只有拥有解密密钥的人才可以解密出被加密的信息。在以上过程中，加密密钥称为公钥，解密密钥称为私钥。

在图 1-3 所示的保密通信机制中，为了在接收端能够有效地恢复出明文信息，要求加密过程必须是可逆的。从图中可见，加密方法、解密方法、密钥和消息(明文、密文)是保密通信中的几个关键要素，它们构成了相应的密码体制(Cipher System)。

定义 1.1 密码体制。密码体制的构成包括以下要素：

(1) M：明文消息空间，表示所有可能的明文组成的有限集；

(2) C：密文消息空间，表示所有可能的密文组成的有限集；

(3) K：密钥空间，表示所有可能的密钥组成的有限集；

(4) E：加密算法集合；

(5) D：解密算法集合。

该密码体制应该满足的基本条件是：对任意的 key$\in K$，存在一个加密规则 $e_{key}\in E$ 和相应的解密规则 $d_{key}\in D$，使得对任意的明文 $x\in M$，$e_{key}(x)\in C$ 且 $d_{key}(e_{key}(x))=x$。

在以上密码体制的定义中，最关键的条件是加密过程中 e_{key} 的可逆性，即密码体制不仅能够对明文消息 x 应用 e_{key} 进行加密，而且应该可以使用相应的 d_{key} 对得到的密文进行解密，从而恢复出明文。

显然，密码体制中的加密函数 e_{key} 必须是一一映射的。我们要避免出现在加密时 $x_1\neq x_2$，而对应的密文 $e_{key}(x_1)=e_{key}(x_2)=y$ 的情况，这时在解密过程无法准确地确定密文 y 对应的明文 x。

自从有了加密算法，对加密信息的破解技术应运而生。加密算法的对立面称为密码分析，也就是研究加密算法的破译技术。加密算法和破译技术构成了一对矛盾体，密码学的主要目的是保护通信消息的秘密以防止被攻击。

假设攻击者 Oscar 完全能够截获 Alice 和 Bob 之间的通信，密码分析是指在不知道密钥的情况下恢复出明文的方法。根据密码分析的 Kerckhoffs 原则：攻击者知道所用的加密算法的内部机理，不知道的仅仅是加密算法所采用的加密密钥。常用的密码分析攻击分为以下四类：

(1) 唯密文攻击(Ciphertext Only Attack)。攻击者有一些消息的密文，这些密文都是用相同的加密算法进行加密得到的。攻击者的任务就是恢复出尽可能多的明文，或者能够推算出加密算法采用的密钥，以便可以采用相同的密钥解密出其他被加密的消息。

(2) 已知明文攻击(Know Plaintext Attack)。攻击者不仅可以得到一些消息的密文，而且也知道对应的明文。攻击者的任务就是用加密信息来推算出加密算法采用的密钥或者导出一个算法，此算法可以对用同一密钥加密的任何新的消息进行解密。

(3) 选择明文攻击(Chosen Plaintext Attack)。攻击者不仅可以得到一些消息的密文和相应的明文，而且还可以选择被加密的明文，这比已知明文攻击更为有效，因为攻击者能够选择特定的明文消息进行加密，从而得到更多有关密钥的信息。攻击者的任务是推算出加密算法采用的密钥或者导出一个算法，此算法可以对用同一密钥加密的任何新的消息进行解密。

(4) 选择密文攻击(Chosen Ciphertext Attack)。攻击者能够选择一些不同的被加密的密文并得到与其对应的明文信息，攻击者的任务是推算出加密密钥。

对于以上任何一种攻击，攻击者的主要目标都是为了确定加密算法采用的密钥。显然这四种类型的攻击强度依次增大，相应的攻击难度则依次降低。

随着信息技术的发展和普及，对信息保密的需求将日益广泛和深入，密码技术的应用也将越来越多地融入到人们的日常工作、学习和生活中。鉴于密码学有着广阔的应用前景和完善的理论研究基础，可以相信，密码学一定能够不断地发展和完善，为信息安全提供坚实的理论基础和支撑，为信息技术的发展提供安全服务和技术保障。

习 题 1

1-1 衡量密码体制安全性的基本准则有哪些？

1-2 谈谈密码在实现保密通信中的作用。

1-3 密码学研究的主要问题是什么？

1-4 谈谈你所了解的密码学的应用。

第2章 基础知识

2.1 数论基础知识

在数学中，研究整数性质的一门分支称为数论。数论中的许多概念是设计公钥密码算法的基础，数论领域中的大整数分解、素性检测、开方求根、求解不同模数的同余方程组等问题在公钥密码学中经常遇到，同时它们也是数论中非常重要的内容。作为本书的基础知识，本章将介绍数论中的一些与现代密码学关系密切的基本知识和算法。

2.1.1 素数与互素

1. 整除与素数

如果整数 a、b、c 之间存在关系 $a=b\cdot c$ 且 $b\neq 0$，那么称 b 整除 a 或者 a 能被 b 整除，且 b 是 a 的因子或除数，a 是 b 的倍数，记为 $b|a$。

整除有如下性质：

(1) $a|a$。

(2) 如果 $a|1$，那么有 $a=\pm 1$。

(3) 对于任何 $a\neq 0$，则有 $a|0$。

(4) 如果 $a|b$ 且 $b|a$，那么 $a=\pm b$。

(5) 如果 $a|b$ 且 $b|c$，那么有 $a|c$。

(6) 如果 $a|b$ 且 $b|c$，那么对所有的 x，$y\in\mathbb{Z}$ 有 $a|(bx+cy)$。(这里 $\mathbb{Z}$ 表示整数集，下同。)

根据整除的定义，上述性质(1)～(6)都是显而易见的，在此不再证明。另外，如不做特别说明，所有的量均取整数。

如果 $p\neq\pm 1$ 且 p 的因子仅为 ± 1 和 $\pm p$，那么整数 p 被称为素数或质数。如果只考虑正整数，那么素数就是只能被 1 和它自身整除的整数(1 除外)。非素数的整数被称为合数。但是，1 既不是素数也不是合数。

素数的一些基本结论如下：

(1) 素数有无穷多个。目前尚没有有效的办法来确定所有的素数，迄今所发现的最大素数是 $2^{32\,582\,657}-1$。

(2) 设 p 是素数，$x_i(i=1,2,\cdots,n)$ 是整数，如果 $p|\prod_{i=1}^{n}x_i$，那么至少存在一个 $x_i(i\in\{1,2,\cdots,n\})$能被 p 整除。