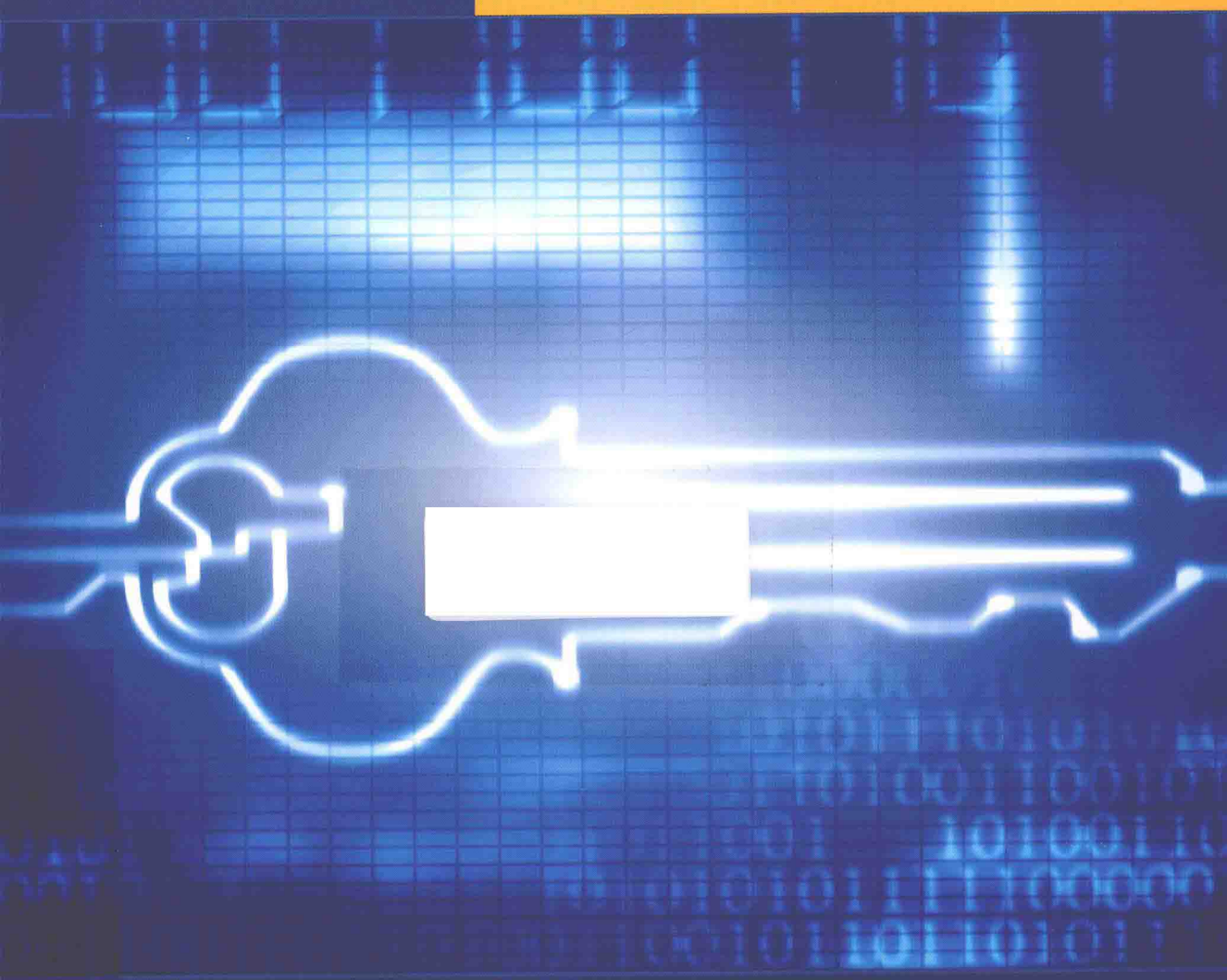
王静文 吴晓艺 编著

密码编码与信息安全

——C++实践



清华大学出版社

王静文 吴晓艺 编著

密码编码与信息安全

——C++实践

清华大学出版社
北京

内 容 简 介

本书主要介绍了密码编码学与信息安全的常用算法所涉及的理论，并介绍了使用C++语言实现这些算法的基本过程与具体实现。本书涵盖了古典密码、对称密钥算法、公钥算法、散列函数和数字签名等几部分内容，并在每章最后附有一定量的习题与实践题供读者练习。

本书可以作为信息安全、信息与计算科学、计算机科学技术、通信工程等专业的本科生教材，也可以为从事信息安全、通信、电子工程等领域的技术人员提供参考。

图书在版编目(CIP)数据

密码编码与信息安全：C++实践/王静文，吴晓艺编著. --北京：清华大学出版社，2015
ISBN 978-7-302-39411-2

Ⅰ. ①密… Ⅱ. ①王… ②吴… Ⅲ. ①密码－加密技术 ②信息安全－安全技术 Ⅳ. ①TN918.4 ②TP309

中国版本图书馆CIP数据核字(2015)第032188号

责任编辑：刘　颖
封面设计：常雪影
责任校对：赵丽敏
责任印制：何　芊

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：北京富博印刷有限公司
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×260mm　　**印　　张**：22.25　　**字　　数**：540千字
版　　次：2015年6月第1版　　**印　　次**：2015年6月第1次印刷
印　　数：1～2500
定　　价：49.00元

产品编号：055283-01

前　言

1. 目的/目标

在密码编码与信息安全的教学与学习过程中，大多以理论教学为主，缺少实践教学，从而对所学的理论难以有较为深入的理解。本书重在以实践帮助读者理解密码编码与信息安全的基本原理。

本书主要讨论密码编码学与信息安全的基本原理，并以基本原理为基础，重在探讨C++的实现方法。通过逐步引导的方法，分析密码编码和信息安全的功能，并针对相应的功能采用C++语言加以实现。帮助读者掌握和理解密码编码与信息安全的原理，并将理论与实践有机结合，为对密码编码和信息安全有兴趣的读者提供参考。

2. 预备知识要求

本书主要讲述密码编码与信息安全的基本原理与实现方法，读者需有基本的C++语言知识，并能够编写简单的应用程序。若有基本的密码编码与信息安全的知识，则更有利于掌握书中的内容。

3. 学习方法

本书是以实践为主，帮助理解密码编码与信息安全的基本原理，从原理出发来分析和完成具体的实现方法与过程是理想的学习方法，切忌复制或抄袭代码，理解后独立完成相关实践内容，不仅有助于理解密码编码的原理，更有助于将理论转化为实践。

在本书的撰写过程中，每一部分的原理都通过分析和实践来完成，同时，将复杂的问题尽可能简化到易于理解，便于实现。读者在学习过程中，可以参考分解问题的方法，提高解决问题的能力。同时在程序设计过程中最好对各项功能进行单独测试，避免在总体完成后增大查找程序存在问题的复杂性。

4. 内容提要

本书共分为古典密码、现代对称密码、公钥密码算法、散列函数和数字签名五个部分，在古典密码中介绍了单表代替密码、移位密码、多表代替密码等古典密码算法。在现代对称密码中介绍了S-DES算法、DES算法、AES算法、IDEA算法、Blowfish算法和CAST-128等多种算法。在公钥密码算法中介绍了大数运算基本原理与实现方法、RSA算法、Diffie-Hellman算法、Elgamal算法等。在散列函数中介绍了MD4、MD5和SHA-1等算法。在数字签名中介绍了RSA数字签名方案、Elgamal数字签名方案和DSA数字签名方案等。并对书中出现的各种算法均给出了C++的具体实现。

5. 教学安排

本书作为教材可以根据教学学时安排具体内容，对于课时在60学时左右的教学计划可以选择大部分内容作为课程教学内容，对于课时在40学时左右的教学计划可以根据需要进行选择。例如：在第2部分内容中可以按照分类各选择一种算法作为教学内容，其中RC算法包含RC4、RC5和RC6算法，教学过程中则可以选择部分内容进行讲解，其余部分则可以作为教学参考。同样第4部分的散列算法也可以选择部分内容进行教学，算法细节不同，但基本结构有不少是相似的。

6. 错误

无论作者有多少发现错误的技巧，总有一些错误漏网，而读者往往最能发现错误，如果读者发现任何认为是错误的地方，请提出纠正建议，并发送电子邮件至 wang_jingwen@yeah.net，我们会非常感谢读者的帮助。

7. 编程环境

本书中的所有示例均采用G++编译器进行编译，编程环境为Code::Blocks，保证了在Windows环境或Linux环境的兼容性，Code::Blocks的下载网址为：http://www.codeblocks.org。若读者在Windows环境中使用VC进行处理，需做相应的修改以适应VC的编译器。

8. 致谢

本书在撰写过程中得到很多人的支持和帮助，特别要感谢何立国教授，对书中许多有关数学知识与相关证明的地方给出了很多宝贵的建议，使得本书更加完善。

编　者

2015年3月

目 录

第 2 部分　现代对称密码

第 4 部分 散 列 函 数

第5部分 数字签名

第1章 概 述

随着网络与通信技术的发展，越来越多的信息通过通信网络、计算机以及电话、传真等技术手段被获取、存储和传输，在信息的处理过程中随时可能受到非法用户或非授权用户的访问、篡改或破坏，信息安全受到人们越来越多的关注和重视，密码编码则是信息安全的重要技术支撑。

1.1 密码学简介

密码学是一门研究信息保密的学科，密码学的基本任务就是通过一定的加密方法对信息提供保密性服务。

确保发送信息安全，同时接收者在获取信息后能正确获得原始信息是密码学的基本内容，这一过程由加密和解密两部分组成。加密通常是将明文进行编码，使其含义变得模糊或不易理解的过程，而解密是加密的逆过程，其作用是将密文变回其原始形式。在一个通信系统中，加密和解密的过程通常可以用图 1-1 所示的模型来表示。

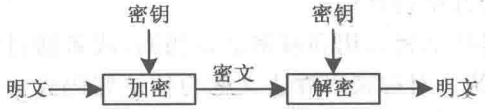


图 1-1 加密-解密基本过程

信息发送方利用加密密钥并采用一定的加密算法，对明文进行加密得到密文，然后将密文发送给接收方。接收方在收到密文之后，利用解密密钥和相应的解密算法将密文进行解密，从而获得原始的信息。在加密和解密过程中，密钥的使用方法又可以分为两类：一类是加密密钥与解密密钥相同，或者通过加密密钥很容易得到解密密钥，这类加密算法被称为单密钥系统；而另一类则是加密密钥和解密密钥不同，通过加密密钥无法或很难计算得到解密密钥，这类加密算法通常被称为双密钥系统。

对于单密钥系统，加密过程和解密过程可以表示为

$$\begin{aligned} C &= E_k(M), \\ M &= D_k(C)。 \end{aligned} \tag{1-1}$$

式中：M 表示明文，C 表示密文，E_k 表示加密密钥，D_k 表示解密密钥，且有 $D_k(E_k(M))=M$。式(1-1)也可以写成

$$C = E(K, M),$$
$$M = D(K, C)。$$

该式表示加密依赖于明文和密钥，解密依赖于密文和密钥，且加密密钥与解密密钥相同。对于双密钥系统，加密过程和解密过程可以表示为

$$C = E_{k1}(M),$$
$$M = D_{k2}(C), \tag{1-2}$$

且有 $D_{k2}(E_{k1}(M))=M$，式(1-2)也可以写成

$$C = E(K_1, M),$$
$$M = D(K_2, C)。$$

该式表示加密依赖于明文和加密密钥，解密依赖于密文和解密密钥，且加密密钥与解密密钥不同。

对称密码算法通常是单密钥系统，公钥密码算法通常是双密钥系统。

在加密和解密过程中包含以下5个基本要素：

(1) 明文——待加密的消息，可以是文本、图片、数字化的语音或数字化的视频等。

(2) 加密算法——是指对明文进行处理的方法或规则，使明文成为“不可理解”的密文。

(3) 密钥——是一种参数，它是在明文转换为密文或将密文转换为明文的算法中输入的数据。

(4) 密文——对明文进行加密后的输出，是不可理解的打乱的信息，通常可以通过算法还原。

(5) 解密算法——解密算法是指对密文进行解密的方法和规则，使密文还原为明文。加密算法和解密算法一般依赖于密钥。

目前所使用的加密算法和解密算法都属于基于密钥的算法，基于密钥的加密算法又可以分为对称密码算法和公开密钥算法。

对称密码算法通常是指加密密钥和解密密钥相同，或者通过加密密钥可以推算出解密密钥的算法，即单密钥系统。对称密码算法又称为传统密码算法，目前，商业上比较有影响力的传统加密算法有DES(数据加密标准)算法、AES(高级加密标准)算法等。对称密码算法的通信模型如图1-2所示。

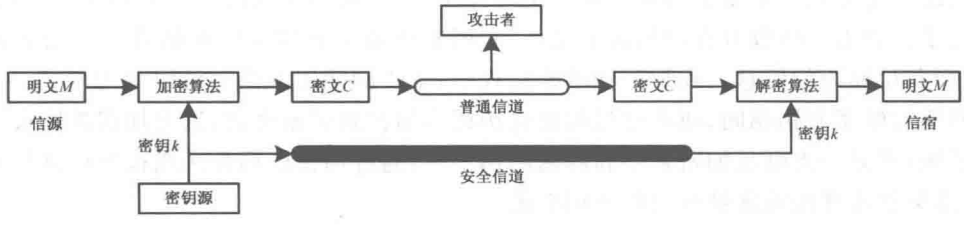


图1-2 对称密码算法通信模型

在使用对称密码算法进行通信的过程中，密钥的传递需要“安全”地进行，若密钥使用普通信道进行传递则很容易受到攻击，当攻击者获得相应密钥之后，“密文”的保密性便不复存在。

公开密钥算法又称为公钥算法，公钥算法通常是指使用一个密钥进行加密，使用另一个密钥进行解密。在公钥算法中，加密密钥一般是公开的，通过加密密钥无法推算出解密密钥或很难推算出解密密钥，公钥系统为双密钥系统。

公钥加密算法也称为非对称密码算法，公钥加密算法不需要加密和解密双方互相信任。目前商业上比较流行的公钥加密算法有 RSA 算法、ECC(椭圆曲线)算法等。公钥密码算法的通信模型如图 1-3 所示。

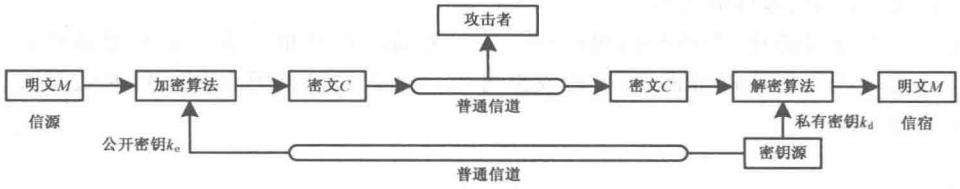


图 1-3 公钥密码算法通信模型

在公钥加密算法中，加密密钥的传递并不需要在一个特殊的安全信道中进行传递，即便攻击者获得加密密钥也无法通过加密密钥计算获得解密密钥，加密密钥可以“公开”，或者在普通的信道内传递加密密钥。

基于明文的加密方法可以分为流加密方法和分组加密方法。

流加密方法通常是对明文每次加密一个字符(或一位数据)，这种加密方法主要在手工加密时代、机械加密时代使用或在语音通信中使用流加密算法，流加密算法具有的最大特点是具有较高的加密速度。

分组加密方法是指将明文分割成一定长度的组，然后使用同一个密钥和算法对每一组明文进行加密，输出的是相应长度的密文。目前使用的对称密码算法通常都是采用分组加密的方法进行加密和解密。

研究对信息进行编码的技术的学科称为密码编码学，其目的是实现对信息的隐蔽和保护。与密码编码学相对应，研究在不知道信息解密方法的情况下进行破解的科学称为密码分析学，有时候也称为破解密码。密码编码学和密码分析学通常是两个对立的学科。

1.2 信息安全遇到的威胁

密码编码与信息安全涉及的范围十分广泛，无论在军事、经济还是在人们的日常生活中，都在不同的程度上与密码编码和信息安全存在一定的联系。

计算机处理的信息主要分为两部分，一部分是计算机内部存储和处理的信息，另一部分是计算机之间互相交换的信息。计算机内部的信息不希望被非法人员访问，可以通过访问权限来限制非法用户读取计算机内部的信息。而计算机之间的信息传递中，传送者和接收者希望能保证传送信息的机密性和完整性。

计算机之间信息传递的安全是信息安全研究的主要内容，而密码编码学则是信息安全的基础。计算机网络的迅速发展也使得信息安全的问题日益突出，信息安全遇到了前所未有的威胁，在信息安全中，威胁通常是指侵犯安全的可能性，即利用安全系统的弱点和潜在危险，在破坏安全或引起危害的环境、行为或事件的情况下，会出现这些威胁。

信息安全中的安全攻击是指任何危害信息安全的活动，对信息的攻击的主要目的是从密文获得明文，更彻底的攻击是获得密钥。信息安全所遇到的威胁包含主动攻击和被动攻击两方面的威胁。

主动攻击是指以各种方式有选择性地进行信息破坏，例如：修改、删除、冒充和传播病毒等。主动攻击具有智能性、隐蔽性、多样性和破坏性的特点。

被动攻击是指在不干扰信息系统正常运行的情况下对计算机内部的信息或计算机通信中的信息进行截取、破译和分析。

主动攻击难以防止，但容易检测，因此，针对主动攻击其重点在于检测并从破坏中得到恢复。被动攻击与主动攻击相反，被动攻击可以防止但难以检测，因此，针对被动攻击其重点在于如何预防。

1.3 密码编码和信息安全提供的服务

密码编码与信息安全主要保障信息的安全利用，提供的服务主要有以下几种：

(1) 机密性

机密性主要是针对私有信息的保护，指一个实体(可以是个人或集体)把自己的数据存放到一个合适的位置，可以方便地读取或存放，而其他未经授权的实体则无法读取和破坏，或未授权用户无法理解信息的内容。

如果信息保存在未被保护的地方，或者信息在不安全的信道内进行传输都存在信息泄密的可能性，信息安全的一个重要任务就是保护信息的机密性，一般采用加密技术来实现机密性保护。

(2) 数据完整性

数据完整性具体体现在对交换信息的保护，指若干个存在利益相关的实体(可以是个人也可以是集体)合作完成相关的交易(或事情)，在交易过程中不被不相关的实体干扰、窃听和破坏。同时又保证各交易方不能进行欺骗或至少不能摆脱对自己行为的责任。

同机密性保护类似，完整性服务的要求同样出现在存储或传输过程中，这时，信息存在被篡改的可能性，在这种情况下，信息安全的任务就是保护信息的完整性。在密码学中可以采用数据加密、报文鉴别和数字签名等技术来实现数据完整性保护。

(3) 鉴别

鉴别通常用于权利保护，是指身份鉴别有关的保护。权利保护的权利是指一个实体利益的知识产权，或代表一个实体责任的控制权限，例如：管理员、负责人的权限被非法盗用，软件、电影以及其他数字产品被盗版。权利保护则使非法人员难以盗用他人权限和盗版，或在盗用后无法去除痕迹，使这些痕迹具有可追踪性。鉴别通常可以通过数据加密、数字签名或鉴别协议等技术来实现。

(4) 抗抵赖

抗抵赖是指用于阻止通信实体的抵赖行为及其相关内容的相关服务。人们为了自身或团体的利益可能抵赖曾经发送过的消息，因此，当消息发送后，接收方需要向他人证实该消息确实是从所声称的发送方发送。抗抵赖一般可以通过数字签名技术或协同可信机构、证书机构来完成相关服务。