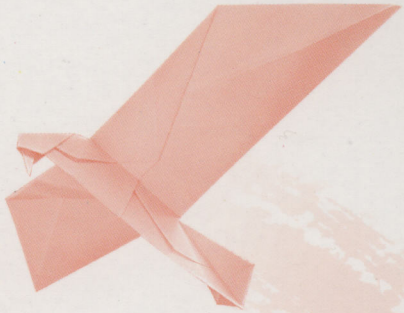
HZ BOOKS

构建安全Java应用的权威经典，5大社区一致鼎力推荐！

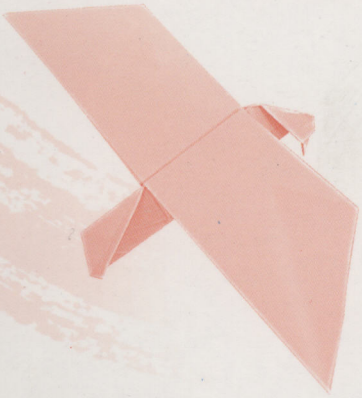
华章原创精品



Java加密与解密的艺术

The Art of Encryption and Decryption about Java

梁栋 著



机械工业出版社
China Machine Press

华章原创精品

Java 加密与解密的艺术

The Art of Encryption and Decryption about Java

梁栋 著

机械工业出版社
China Machine Press

本书是Java安全领域的百科全书，密码学领域的权威经典，5大社区一致鼎力推荐。

全书包含3个部分，基础篇对Java企业级应用的安全知识、密码学核心知识、与Java加密相关的API和通过权限文件加强系统安全方面的知识进行了全面的介绍；实践篇不仅对电子邮件传输算法、消息摘要算法、对称加密算法、非对称加密算法、数字签名算法等现今流行的加密算法的原理进行了全面而深入的剖析，而且还结合翔实的范例说明了各种算法的具体应用场景；综合应用篇既细致地讲解了加密技术对数字证书和SSL/TLS协议的应用，又以示例的方式讲解了加密与解密技术在网络中的实际应用，极具实践指导性。

Java开发者将通过本书掌握密码学和Java加密与解密技术的所有细节；系统架构师将通过本书领悟构建安全企业级应用的要义；其他领域的安全工作者也能通过本书一窥加密与解密技术的精髓。

图书在版编目（CIP）数据

Java加密与解密的艺术/梁栋著. —北京：机械工业出版社，2010.3

ISBN 978-7-111-29762-8

Ⅰ.J…　Ⅱ.梁…　Ⅲ.JAVA语言-保密编码-程序设计　Ⅳ.TP312

中国版本图书馆CIP数据核字（2010）第027465号

机械工业出版社（北京市西城区百万庄大街22号　邮政编码　100037）

责任编辑：李俊竹　　陈佳媛

北京京师印务有限公司印刷

2010年4月第1版第1次印刷

186mm×240mm · 29印张

标准书号：ISBN 978-7-111-29762-8

定价：69.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

客服热线：（010）88378991；88361066

购书热线：（010）68326294；88379649；68995259

投稿热线：（010）88379604

读者信箱：hzjsj@hzbook.com

在如今这个信息化时代，数据是一切应用的核心和基础，有数据存在的地方就会有安全隐患，而密码学则是解决绝大多数安全问题的银弹。

Java作为全球最受欢迎的编程语言，它的应用遍及企业级应用的各个领域，安全是所有企业级应用中最突出、重要的问题。然而，这些问题从来就不是一种武器就能解决的。消息摘要算法用于数据校验、对称加密算法用于数据加密、非对称加密算法用于密钥交换、数字签名算法用于身份验证，等等。若要构建安全、坚固的Java企业级应用，不仅要深入了解每种算法的原理并将它们综合运用，而且还要悟透Java加密与解密技术的本质。

作者简介

梁 栋 资深Java开发者，有丰富的Spring、Hibernate、iBatis等Java技术的使用和开发经验，擅长Java企业级应用开发；安全技术专家，对Java加密与解密技术有系统深入的研究，实践经验亦非常丰富。他还是一位出色的项目经理，是V8Booker（手机电子书）项目的核心开发团队成员之一，负责核心模块的开发；同时他还在V8NetBank（网银系统）项目中担任项目经理，负责系统的架构和核心模块的开发。

Praise 赞 誉

作为一名Java开发者，编写安全的代码比编写优雅的代码更重要，因为安全是一切应用的根本。所有Java开发者都应该全面掌握Java加密与解密的技术，尽可能不让你自己编写的代码给别有用心的人留下可乘之机。如果你是一名Java开发者，强烈建议你阅读并收藏本书，它不仅能作为系统学习Java安全知识之用，还可以作为开发时的参考手册。

——Java开发者社区

作为一名架构师，构建系统时首先应该考虑的就是安全问题。如何才能让你构建的系统坚不可摧，没有安全隐患？掌握加密与解密的技术将会让你在进行系统架构时游刃有余。本书可谓是安全领域的权威经典，是所有Java应用架构师的必备参考手册，强烈推荐。

——架构师社区

本书是目前Java加密与解密领域最全面、最详尽、最前沿的著作之一，它将带领你领略Java安全之美。

——Java中文技术网

密码学是人类最伟大的发明创造之一，是一切安全问题的核心和基础。经过几千年的发展，它在很多行业都发挥着至关重要的作用，尤其是IT领域。本书以通俗的语言，详尽的示例对Java加密与解密的技术进行了详细的阐述，近乎完美。

——Spring开发者社区

对于Java企业级应用开发者而言，加密与解密技术是最重要、最关键的技术之一，必须掌握。本书是Java加密与解密领域的百科全书，不仅内容全面、翔实、实践性强，而且不乏深度。

——51CTO技术博客

前　言 Preface

众所周知，Java EE是目前企业应用中使用最广泛的技术之一，几乎在任何一个领域都能看到Java EE的身影。随着加密与解密算法的发展，Java加密与解密技术不断演进，不断提高着数据的安全性，已成为各大企业应用中一项关键性的技术。

很多企业应用领域的架构师都很关注加密与解密算法在应用中的使用，譬如用户密码加密、网络协议加密等。如何在名目繁多的Java加密与解密技术中选择合适的算法进行企业级应用开发，如何解决Java加密与解密技术开发过程中遇到的各种问题，这成为许多开发者，尤其是架构师关注的焦点问题。然而，国内目前还没有一本书能解决这些问题。本书的作者因工作需要，采用Java加密与解密技术成功构建了企业级网银系统。在开发过程中，作者感受到了Java加密与解密技术的精妙。作者希望把Java加密与解密技术在企业应用开发领域的经验和心得分享给广大读者，提升企业应用的安全性。

本书面向的读者

本书主要适合以下读者：

❑ 所有利用Java进行企业级应用开发的软件工程师

对于企业级应用软件工程师来讲，这将是一次系统的密码学之旅。本书将介绍密码学理论、Java相关算法实现、开源组件包介绍、数字证书与安全协议等相关内容，并配有相关实例为读者提供详尽实现指导，为构建企业级安全应用提供完整的技术支持。

❑ 系统架构师

对于系统架构师来讲，如何使用成熟技术快速构建安全企业应用是安全工作的第一要务。在算法方面，本书详述了Java 6对于密码学算法的相关实现，针对AES算法密钥长度受限问题给出解决办法。同时，针对当前Java 6不支持的算法，如SHA224、ElGamal和ECDSA等，本书详细介绍如何使用第三方开源加密组件包Bouncy Castle进行相关算法实现补充，并且还详细介

绍了Apache Commons Codec，这些成熟的组件包都是构建安全企业应用必不可少的工具包。在架构方面，本书浓墨重彩地介绍了数字证书的构建、SSL/TLS协议服务搭建，并通过相关实例介绍如何构建单向/双向认证服务。

❑ 其他安全领域的软件工程师

如今企业级应用已经逐步转变以服务为主的异构体应用，如Web Service应用等。Java加密算法实现遵循密码学相关国际标准，完全可以与其他计算机语言（如C++、C#等）构建的异构体应用进行数据加密交互。本书为读者选择合适的算法并提供详尽的技术实现。

如何阅读本书

全书共分为3个部分：基础篇、实践篇、综合应用篇。

❑ 基础篇

本篇共包含4个章节，主要对Java企业级应用安全、密码学理论和Java中与加密相关的API进行了详细介绍，并详细阐述了第三方组件包Bouncy Castle和Apache Commons Codec相关的API。

第1章主要阐述了当前的安全问题，并给出了安全的相关标准。本书将在后续章节内通过各个算法介绍逐一实现这些标准，这些标准也是评判系统安全级别的准则。

第2章主要详述了密码学相关理论知识，并回顾密码学的发展历程。未曾接触过密码学的读者，可通过本章了解密码学理论的基础，本书将在后续章节中多处应用该章相关技术名词。

第3章详细阐述了Java 6安全领域相关API内容，为读者详尽介绍每一个与密码学相关的类以及方法。该章将是每位安全领域软件工程师必读的内容，在阅读本书的后续章节时需经常翻阅该章内容。

第4章主要介绍如何通过权限文件加强系统安全级别，并详述开源组件Bouncy Castle和Apache Commons Codec相关的API内容。如果您正苦于AES算法密钥长度受限，SHA224、ElGamal、ECDSA等算法缺少支持等问题，那么请您阅读该章；如果您非常希望找到Base64及十六进制编码算法的成熟开源组件，也请您阅读该章。本书将在后续章节中介绍如何使用这些开源组件并实现相关算法。

❑ 实践篇

这篇主要对现今流行的所有加密算法进行了全面阐述和深入剖析，并配合相关测试用例演示算法实现。在阅读这篇前，请阅读本书第2章相关理论知识，并了解第3～4章相关的API内容。

这篇将是所有企业级应用Java软件工程师的必读内容。

第5章介绍了极为简单的Base64算法，该算法可以作为加密算法的入门算法。如果仅仅需要确保应用交互之间的数据达到隐藏的目的，那么您在第5章中一定可以找到满意的答案。

第6章主要详述了MD系列、SHA系列以及MAC系列三大消息摘要算法相关实现。并详细介绍如何使用Bouncy Castle构建Java 6所不支持的算法实现。对于一般网络应用，经常需要为下载软件提供对应的摘要信息用于校验文件完整性。相信在阅读这章内容后，您可以熟练地使用Apcahe Commons Codec为应用实现校验文件完整性的需求。

第7章将沿着对称加密算法的发展历程，详述DES、DESede、AES和PBE四大算法的实现细节。并详细介绍如何使用Bouncy Castle构建目前较为常用的IDEA算法。这些算法适用于中小型企业级应用网络数据加密交互需求，同时也适用于其他安全领域的相关需求，是应用最为广泛的加密算法，更是密码学领域的的核心算法。如果仅仅想要通过对称加密算法以及消息摘要算法构建简单的加密网络应用，那么该章提供的实例将非常合适。

第8章主要详述了构建于对称加密算法之上的非对称加密算法，包括DH、RSA和ElGamal三大常用算法。该章是本书后续章节内容的基础，数字签名算法、数字证书、安全协议等内容都与该章内容息息相关，请在阅读后续章节前能够对该章内容有较深入的阅读。如果对单向/双向认证服务底层实现非常有兴趣，并想要知道它的来龙去脉，那么该章就是探究该技术旅途上的第一个驿站。

第9章详述了基于消息摘要算法和非对称加密算法之上的数字签名算法，包括RSA、DSA和ECDSA三大常用算法。数字签名算法是消息摘要算法的延续，是单向/双向认证服务核心认证技术。如果想通过非对称加密算法构建简单的网络加密应用，并期望使用数字签名算法对数据进行校验，那么该章的实例将非常合适。

❑ 综合应用篇

这篇不仅细致地介绍了加密技术对数字证书和SSL/TLS协议的应用，而且还以示例的方式讲解了加密解密技术在实际网络中的各种应用，极具实践指导性。请在阅读这篇前仔细阅读实践篇的相关内容。这篇内容将是系统架构师的最爱。

第10章详细介绍了如何使用KeyTool和OpenSSL两大工具进行数字证书管理，并详细介绍如何在Java中使用数字证书。数字证书是非对称加密算法公钥的载体，是SSL/TLS协议和单向/双向认证服务基础。如果想要构建安全的HTTPS网络服务应用，请先阅读该章内容。

第11章主要介绍了SSL/TLS协议及单向/双向认证服务。这将是探究单向/双向认证服务技术旅途上的最后一站。该章将详述如何通过简单配置Tomcat服务器快速构建单向/双向认证服

务，内容详实、极具实践性。

第12章是本书的实例集合，通过三套网络应用实例揭示常规网络应用安全、即时通信网络应用安全和以数据交互为主的Web Service应用安全，并通过网络监测工具WireShark对其效果进行检测。通过不同算法的组合，三套实例逐步升级自身系统的安全级别，极具指导意义。该章为解决网络安全问题提供了可行性参考。

通过阅读本书，读者不仅能全面掌握Java加密与解密的各种基础知识，而且还能进一步了解Java加密与解密的高级技术和技巧，从而将这些知识都运用到实际开发中去。

目　录 Contents

Part1 第一部分

基 础 篇

第1章

企业应用安全

当计算机将我们包围、当网络无处不在时，安全问题也成为我们日益关心的问题。我们依赖于网络，同时又受限于网络，而网络本身却是不安全的！如今越来越多的企业应用都架设在网络平台之上，虽然能为用户提供更快捷和便利的服务支持，但这些服务支持也越来越庞大。与此同时，为了满足用户日益增长的服务需求，企业应用不断在如何提供更好的服务支持和更大信息量的传输方面加大技术投入。而与此失衡的是，企业应用的安全性却未能受到足够的重视。单凭用户名和口令鉴别用户身份，继而授权用户使用的方式难以确保数据的安全性。

1.1 我们身边的安全问题

安全，似乎是个问题。但是，我们觉得这个话题似乎不是那么关键！通常情况下，我们为用户提供用户名和口令验证的方式就可以避免这个问题，但这不是最佳答案，因为这样做是远远不够的。安全隐患无处不在，还是先来看看我们所处环境的安全状况吧！

❑ 存储问题

闪存芯片的快速革命使得移动存储行业发生了质的变化，各种数据存储在各种不同的移动存储设备上。当一部优盘塞满了公司的年度报表、下一年企划策略等各种商业机密后，突然不翼而飞时，我们才会猛然惊醒——优盘中的数据没有任何安全措施，甚至连口令都没有！

❑ 通信问题

我们习惯于通过IM工具与好友聊天、交换心情、透漏隐私，甚至通过IM工具与合作公司交换公司私密数据！当你的隐私成为公共话题，当你的公司的商业数据被曝光，你突然发现原来IM工具是不安全的！没错，不管是哪一种IM工具，都在不遗余力地告诫用户聊天信息可能被盗取，“安全提示：不要将银行卡号暴露在您的聊天信息中！”相信大家都不会对这条提示信息感到陌生。

❑ B2C、B2B交易问题

到邮局排队汇款的日子已经一去不复返了，取而代之的是网上银行，轻松地点击一下按钮就能顺利完成转账的操作。网上银行的确为我们的生活带来了便利，但是，如果我们有被钓鱼网站骗取银行卡号和密码的不幸遭遇，现在想起来是不是仍然心有余悸？难道没有一种办法能

确保我们输入的信息被发送到安全的地方吗？

❑ 服务交互问题

随着大型应用对交互性的需求越来越高，这些应用之间的数据交互也越来越频繁，甚至是大批量、高负荷的数据交互。当你公司的应用通过Web Service接口与合作伙伴交互数据的时候，你该如何确定对方就是你所信赖的合作伙伴呢？你的Web Service接口安全吗？

❑ 移动应用服务问题

3G时代已经来临，在不远的某一天，你将完全可以通过手机完成现在只能通过PC完成的事情。视频聊天、B2C购物、银行转账，等等。3G时代预示着智能手机将无所不能！其实手机也是计算机，只不过它与你熟悉的PC在体积上有较大的差别而已。3G手机一样要通过网络完成你要执行的操作，将平台由PC转换为手机，并不能保证手机平台就能比PC平台有着更高的安全性！

用手机在WAP网站上下载一款软件，是再平常不过的事情了。但是，如何避免用户因不够信任该软件而取消下载呢？下载后，手机如何鉴别这个软件是安全的呢？如何避免发布的软件在被客户成功下载之前被篡改呢？

❑ 内部人为问题

前面列举的问题都来源于外部，我们往往忽略了内部人为问题。现在的企业应用都能为用户提供用户名和口令来确保用户的数据安全，但很多时候用户名和口令在数据库中却一目了然，甚至有的是以明文方式存储的！企业内部任何能访问数据库的员工都能轻而易举地盗取用户的用户名口令，冒充用户的身份完成各种合乎用户行为的操作，侵害用户的利益。企业因此被用户投诉之后，却又找不到任何蛛丝马迹。

当我们的利益受到侵犯时我们才会想起安全问题，安全原来如此重要！一不小心，你的企业应用就会因为数据泄露而丧失良机、引发投诉，甚至是巨额赔款！安全问题关系着企业的生死存亡！

1.2 拿什么来拯救你，我的应用

“拿什么来保护你，我的应用？”这几乎是每一位架构师和安全工作者所关注的问题。看了上面那么多让人不寒而栗的安全问题，免不了让我们心里发怵。道高一尺，魔高一丈，我们先来看看有什么武器可以应对企业应用的安全问题。接下来会讨论安全技术目标、OSI安全体系结构与TCP/IP安全体系结构这三方面的内容。

1.2.1 安全技术目标

国际标准化组织（ISO）对“计算机安全”的定义为：“为数据处理系统建立和采取的技术和管理的安全保护，保护计算机硬件、软件数据不因偶然和恶意的原因而遭到破坏、更改和泄露。”根据美国国家信息基础设施（NII）提供的文献，安全技术目标包含保密性（Confidentiality）、完整性（Integrity）、可用性（Availability）、可靠性（Reliability）和抗否认性（Non-Repudiation）。