HZ BOOKS
华章科技

经典著作全新升级，第1版4年来畅销不衰，繁体版在台湾出版，大陆和台湾的读者都给予了极高的评价

Java安全领域公认的标杆之作，资深专家撰写，全面介绍Java 7中与安全相关的各种API和工具，深入剖析现今流行的各种加密算法及其应用，包含多个前沿的应用案例，实践性强

华章原创精品

第2版

Java 加密与解密的艺术

The Art of Encryption and Decryption about Java

Second Edition

梁栋 著

机械工业出版社
China Machine Press

华章原创精品

第2版

Java 加密与解密的艺术

The Art of Encryption and Decryption about Java

Second Edition

梁栋 著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

Java加密与解密的艺术 / 梁栋著. —2版. —北京：机械工业出版社，2014.1
（华章原创精品）

ISBN 978-7-111-44678-1

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（2013）第264025号

本书是Java安全领域公认的标杆之作，被奉为每一位Java开发工程师必读的著作之一。由资深专家撰写，第1版4年来畅销不衰，繁体版在台湾出版，大陆和台湾的读者都给予了极高的评价。第2版根据Java 7全面更新，不仅新增了很多重要的内容，而且对第1版中存在的瑕疵和不足进行了完善，使得本书内容更为详尽、更加与时俱进，能更好地满足广大Java企业级应用开发工程师和系统架构师的需求。

全书共12章，分为3个部分：基础篇（第1~4章）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（第5~9章）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，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（第10~12章）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/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。

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：孙海亮
藁城市京瑞印刷有限公司印刷
2014年1月第2版第1次印刷
186mm × 240mm · 31.75印张
标准书号：ISBN 978-7-111-44678-1
定 价：89.00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 投稿热线：（010）88379604
购书热线：（010）68326294 88379649 68995259 读者信箱：hzjsj@hzbook.com

前　言

为什么要写这本书

当你在用IM与好友聊天时，当你通过B2C网站购物时，当你用邮件与客户交流时，当你公司的应用服务器与合作伙伴交换商业数据时……你是否考虑过你的数据是否安全？你的隐私是否会泄露？你的银行卡是否会被盗用？你的竞争对手是否能破解你的敏感数据？

任何一项通过网络交互的数据都有可能是不安全的，而我们却越来越依赖于网络。用户密码、聊天消息、银行卡号、邮件信息、商业敏感数据，如果通过明文传输，后果不堪设想。自己的账号被盗用、隐私成为公共话题、信用卡被人滥用、竞争对手盗用自己的数据……于是，为了确保数据不被侵犯，数据加密与解密技术应运而生，成为众多应用中的一项核心技术。

众所周知，Java EE是目前企业应用中使用最广泛的语言之一，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，例如用户密码加密、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加密与解密技术在开发过程中遇到的各种问题，成为许多开发者，尤其是架构师关注的焦点问题。然而，国内目前还没有哪一本书能解决这些问题。笔者因工作需要，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，笔者感受到了Java加密与解密技术的精妙。笔者希望把自己Java加密与解密技术运用在企业应用开发领域的经验和心得分享给广大读者，以帮助大家掌握提升企业应用的安全性的方法。

本书面向的读者

本书主要适合于以下读者：

(1) 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。本书将为您介绍密码学理论、Java相关算法实现、开源组件包、数字证书与安全协议等相关内容，并配有相关实例为您提供详尽实现指导，为您构建企业级安全应用提供完整的技术支持。

(2) 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 7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 7不支持的算法，如SHA224、ElGamal和ECDSA等，本书详细介绍了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，并且对Apache Commons Codec进行了详尽的介绍。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。

(3) 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为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算法及实现提供了详尽的技术支持。

如何阅读本书

全书一共分为3个部分：基础篇、实践篇、综合应用篇。

(1) 基础篇

本篇共包含4章，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及与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。本书将在后续章节中通过各个算法介绍逐一实现这些标准，这些标准同样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。如果您不曾接触过密码学，本章将是您了解密码学理论的基础教程。本书后续章节会多处应用本章介绍的相关技术名词。

第3章主要详述了Java 7安全领域相关API内容，为您详尽介绍每一个与密码学相关的类以

及方法。本章将是每位安全领域软件工程师必读内容，您将在阅读本书的后续章节时经常翻阅本章内容。

第4章主要介绍了如何通过权限文件加强系统安全级别，并详述了开源组件Bouncy Castle及与Apache Commons Codec相关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，那么请您阅读本章；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，也请您阅读本章。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。

（2）实践篇

本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。在阅读本篇前，请阅读第2章相关理论知识，并了解第3～4章相关API内容。本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入门算法。如果您仅需要确保应用交互的数据可以达到隐藏的目的，那么在第5章中您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，并详细介绍了如何使用Bouncy Castle构建Java 7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以校验文件完整性。相信在阅读完本章后，您便可熟练使用Apache 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，详述了DES、DESede、AES和PBE四大算法的实现细节，并详细介绍了如何使用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相关需求，是应用最为广泛的加密算法，更是密码学领域的核心算法。如果您仅想通过对称加密算法及消息摘要算法构建简单的加密网络应用，那么本章提供的实例将非常适合您。

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。本章是本书后续内容的基础，数字签名算法、数字证书、安全协议等内容都与本章内容息息相关，请您在阅读后续章节前仔细阅读本章。如果您对单向/双向认证服务底层实现非常感兴趣，并想要知道它的来龙去脉，那么本章就是您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。如果您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，那么本章的实例将非常适合您。

（3）综合应用篇

本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，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。请您在阅读本章前仔细阅读实践篇相关内容。本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，并详细介绍了如何在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/双向认证服务的基础。如果您想要构建安全的HTTPS网络服务应用，请先阅读本章。

第11章主要介绍了SSL/TLS协议及单向/双向认证服务。这将是您探究单向/双向认证服务技术旅途上的最后一站。本章详述了如何通过简单配置Tomcat服务器快速构建单向/双向认证服务，内容翔实、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。您将在本章找到解决网络安全问题的可行性参考。

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，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。

新版变更说明

对比上一版本，在新版中主要对JDK、Bouncy Castle等进行了版本更新，补充了新版本中特有的算法实现与实例，并对上一版中存在的疏漏进行了修正。新版内容基于Java 7，对比Java 6其在安全性上有所提升。新增了EC算法安全提供者，同时增加了用于EC密钥构建的API等。根据笔者的观察，种种现象预示着在Java SE后续版本中可能会进一步增强EC系列算法的相应实现，如ECDH算法等。同时，一些只能在Bouncy Castle中才能实现的算法，正被Java SE 7所蚕食，如SHA256withRSA算法等。在新版中引入了Bouncy Castle 1.49，扩展了对于OpenSSL的PEM文件操作实现等。同时，应读者需求，新版中补充了OpenSSL在Base64、消息摘要方面的操作运用。

读者约定

本书内容主要基于Java 7，书中的代码实现请参考相关API。

在本书中，我们用环境变量%JDK_HOME%来表示JDK的安装路径，用环境变量%JRE_HOME%来表示JRE的安装路径。如将JDK安装在C:\java\jdk目录下，变量%JDK_HOME%则指向该目录。相应的，如将JRE安装在C:\ java \jre目录下，变量%JRE_HOME%则指向该目录。

本书代码演示所使用的IDE为Eclipse。

阅读本书前，我们约定您已了解了以下内容：

（1）测试组件包——JUnit

本书将通过测试工具JUnit，以白盒测试的方式演示如何使用Java完成相应的加密与解密操作。

本书将使用JUnit 4.5版本，以注解的方式构建白盒测试。读者可通过其官方网站（http://www.junit.org/）下载最新版本。

（2）编码组件包——Commons Codec

Commons Codec（http://commons.apache.org/codec/）是一款开源编码组件，它位于国际开源组织Apache（http://www.apache.org/）旗下。它对Java API做了进一步封装，用于Hex、Base64编码增强实现。本书中使用的版本为1.4。读者朋友可通过其官方网站下载最新版本。

（3）加密组件包——Bouncy Castle

Bouncy Castle（http://www.bouncycastle.org/）是一个开源加密组件。它提供了多种Java API所不支持的算法实现，如消息摘要算法MD4和SHA224、对称加密算法IDEA、数字签名算法ECDSA等。本书中使用的版本为1.49。

（4）网络监听工具——WireShark

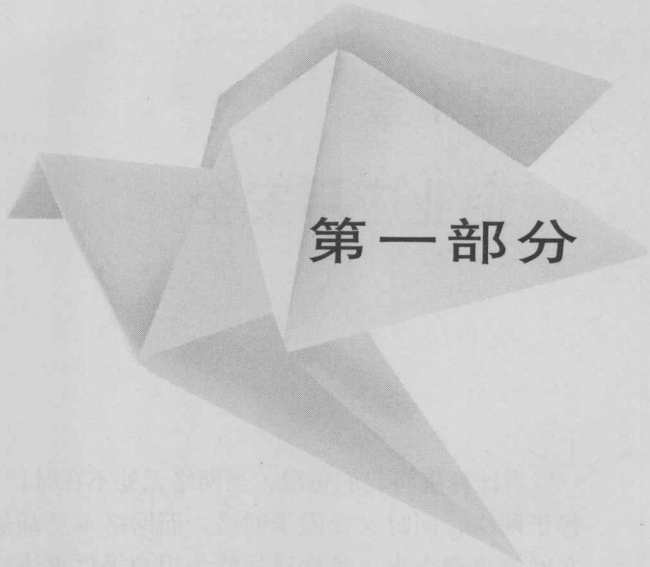
本书将通过网络监听工具WireShark完成对网络数据的监控，请读者参考相关文档。读者可通过其官方网站（http://www.wireshark.org/）下载最新版本。

（5）密码&证书管理工具——OpenSSL

OpenSSL（http://www.openssl.org/）是一个基于命令行密码&证书管理工具，可用于密钥的生成、加密/解密、签名/验证、数字证书管理等。

目 录

第二部分 实践篇



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，安全问题成为了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，虽然这样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，我们通过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：闪存芯片的快速的、革命性的发展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。当塞满了公司的年度报表、下一年企划策略等各种商业机密的优盘突然不翼而飞时，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时，或当你的公司的商业数据被曝光时，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，那么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，如视频聊天、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和口令，然后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，甚至是付出巨额赔款！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

“拿什么来拯救你，我的应用？”这几乎是每一位架构师和安全工作者都会关注的问题。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。魔高一尺，道高一丈，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）。

- **保密性**：又称机密性。保密性确保数据仅能被合法的用户访问，即数据不能被未授权的第三方使用。
- **完整性**：主要确保数据只能由授权方或以授权的方式进行修改，即数据在传输过程中不能被未授权方修改。
- **可用性**：主要确保所有数据仅在适当的时候可以由授权方访问。
- **可靠性**：主要确保系统能在规定条件下、规定时间内、完成规定功能时具有稳定的概率。
- **抗否认性**：又称抗抵赖性，主要确保发送方与接收方在执行各自操作后，对所做的操作不可否认。

除此之外，计算机网络信息系统的其他安全技术目标还包括：

- **可控性**：主要是对信息及信息系统实施安全监控。
- **可审查性**：主要是通过审计、监控、抗否认性等安全机制，确保数据访问者（包括合法用户、攻击者、破坏者、抵赖者）的行为有证可查，当网络出现安全问题时，提供调查依据和手段。
- **认证（鉴别）**：主要确保数据访问者和信息服务者的身份真实有效。
- **访问控制**：主要确保数据不被非授权方或以未授权方式使用。

安全技术目标制定的主旨在于预防安全隐患的发生。安全技术目标是构建安全体系结构的基础。

1.2.2 OSI安全体系结构

OSI参考模型是由国际标准化组织制定的开放式通信系统互联参考模型（Open System Interconnection Reference Model，OSI/RM）。OSI参考模型包括网络通信、安全服务和安全机制。网络通信共分七层，按照由下至上的次序分别由物理层（Physical Layer）、数据链路层（Data Link Layer）、网络层（Network Layer）、传输层（Transport Layer）、会话层（Session Layer）、表示层（Presentation Layer）和应用层（Application Layer）构成。其中，数据链路层通常简称链路层。国际标准化组织于1989年在原有网络通信协议七层模型的基础上扩充了OSI参考模型，确立了信息安全体系结构，并于1995年再次在技术上进行了修正。OSI安全体系结构包括五类安全服务以及八类安全机制。

OSI参考模型结构如图1-1所示。

五类安全服务包括认证（鉴别）服务、访问控制服务、数据保密性服务、数据完整性服务和抗否认性服务。

- **认证（鉴别）服务**：在网络交互过程中，对收发双方的身份及数据来源进行验证。
- **访问控制服务**：防止未授权用户非法访问资源，包括用户身份认证和用户权限确认。
- **数据保密性服务**：防止数据在传输过程中被破解、泄露。
- **数据完整性服务**：防止数据在传输过程中被篡改。