<<Java加密与解密的艺术>>

图书基本信息

书名：<<Java加密与解密的艺术>>

13位ISBN编号：9787111297628

10位ISBN编号：7111297628

出版时间：2010年4月

出版时间：机械工业出版社

作者：梁栋

页数：450

<<Java加密与解密的艺术>>

前言

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。

<<Java加密与解密的艺术>>

内容概要

本书是Java安全领域的百科全书，密码学领域的权威经典，4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。

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人员之一

<<Java加密与解密的艺术>>

书籍目录

章节摘录

插图：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。

媒体关注与评论

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。
——Ajax中国

编辑推荐

《Java加密与解密的艺术》：构建安全Java应用的百科全书和权威经典,5大社区推荐！
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？
你的隐私是否会被泄露？
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。
如果用户密码、聊天消息、银行账号、邮件信息、商业敏感数据等通过明文传输，后果将不堪设想。
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在企业应用中都扮演着非常重要的角色。
如果你在思考下面这些问题，也许《Java加密与解密的艺术》就是你想要的！
·作为一名系统架构师，如何让你的系统不留有安全隐患？
作为一名程序员，如何让你编写的代码没有安全漏洞？
·为什么密码学是解决一切安全问题的银弹？
密码学究竟是怎样一门学科？
近千年来，它经历了怎样的发展历程？
它是如何延续至今并逐步发展壮大的？
·博客、论坛、社区、网络聊天、企业级数据交互应用、网银平台等网络应用都无法逃避网络安全问题，如何在合适的环节选用合适的加密算法。
从而提高系统的安全性？
·Java 6支持哪些加密算法？
如何扩充Java 6尚不支持的加密算法？
如何增强系统的安全级别？
·消息摘要算法和文件校验算法有什么关联？
它与普通的循环冗余校验算法有何差别？
如何使用消息摘要算法隐蔽敏感信息？
·为何Base64算法可以隐蔽敏感信息但却无法真正起到数据加密的作用，而对称加密算法却能轻而易举地起到数据加密的作用？
Base64算法与对称加密算法之间究竟有何关系？
·Sun并没有提供官方的Base64算法支持。
我们又该如何构建该算法？
针对Base64算法，Apache Commons Codec和BO Lracy Castle提供了怎样的支持？
在其他加密算法中又起到了怎样的作用？
·对称加密算法已经几乎能胜任所有的加密需求，为何要研制非对称加密算法？
对称加密算法究竟有何弊端？
非对称加密算法会是对称加密算法的替代者吗？
·数字签名是手写签名的数字化产物，其算法与消息摘要算法有何关联？
为什么这种算法在结合非对称加密算法密钥后就具备了认证身份的作用？
·对称加密算法和非对称加密算法如何分发密钥，数字证书在其中充当了何种角色？
数字证书又是如何发放的？
·数字证书集多种加密算法于一身，它是如何传递密钥的？
又是如何起身份认证作用的？
在HTTPS协议中又是如何与SSL/TLS协议相结合构建安全平台的？
·Key Tool和Open SSL构建的数字证书究竟有何差别？
如何在Java中使用这些工具构建的数字证书？

·基于HTTPS协议的网银平台，堪称安全级别最高的网络应用，更是密码学应用领域最为成功的案例。
Java6提供了完备的HTTPS协议相关的API，如何使用这些API构建固若金汤的HTTPS平台？
·HTTPS协议和SSL/TLS协议是何关系？
这些协议与数字证书、加密算法有何关联？
如何使用HTTPS协议构建安全的网络应用？
·单向认证服务和双向认证服务两者之间有何不同？
它们与HTTPS协议有何关系？
如何运用这两种认证服务保护我们的应用？
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。

<<Java加密与解密的艺术>>

版权说明