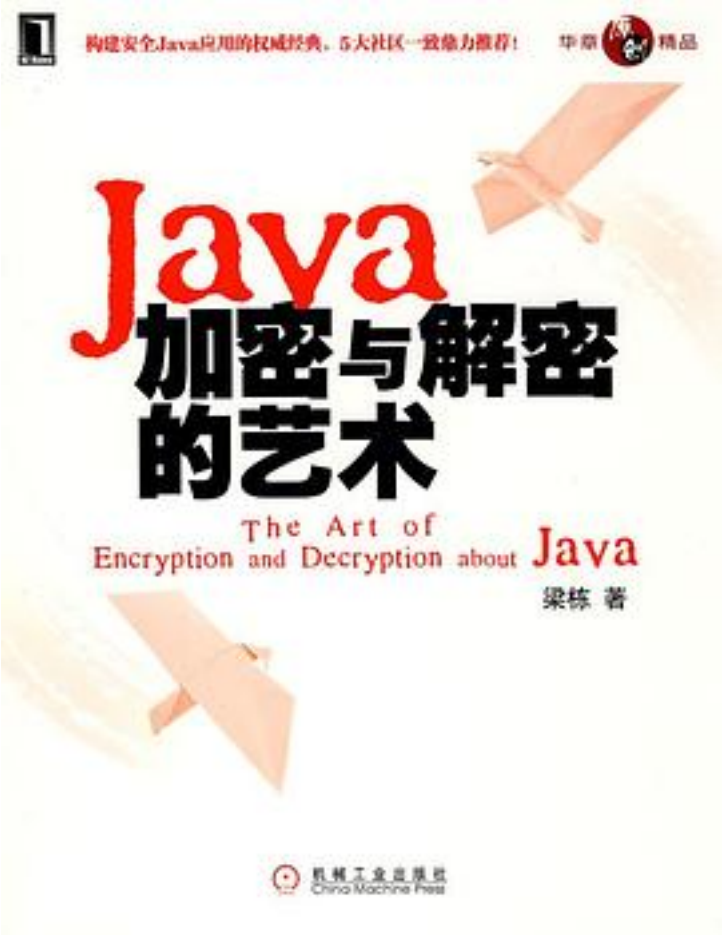
Java加密与解密的艺术



Java加密与解密的艺术_下载链接1_

著者:梁栋

出版者:机械工业出版社

出版时间:2010-4

装帧:平装

isbn:9787111297628

Java安全领域的百科全书，密码学领域的权威经典

Java应用架构师的必备参考手册

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。

作者介绍:

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，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。

目录: 第一部分 基础篇第1章 企业应用安全 1.1 我们身边的安全问题 1.2
拿什么来拯救你，我的应用 1.3 捍卫企业应用安全的银弹 1.4 为你的企业应用上把锁 1.5
小结第2章 企业应用安全的银弹—密码学 2.1 密码学的发家史 2.2
密码学定义、术语及其分类 2.3 保密通信模型 2.4 古典密码 2.5 对称密码体制 2.6
非对称密码体制 2.7 散列函数 2.8 数字签名 2.9 密码学的未来 2.10 小结第3章
Java加密利器 3.1 Java与密码学 3.2 java.security包详解 3.3 javax.crypto包详解 3.4
java.security.spec包和javax.crypto.spec包详解 3.5 java.security.cert包详解 3.6
javax.net.ssl包详解 3.7 小结第4章 他山之石，可以攻玉 4.1 加固你的系统 4.2
加密组件Bouncy Castle 4.3 辅助工具Commons Codec 4.4 小结 第二部分 实践篇第5章
电子邮件传输算法—Base64 5.1 Base64算法的由来 5.2 Base64算法的定义 5.3
Base64算法与加密算法的关系 5.4 实现原理 5.5 模型分析 5.6 Base64算法实现 5.7 Url
Base64算法实现 5.8 应用举例 5.9 小结第6章 验证数据完整性—消息摘要算法 6.1
消息摘要算法简述 6.2 MD算法家族 6.3 SHA算法家族 6.4 MAC算法家族 6.5
其他消息摘要算法 6.6 循环冗余校验算法—CRC算法 6.7 实例：文件校验 6.8 小结第7章
初等数据加密—对称加密算法 7.1 对称加密算法简述 7.2 数据加密标准—DES 7.3
三重DES—DESede 7.4 高级数据加密标准—AES 7.5 国际数据加密标准—IDEA 7.6
基于口令加密—PBE 7.7 实例：对称加密网络应用 7.8 小结第8章
高等数据加密—非对称加密算法 8.1 非对称加密算法简述 8.2 密钥交换算法—DH 8.3
典型非对称加密算法—RSA 8.4 常用非对称加密算法—ElGamal 8.5
实例：非对称加密网络应用 8.6 小结第9章 带密钥的消息摘要算法—数字签名算法 9.1
数字签名算法简述 9.2 模型分析 9.3 经典数字签名算法—RSA 9.4
数字签名标准算法—DSA 9.5 椭圆曲线数字签名算法—ECDSA 9.6
实例：带有数字签名的加密网络应用 9.7 小结 第三部分 综合应用篇第10章
终极武器—数字证书 10.1 数字证书详解 10.2 模型分析 10.3 证书管理 10.4 证书使用 10.5
应用举例 10.6 小结第11章 终极装备—安全协议 11.1 安全协议简述 11.2 模型分析 11.3
单向认证服务 11.4 双向认证服务 11.5 应用举例 11.6 小结第12章
量体裁衣—为应用选择合适的装备 12.1 实例：常规Web应用开发安全 12.2
实例：IM应用开发安全 12.3 实例：Web Service应用开发安全 12.4 小结附录A Java

6支持的算法附录B Bouncy Castle支持的算法
・・・・・・(收起)

Java加密与解密的艺术_下载链接1_

标签

Java

安全

Java加密与解密的艺术

软件开发

编程

计算机

信息安全

计算机科学

评论

除了第三方组件和API，就是列出一大段调用API的代码。。。这书最多算“编著”，书中没有任何作者自己的原创，居然用“著”来忽悠人！

感觉不咋的，作者博客：http://snowolf.javaeye.com/ 目录：http://goo.gl/KVKQ

非常棒的一本书，做Java应用开发的朋友都该收藏一本。

电子版不全，也没有什么有用的东西。。。

很不错的java加密解密方面的参考

一般吧

例子的冗余代码较多,可以精简,把书搞薄点,看起来更无压力啊.

该书重点介绍Java平台密码学API使用
包括编码、对称加密、非对称加密、哈希散列、数字证书、HTTPS等相关API使用和Demo例子，对密码学知识本身只是简单介绍性，还需要参考相应书籍。至于书名加上艺术两字，估计是出版社出于营销考虑

为数不多的讲java加解密相关的书

看得出作者还是很用心的，但对RSA和数字证书相关章节不太满意，比如358页说的『我们假定密钥库文件zlex.keystore存储在D盘根目录，数字证书文件zlex.cer也存储在D盘根目录』，作者没有说清楚zlex.keystore对应的是私钥，zlex.cer对应的是公钥，它们是如何生成的，如果用openssl产生私钥，签发，生成了证书，那么如何才能得到转换成这个私钥对应的keystore呢？在讲keytool的340页看来看去也只是说将证书（含有公钥信息的）转换成keystore文件，并且感觉『代码清单10-6
导入数字证书』这种描述太模糊，356和357页将『解密』写成『加密』了。

枯燥无味

用来系统的整理一下安全方面的思路还行。不过书里面对jdk里的api的解释占了很多篇幅，事实上这些东西看api文档比看这书要强。

入門佳作。

很实用，对以后在软件编程方面有很大的帮助~~ 娃哈哈，，不错不错！！！

2013/04/18 - 2013/04/25 这本书凑字数的水分太多了，精简精简会更好

干货率5% 这本书简直就是api说明书. 除此之外就剩下一点点的使用api方面的简单的坑. 用大量的代码来让书显得厚. 加密的原理原本就不复杂. 复杂的是加密的算法.
这本书几乎不讲. 所以书名叫艺术, 没叫技术.

概念都讲不清楚

Code和api都占了一半，有种凑页数的嫌疑，一些东西讲的也不是很深入

1.先讲解了加解密及相关算法的基础知识；2.接着讲解了在Java中的具体实践。难得的入门佳作啊，想要研究具体加解密的算法的不适合看这本书。

不是很懂原理。挑着看了AES, RSA,
数字签名，数字证书，密钥库这几个跟工作相关的知识点，代码敲了一遍。前几天看到一个别人按照公司规范写的AES加密，感觉安全方面的知识还是挺深奥的。现在大致了解下，有机会再深入学习。

Java加密与解密的艺术_下载链接1_

书评

书的内容不错，由浅入深，优点就不多说了
缺点是书中的错误太多了，很多驴嘴不对马尾的地方，就拿第10章和11章讲吧，数字证书和HTTPS，从内容中经常有错误的注释，画的UML也有很多不对的地方，该讲的内容没讲，基础的内容占很大篇幅，这倒无所谓，只是千万别误人子弟啊

---
java
加密解密的经典，很好的概括和解释了加密解密的算法和应用，无论是理论还是实践，都是非常值得收藏和拜读的一本书

内容太过简单， 所讲的内容没有超出oralce java security tutorial的范围,
有兴趣的朋友可以看官方的文档进一步的了解整个java security
的概貌。http://docs.oracle.com/javase/6/docs/technotes/guides/security/。
优点是在介绍加解密算法的时候，给出了详尽的示例。缺点也...

十分佩服作者，让我明白了各类密码算法和数据完整性算法在现实世界中的应用场合。
如：CRC32算法是各种压缩算法中最为常用的数据完整性校验算法。 还有等等等等。

转互动网读者评论：http://www.china-pub.com/196506
最近刚忙完毕设，就迫不及待的看起了《Java加密与解密的艺术》这本书，在阅读这本书之前，也看过不少本书作者梁栋写的博客，因为在博客方面，作者写得还是很不错的，由此也对本书更多了一份期待。 花了一周时间通读...

继《正在爆发的互联网革命》、《设计模式之禅》后，《Java加密与解密的艺术》的版权又输出到台湾，值得庆贺！
该书一经上市，在大陆颇受好评，多家台湾出版社争相评估，最终决定将繁体版版权授予台湾基峰公司。 作者写作这本书的经历可以看这里，推荐有写作经历的朋友看看：...

首先，必须先说明一下这本书不是精通书籍，而是一本入门以及注重实践的书。
这本书的结构安排比较合理，从基础的工具准备篇（Java

加解密库）到本书的重点加解密算法的介绍和实践，到最后的比较高级以及常用的综合应用，衔接得很不错。 这本书对于不熟悉加解密算法的同学我觉...

除了第一章写的有点意思外，其它章节太枯燥了，很多地方几乎是Java API的中文翻译。如果官方文档里能找到，有必要花那么长的篇章写吗?
作者写的代码，几乎原封不动贴到书里，连注释都被复制到所有的地方，比如@author 梁栋，@version 1.0,@since 1.0, 出现在N多地方，凑字数也...

因为作者是这方面的专家，而且写作非常用心，所以它上市后得到了广大读者朋友的一致认可，销量非常不错，本书上个月已经重印了，谢谢大家的支持。

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。 (来自卓越)

IT界的3大主题：安全、移动应用开发和云计算。
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。 （来自卓越）

非常好的一本书，内容充实，可读性强，实践指导性非常好，从头到尾非常有序，让读者由不知到熟悉再到应用都有有一很清晰的思路。特别是java加密利器与综合应用篇对安全性特别高的项目，但又不知道从何下手的读者特别有帮助。

最近刚忙完毕设，就迫不及待的看起了《Java加密与解密的艺术》这本书，在阅读这本书之前，也看过不少本书作者梁栋写的博客，因为在博客方面，作者写得还是很不错的，由此也对本书更多了一份期待。
花了一周时间通读全书，虽然有好些地方应该细细品味，但迫于时间的...

对于没有编程基础的人还是先不要看了，这本书主要是面对有编程基础的人看的，写的很好，很细，对java中api的使用进行了详细的介绍，今天拿到的书正在看

这是一本非常实用的书，从密码学理论、Java API实现，包括Bouncy Castle和Commons Codec的API实现、单向双向认证等多方面阐述如何使用Java这门语言加强系统安全。其实，在Java安全这个行业里，未必有多少人系统地学习过这些理论知识，基本上都是单纯去实现一些安全技术根本都不...

MD5/SHA1，DSA，DESede/DES 消息摘要，数字签名，对称加密等介绍的都很详细 原理和应用实例也很清晰 从不同的应用中体现在实际应用中的价值。非常不错。。

最近工作中涉及到了java加解密和安全方面的技术，在网上找了很多资料，但有些杂乱。前些天网上看见这本书将出版，一直跟踪着，上周在网上买来，这几天一直在看，感觉这本书写的不错，很具体，实例很多。很多实践可以直接拿来应用，也可以作为工具书翻阅查询也不错。

很不错的安全书籍
此本加密解密算法书，从理论到实际，实战的经验，实用的写作，通俗易懂，值得拥有的一本书。 书名很彪悍，内容很适用。

读这本书之前，读过《Java安全:第二版》，感觉太抽象，看了半天没找到感觉，还是不知道怎么做。相比《Java安全》，这本书讲的挺全面，至少是JDK1.6版本了。当初构建WebService时，一直找不到构建HTTPS协议平台的完整实施方案，没想到都在这本书里了。力荐，一定要力荐！

Java加密与解密的艺术_下载链接1_