

Java加密与解密的艺术(第2版)



[Java加密与解密的艺术\(第2版\)_下载链接1](#)

著者:梁栋

出版者:机械工业出版社

出版时间:2013-12-15

装帧:平装

isbn:9787111446781

《Java加密与解密的艺术（第2版）》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。

《Java加密与解密的艺术（第2版）》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。

作者介绍:

梁栋 资深Java EE技术专家和Java EE企业级应用架构师。安全技术专家，对Java加密与解密技术有系统深入的研究。开源技术爱好者，有着丰富的Spring、Apache系列等开源框架的实践经验。国内Bouncy Castle扩展加密技术引入者，对其算法实现与应用有深入研究，并将其整理成册，供广大技术人员参考学习。擅长分布式、高并发系统的设计与架构，在分布式缓存、NoSQL、消息队列等方面有非常丰富的实践经验。

目录: 前言

第一部分 基础篇

第1章 企业应用安全 2

1.1 我们身边的安全问题 2

1.2 拿什么来拯救你，我的应用 3

1.2.1 安全技术目标 3

1.2.2 OSI安全体系结构 4

1.2.3 TCP/IP安全体系结构 6

1.3 捍卫企业应用安全的银弹 8

1.3.1 密码学在安全领域中的身影 8

1.3.2 密码学与Java EE 8

1.4 为你的企业应用上把锁 9

1.5 小结 10

第2章 企业应用安全的银弹—密码学 11

2.1 密码学的发家史 11

2.1.1 手工加密阶段 11

2.1.2 机械加密阶段 12

2.1.3 计算机加密阶段 13

2.2 密码学定义、术语及其分类 15

2.2.1 密码学常用术语 15

2.2.2 密码学分类 16

2.3 保密通信模型 17

2.4 古典密码 18

2.5 对称密码体制 19

- 2.5.1 流密码 20
- 2.5.2 分组密码 21
- 2.6 非对称密码体制 27
- 2.7 散列函数 28
- 2.8 数字签名 29
- 2.9 公钥基础设施 31
 - 2.9.1 PKI的标准 31
 - 2.9.2 PKI系统的组成 32
 - 2.9.3 数字证书 33
- 2.10 PGP、OpenPGP与GPG 34
- 2.11 密码学的未来 34
 - 2.11.1 密码算法的破解 35
 - 2.11.2 密码学的明天 36
- 2.12 小结 36
- 第3章 Java加密利器 38
 - 3.1 Java与密码学 38
 - 3.1.1 Java安全领域组成部分 38
 - 3.1.2 安全提供者体系结构 39
 - 3.1.3 关于出口的限制 40
 - 3.1.4 关于本章内容 40
 - 3.2 java.security包详解 40
 - 3.2.1 Provider类 41
 - 3.2.2 Security类 44
 - 3.2.3 MessageDigest类 46
 - 3.2.4 DigestInputStream类 49
 - 3.2.5 DigestOutputStream类 49
 - 3.2.6 Key接口 52
 - 3.2.7 AlgorithmParameters类 53
 - 3.2.8 AlgorithmParameterGenerator类 55
 - 3.2.9 KeyPair类 56
 - 3.2.10 KeyPairGenerator类 57
 - 3.2.11 KeyFactory类 59
 - 3.2.12 SecureRandom类 61
 - 3.2.13 Signature类 62
 - 3.2.14 SignedObject类 65
 - 3.2.15 Timestamp类 66
 - 3.2.16 CodeSigner类 67
 - 3.2.17 KeyStore类 69
 - 3.3 javax.crypto包详解 73
 - 3.3.1 Mac类 73
 - 3.3.2 KeyGenerator类 75
 - 3.3.3 KeyAgreement类 77
 - 3.3.4 SecretKeyFactory类 78
 - 3.3.5 Cipher类 80
 - 3.3.6 CipherInputStream类 84
 - 3.3.7 CipherOutputStream类 83
 - 3.3.8 SealedObject类 86
 - 3.4 java.security.spec包和javax.crypto.spec包详解 88
 - 3.4.1 KeySpec和Algorithm-ParameterSpec接口 88
 - 3.4.2 EncodedKeySpec类 89
 - 3.4.3 SecretKeySpec类 92
 - 3.4.4 DESKeySpec类 93
 - 3.5 java.security.cert包详解 94
 - 3.5.1 Certificate类 94

- 3.5.2 CertificateFactory类 95
- 3.5.3 X509Certificate类 97
- 3.5.4 CRL类 98
- 3.5.5 X509CRLEntry类 99
- 3.5.6 X509CRL类 100
- 3.5.7 CertPath类 102
- 3.6 javax.net.ssl包详解 103
 - 3.6.1 KeyManagerFactory类 103
 - 3.6.2 TrustManagerFactory类 105
 - 3.6.3 SSLContext类 106
 - 3.6.4 HTTPSURLConnection类 109
 - 3.6.5 SSLSession接口 111
 - 3.6.6 SSLSocketFactory类 111
 - 3.6.7 SSLSocket类 112
 - 3.6.8 SSLServerSocketFactory类 114
 - 3.6.9 SSLServerSocket类 114
- 3.7 小结 117
- 第4章 他山之石，可以攻玉 119
 - 4.1 加固你的系统 119
 - 4.1.1 获得权限文件 120
 - 4.1.2 配置权限文件 120
 - 4.1.3 验证配置 121
 - 4.2 加密组件Bouncy Castle 121
 - 4.2.1 获得加密组件 122
 - 4.2.2 扩充算法支持 122
 - 4.2.3 相关API 126
 - 4.3 辅助工具Commons Codec 130
 - 4.3.1 获得辅助工具 130
 - 4.3.2 相关API 131
 - 4.4 小结 141
- 第二部分 实践篇
- 第5章 电子邮件传输算法—Base64 144
 - 5.1 Base64算法的由来 144
 - 5.2 Base64算法的定义 144
 - 5.3 Base64算法与加密算法的关系 145
 - 5.4 实现原理 146
 - 5.4.1 ASCII码字符编码 146
 - 5.4.2 非ASCII码字符编码 147
 - 5.5 模型分析 147
 - 5.6 Base64算法实现 148
 - 5.6.1 Bouncy Castle 148
 - 5.6.2 Commons Codec 150
 - 5.6.3 两种实现方式的差异 154
 - 5.6.4 不得不说的的问题 154
 - 5.7 Url Base64算法实现 157
 - 5.7.1 Bouncy Castle 157
 - 5.7.2 Commons Codec 159
 - 5.7.3 两种实现方式的差异 160
 - 5.8 应用举例 161
 - 5.8.1 电子邮件传输 161
 - 5.8.2 网络数据传输 161
 - 5.8.3 密钥存储 162
 - 5.8.4 数字证书存储 162
 - 5.8.5 OpenSSL操作Base 64编码 163

5.9 小结	163
第6章 验证数据完整性—消息摘要算法	165
6.1 消息摘要算法简述	165
6.1.1 消息摘要算法的由来	165
6.1.2 消息摘要算法的家谱	166
6.2 MD算法家族	167
6.2.1 简述	167
6.2.2 模型分析	168
6.2.3 实现	170
6.3 SHA算法家族	177
6.3.1 简述	177
6.3.2 模型分析	178
6.3.3 实现	179
6.4 MAC算法家族	191
6.4.1 简述	191
6.4.2 模型分析	192
6.4.3 实现	192
6.5 其他消息摘要算法	205
6.5.1 简述	205
6.5.2 实现	205
6.6 循环冗余校验算法—CRC算法	216
6.6.1 简述	216
6.6.2 模型分析	217
6.6.3 实现	217
6.7 实例：文件校验	219
6.8 小结	222
第7章 初等数据加密—对称加密算法	224
7.1 对称加密算法简述	224
7.1.1 对称加密算法的由来	224
7.1.2 对称加密算法的家谱	225
7.2 数据加密标准—DES	225
7.2.1 简述	225
7.2.2 模型分析	226
7.2.3 实现	227
7.3 三重DES—DESede	233
7.3.1 简述	233
7.3.2 实现	233
7.4 高级数据加密标准—AES	238
7.4.1 简述	238
7.4.2 实现	239
7.5 国际数据加密标准—IDEA	243
7.5.1 简述	243
7.5.2 实现	243
7.6 基于口令加密—PBE	247
7.6.1 简述	247
7.6.2 模型分析	247
7.6.3 实现	248
7.7 实例：对称加密网络应用	253
7.8 小结	265
第8章 高等数据加密—非对称加密算法	267
8.1 非对称加密算法简述	267
8.1.1 非对称加密算法的由来	267
8.1.2 非对称加密算法的家谱	268
8.2 密钥交换算法—DH&ECDH	269

8.2.1 简述	269
8.2.2 模型分析	269
8.2.3 DH实现	270
8.2.4 ECDH实现	280
8.3 典型非对称加密算法—RSA	289
8.3.1 简述	289
8.3.2 模型分析	290
8.3.3 实现	291
8.4 常用非对称加密算法—ElGamal	298
8.4.1 简述	298
8.4.2 模型分析	298
8.4.3 实现	299
8.5 实例：非对称加密网络应用	305
8.6 小结	317
第9章 带密钥的消息摘要算法—数字签名算法	319
9.1 数字签名算法简述	319
9.1.1 数字签名算法的由来	319
9.1.2 数字签名算法的家谱	320
9.2 模型分析	320
9.3 经典数字签名算法—RSA	321
9.3.1 简述	322
9.3.2 实现	322
9.4 数字签名标准算法—DSA	328
9.4.1 简述	328
9.4.2 实现	328
9.5 椭圆曲线数字签名算法—ECDSA	333
9.5.1 简述	333
9.5.2 实现	333
9.6 实例：带有数字签名的加密网络应用	341
9.7 小结	352
第三部分 综合应用篇	
第10章 终极武器—数字证书	356
10.1 数字证书详解	356
10.2 模型分析	359
10.2.1 证书签发	359
10.2.2 加密交互	360
10.3 证书管理	361
10.3.1 KeyTool证书管理	361
10.3.2 OpenSSL证书管理	368
10.4 证书文件操作	379
10.4.1 JKS文件操作	379
10.4.2 PFX文件操作	388
10.4.3 PEM文件操作	390
10.5 应用举例	394
10.6 小结	394
第11章 终极装备—安全协议	396
11.1 安全协议简述	396
11.1.1 HTTPS协议	396
11.1.2 SSL/TLS协议	397
11.2 模型分析	398
11.2.1 协商算法	399
11.2.2 验证证书	399
11.2.3 产生密钥	400
11.2.4 加密交互	402

11.3 单向认证服务	403
11.3.1 准备工作	403
11.3.2 服务验证	408
11.3.3 代码验证	410
11.4 双向认证服务	415
11.4.1 准备工作	415
11.4.2 服务验证	418
11.4.3 代码验证	420
11.5 应用举例	421
11.6 实例	422
11.6.1 SSLSocket获取数字证书	422
11.6.2 SSLSocket加密交互	425
11.7 小结	429
第12章 量体裁衣—为应用选择合适的装备	431
12.1 实例：常规Web应用开发安全	431
12.1.1 常规Web应用基本实现	431
12.1.2 安全升级1—摘要处理	436
12.1.3 安全升级2—加盐处理	438
12.2 实例：IM应用开发安全	441
12.2.1 IM应用开发基本实现	441
12.2.2 安全升级1—隐藏数据	454
12.2.3 安全升级2—加密数据	457
12.3 实例：Web Service应用开发安全	462
12.3.1 Web Service应用基本实现	462
12.3.2 安全升级1—单向认证服务	469
12.3.3 安全升级2—双向认证服务	480
12.4 小结	485
附录A Java 7支持的算法	487
附录B Bouncy Castle支持的算法	490
• • • • •	(收起)

[Java加密与解密的艺术\(第2版\) 下载链接1](#)

标签

Java

Security

加解密

安全

计算机

编程

技术

加密工具

评论

虽然书名带着艺术字眼
但是对书本身内容很失望，对加密算法本身介绍太简单，大量的篇幅是代码例子展示JDK和第三方加密组件API使用。其实只要知道几个加密算法，然后Google算法原理，API使用对用经验的程序员轻而易举的事情，不推荐买该书

就像有个豆友评论的那样，这本书——对加密算法本身介绍太简单，大量的篇幅是代码例子展示JDK和第三方加密组件API使用。对于加密解密完全不懂得的童鞋会有点帮助吧，有经验的人就不要买了。

书很厚，没实质用途

对java的加解密方面介绍的很系统，代码详尽，非常适合加解密的入门。

本书是从技术应用层面出发的，对于各个算法的底层理论涉及较少

作者的语言表达能力真是烂到家了

[Java加密与解密的艺术\(第2版\)_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oracle 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\(第2版\) 下载链接1](#)