



构建安全Java应用的权威经典，5大社区一致鼎力推荐！

华章  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

Java加密与解密的艺术

梁栋 著

ISBN : 978-7-111-29762-8

本书纸版由机械工业出版社于2010年出版，电子版由华章分社（北京华章图文信息有限公司）全球范围内制作与发行。

版权所有，侵权必究

客服热线：+ 86-10-68995265

客服信箱：service@bbbvip.com

官方网址：www.bbbvip.com

新浪微博 @研发书局

腾讯微博 @yanfabook

目 录

赞誉

前言

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

1.2.1 安全技术目标

1.2.2 OSI安全体系结构

1.2.3 TCP/IP安全体系结构

1.3 捍卫企业应用安全的银弹

1.3.1 密码学在安全领域中的身影

1.3.2 密码学与Java EE

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

2.1.1 手工加密阶段

2.1.2 机械加密阶段

2.1.3 计算机加密阶段

2.2 密码学定义、术语及其分类

2.2.1 密码学常用术语

2.2.2 密码学分类

2.3 保密通信模型

2.4 古典密码

2.5 对称密码体制

2.5.1 流密码

2.5.2 分组密码

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

2.9.1 密码算法的破解

2.9.2 密码学的明天

2.10 小结

第3章 Java加密利器

3.1 Java与密码学

3.1.1 Java安全领域组成部分

3.1.2 关于出口的限制

3.1.3 本书所使用的软件

3.1.4 关于本章内容

3.2 java.security包详解

3.2.1 Provider

3.2.2 Security

3.2.3 MessageDigest

3.2.4 DigestInputStream

3.2.5 DigestOutputStream

3.2.6 Key

3.2.7 AlgorithmParameters

3.2.8 AlgorithmParameterGenerator

3.2.9 KeyPair

3.2.10 KeyPairGenerator

3.2.11 KeyFactory

3.2.12 SecureRandom

3.2.13 Signature

3.2.14 SignedObject

3.2.15 Timestamp

3.2.16 CodeSigner

3.2.17 KeyStore

3.3 javax.crypto包详解

3.3.1 Mac

3.3.2 KeyGenerator

3.3.3 KeyAgreement

3.3.4 SecretKeyFactory

3.3.5 Cipher

3.3.6 CipherInputStream

3.3.7 CipherOutputStream

3.3.8 SealedObject

3.4 java.security.spec包和javax.crypto.spec包详解

3.4.1 KeySpec和AlgorithmParameterSpec

3.4.2 EncodedKeySpec

3.4.3 SecretKeySpec

3.4.4 DESKeySpec

3.5 java.security.cert包详解

3.5.1 Certificate

3.5.2 CertificateFactory

3.5.3 X509Certificate

3.5.4 CRL

3.5.5 X509CRLEntry

3.5.6 X509CRL

3.5.7 CertPath

3.6 javax.net.ssl包详解

3.6.1 KeyManagerFactory

3.6.2 TrustManagerFactory

3.6.3 SSLContext

3.6.4 HTTPSURLConnection

3.7 小结

第4章 他山之石，可以攻玉

4.1 加固你的系统

4.1.1 获得权限文件

4.1.2 配置权限文件

4.1.3 验证配置

4.2 加密组件Bouncy Castle

4.2.1 获得加密组件

4.2.2 扩充算法支持

4.2.3 相关API

4.3 辅助工具Commons Codec

4.3.1 获得辅助工具

4.3.2 相关API

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

5.4.1 ASCII码字符编码

5.4.2 非ASCII码字符编码

5.5 模型分析

5.6 Base64算法实现

5.6.1 Bouncy Castle

5.6.2 Commons Codec

5.6.3 两种实现方式的差异

5.6.4 不得不说的的问题

5.7 Url Base64算法实现

5.7.1 Bouncy Castle

5.7.2 Commons Codec

5.7.3 两种实现方式的差异

5.8 应用举例

5.8.1 电子邮件传输

5.8.2 网络数据传输

5.8.3 密钥存储

5.8.4 数字证书存储

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

6.1.1 消息摘要算法的由来

6.1.2 消息摘要算法的家谱

6.2 MD算法家族

6.2.1 简述

6.2.2 模型分析

6.2.3 实现

6.3 SHA算法家族

6.3.1 简述

6.3.2 模型分析

6.3.3 实现

6.4 MAC算法家族

6.4.1 简述

6.4.2 模型分析

6.4.3 实现

6.5 其他消息摘要算法

6.5.1 简述

6.5.2 实现

6.6 循环冗余校验算法—CRC算法

欢迎访问：电子书学习和下载网站 (<https://www.shgis.com>)

文档名称：《Java加密与解密的艺术》梁栋 著.pdf

请登录 <https://shgis.com/post/3275.html> 下载完整文档。

手机端请扫码查看：

