

<<.NET安全性与密码术>>

图书基本信息

书名：<<.NET安全性与密码术>>

13位ISBN编号：9787302088578

10位ISBN编号：7302088578

出版时间：2004-8

出版时间：清华大学出版社

作者：(美)Peter Thorsteinson等

页数：340

字数：563000

译者：梁志敏

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<.NET安全性与密码术>>

内容概要

安全性与密码术一直是计算工业的重要组成部分。

在过去几年中，两者的重要性显著提高。

Microsoft ' s .NET Framework为开发人员提供了一个实现应用程序安全性的功能强大的全新工具包。

本书为在基于.NET的平台上实现安全性和密码术特性提供了实用通俗的指导。

作者提供了大量用C # 和Visual Basic.NET编写的清晰且有针对性的示例，并详细阐述了这些代码的工作原理。

全书逻辑清晰、条理清楚、易于理解。

书中所有示例代码都可以从www.objectinnovations.com/library/books/books_dotnet.html站点中下载。

本书主要目的 · 强化密码术的基本理论，以便理解.NET Framework安全工具的功能。

- 学会使用对称算法、非对称算法和数字签名。
- 掌握传统的加密编程以及XML加密和XML签名等新技术。
- 介绍如何将这些工具应用于ASP.NET安全性和Web服务安全性。

<<.NET安全性与密码术>>

作者简介

Peter Thorsteinson是一位系统分析家，有着10年以上从事编程、教学以及为软件开发研究指导性材料的经验。

他的专业兴趣有C++、Java和C#,以及ATL、COM+、.NET和J2EE。

Peter拥有Manitoba大学的电子工程学学士学位，与他们合著了.NET Architecture and Programming Using Vis

<<.NET安全性与密码术>>

书籍目录

第1章 .NET密码术与安全性简介 1.1 本书的特点 1.2 密码术与安全性的特性 1.2.1 密码术与安全性的重要性 1.2.2 密码术与安全性的功能 1.3 Windows安全性的演化 1.4 .NET Framework与CLR 1.4.1 .NET Framework简化安全性的方法 1.4.2 可靠性与.NET平台 1.4.3 托管代码和类型安全 1.5 .NET密码术编程 1.6 .NET安全编程 1.6.1 基于角色的安全性和主名 1.6.2 CAS、证据、策略和权限 1.7 小结第2章 密码术基础 2.1 安全性与保密 2.1.1 基本的密码术术语 2.1.2 秘密密钥与秘密算法 2.1.3 古典保密技术 2.1.4 穷举攻击工作因数 2.1.5 任意精度运算 2.2 隐写术 2.3 现代密码 2.3.1 密码术与.NET Framework 2.3.2 对称密码术 2.3.3 非对称密码术 2.3.4 密码算法 2.3.5 密码协议 2.4 密码攻击 2.5 人际交流与信任问题 2.5.1 风险和利益 2.5.2 其他重要概念 2.6 小结第3章 对称密码术 3.1 对称密码 3.1.1 DES 3.1.2 操作模式 3.1.3 Triple DES 3.1.4 Rijndael 3.1.5 RC2 3.2 使用对称密码术的.NET编程 3.2.1 主要的密码术类 3.2.2 SymmetricAlgorithm类 3.2.3 SymmetricAlgorithm的派生类 3.2.4 SymmetricAlgorithm示例 3.2.5 密码流 3.2.6 避免使用弱密钥 3.3 密钥交换问题 3.3.1 加密的散列代码和消息完整性 3.3.2 加密的散列函数和消息完整性 3.4 小结第4章 非对称密码术 4.1 对称算法存在的问题 4.1.1 密钥交换问题 4.1.2 信任问题 4.2 非对称密码术的原理 4.2.1 使用非对称密码术 4.2.2 密码锁模型 4.2.3 陷门单向函数 4.2.4 非对称加密方法的优点 4.2.5 非对称算法与对称算法的结合 4.3 现有的非对称算法 4.4 RSA：最常用的非对称算法 4.4.1 RSA基础 4.4.2 一个小型的RSA示例 4.5 可证性问题 4.6 使用非对称密码术的.NET编程 4.6.1 一个RSA算法示例 4.6.2 将密钥保存为XML格式 4.7 数字证书 4.8 小结第5章 数字签名.....第6章 XML密码术第7章 .NET基于用户的安全性第8章 .NET代码访问安全性第9章 ASP.NET安全性第10章 Web服务安全性附录A 堆栈溢出安全攻击示例附录B RSA密码的工作原理附录C GNU GMP库的用法附录D 密码术与安全性资源附录E Web服务研究

<<.NET安全性与密码术>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>