《现代密码学》

图书基本信息

书名：《现代密码学》

13位ISBN编号：9787118070651

10位ISBN编号：7118070653

出版时间：2011-1

出版社：国防工业出版社

作者：Jonathan Katz,Yehuda Lindell

页数：350

译者：任伟

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

《现代密码学》

内容概要

《现代密码学:原理与协议》内容简介：密码学在确保数据的私密性和完整性，以及计算机网络的安全性方面扮演了关键角色。乔纳森·卡茨和耶胡达·林德尔所著的《现代密码学：原理与协议》一书提供了对现代密码学严格而又容易理解的介绍，关注形式化的定义、精确的假设以及严格的证明。《现代密码学：原理与协议》介绍了现代密码学的核心原则，包括现代的、基于计算复杂性的安全，以克服完美安全的局限性。对对称密钥加密和消息鉴别也做了较大篇幅的介绍。同时，举例说明了分组密码，如DES和AES的设计原则，并且在低级原语层面展示了分组密码的可证明安全构造方法。《现代密码学：原理与协议》下半部分介绍公钥密码学。首先对数论知识进行了介绍，这些知识是理解RSA、Diffie-Hellman、El Gamal以及其他密码学系统所需要的。在探讨了公钥加密和数字签名之后，介绍了随机预言模型及其应用。无论作为教材、参考书或者自学用书，《现代密码学:原理与协议》呈献给读者透彻理解现代密码学这一迷人主题所需要的工具。

《现代密码学》

书籍目录

第一部分 经典密码学介绍
第1章 概论
1.1 密码学和现代密码学
1.2 对称密钥加密的基本设置
1.3 古典加密术及其密码分析
1.4 现代密码学的基本原则
1.4.1 原则l——形成精确的定义
1.4.2 原则2-精确假设的依赖
1.4.3 原则3——严格的安全证明
参考文献和扩展阅读材料介绍
练习
第2章 完善保密加密
2.1 定义和基本属性
2.2 一次一密(Vemam加密)
2.3 完善保密的局限
2.4 香农定理
2.5 小结
参考文献和扩展阅读材料介绍
练习
第二部分 对称密钥(对称)密码学
第3章 对称密钥加密以及伪随机性
3.1 密码学的计算方法
3.1.1 计算安全的基本思想
3.1.2 有效的算法和可忽略的成功概率
3.1.3 规约证明
3.2 定义计算安全的加密
3.2.1 安全的基本定义
3.2.2 定义的属性
3.3 伪随机性
3.4 构造安全加密方案
3.4.1 一个安全的定长加密方案
3.4.2 处理变长消息
3.4.3 流密码和多个加密
3.5 选择明文攻击(CPA)的安全性
3.6 CPA安全的加密方案创建
3.6.1 伪随机函数
3.6.2 基于伪随机函数的CPA安全加密
3.6.3 伪随机置换和分组加密
3.6.4 加密操作模式
3.7 CCA安全性
参考文献和扩展阅读材料介绍
练习
第4章 消息鉴别码和抗碰撞散列函数
4.1 安全通信与消息完整性
4.2 加密与消息鉴别的比较
4.3 消息鉴别码——定义
4.4 构造安全的消息鉴别码

4.5 CBC.MAC
4.6 抗碰撞散列函数
4.6.1 抗碰撞的定义
4.6.2 散列函数安全性的一个较弱的定义
4.6.3 通用“ 生日 ”攻击
4.6.4 Merkle-Damgard变换
4.6.5 实践中的抗碰撞散列函数
4.7 NMAC与HMAC
4.7.1 嵌套MACmMAC
4.7.2 HMAC
4.8 构造CCA安全加密方案
4.9 获得私密性和消息鉴别
参考文献和扩展阅读材料介绍
练习
第5章 伪随机置换(分组加密)的实际构建
5.1 代替一置换网络
5.2 Feistel网络
5.3 DES——数据加密标准
5.3.1 DES的设计
5.3.2 对减少轮数的DES变种的攻击
5.3.3 DES的安全性
5.4 增加分组密码的密钥长度
5.5 AES——高级加密标准
5.6 差分密码分析和线性密码分析简介
参考文献和扩展阅读材料介绍
练习
第6章 伪随机对象的理论构造
6.1 单向函数
6.1.1 定义
6.1.2 候选单向函数
6.1.3 硬核谓词
6.2 概述：从单向函数到伪随机置换
6.3 任意单向函数的硬核谓词
6.3.1 简单情形
6.3.2 复杂情形
6.3.3 完整证明
6.4 构造伪随机发生器
6.4.1 具有最小扩展的伪随机发生器
6.4.2 提高扩展系数
6.5 构造伪随机函数
6.6 构造(强)伪随机置换
6.7 对称密钥密码学的必要假设
6.8 偏离——计算不可区分性
6.8.1 伪随机性和伪随机发生器
6.8.2 多重抽样
参考文献及扩展阅读材料介绍
练习
第三部分公钥(非对称密钥)密码学
第7章 数论和密码学困难性假设

7.1 预备知识和基本群论
7.1.1 素数与可除}生
7.1.2 模算术
7.1.3 群
7.1.4 Z*N群
7.1.5 群同构和中国剩余定理
7.2 素数、大数分解和RSA
7.2.1 随机素数的产生
7.2.2 素数判定
7.2.3 因子分解假设
7.2.4 RSA假设
7.3 循环群中的假设
7.3.1 循环群和生成元
7.3.2 离散对数和Diffie-Hellman假设
7.3.3 在Zp(的子群)中工作
7.3.4 椭圆曲线群
7.4 数论假设的密码学应用
7.4.1 单向函数和置换
7.4.2 构造抗碰撞的散列函数
参考文献和扩展阅读材料介绍
练习
第8章 因子分解和离散对数算法
8.1 因子分解算法
8.1.1 Pollard的p-1方法
8.1.2 Pollard的Rho方法
8.1.3 二次筛选算法
8.2 计算离散对数的算法
8.2.1 “ 小步大步 ” 算法
8.2.2 Pohlig-Hellman算法
8.2.3 ZN中的离散对数问题
8.2.4 索引演算方法
参考文献和扩展阅读材料介绍
练习
第9章 对称密钥管理和公钥革命
9.1 对称密钥加密的局限性
9.2 局部解决方法——密钥分配中心
9.3 公钥革命
9.4 Diffe-Hellman密钥交换
参考文献和扩展阅读材料介绍
练习
第10章 公钥加密
10.1 公钥加密简介
10.2 定义
10.2.1 选择明文攻击的安全性
10.2.2 多重加密
10.3 混合加密
10.4 RSA加密
10.4.1 “ 教科书式RSA ” 加密方案及其不安全性
10.4.2 对 “ 教科书式RSA ” 加密方案的攻击

10.4.3 填充RSA
10.5 E1Gamal加密
10.6 选择密文攻击的安全性
10.7 陷门置换
10.7.1 定义
10.7.2 来自陷门置换的公钥加密
参考文献和扩展阅读材料介绍
练习
第11章 其他公钥加密方案
11.1 Goldwasser-Micali加密方案
11.1.1 素数模二次剩余
11.1.2 合数模二次剩余
11.1.3 二次剩余假设
11.1.4 Goldwasser-Micali加密方案
11.2 Rabin加密方案
11.2.1 计算模平方根
11.2.2 基于分解的陷门置换
11.2.3 Rabin加密方案
11.3 Paillier加密方案
11.3.1 Z*N2结构
11.3.2 Paillier加密方案
11.3.3 同态加密
参考文献和扩展阅读材料介绍
练习
第12章 数字签名
12.1 数字签名简介
12.2 定义
12.3 RSA签名
12.3.1 “ 教科书式RSA ”签名方案及其不安全性
12.3.2 “ 散列后RSA ”签名方案
12.4 “ Hash-and-Sign ”范例
12.5 Lamport的“ 一次性签名方案 ”
12.6 来自抗碰撞散列的签名
12.6.1 基于Chain的签名
12.6.2 基于Tree的签名
12.7 数字签名标准(DSS)
12.8 数字证书和公钥基础设施
参考文献和扩展阅读材料介绍
练习一
第13章 随机预言机模型中的公钥密码系统
13.1 随机预言机方法学
13.1.1 随机预言机模型
13.1.2 随机预言机方法是否合理
13.2 随机预言机模型中的公钥加密
13.2.1 选择明文攻击安全
13.2.2 选择密文攻击安全
13.2.3 OAEP
13.3 随机预言机模型中的签名
参考文献和扩展阅读材料介绍

练习
常用符号索引
附录
附录A数学知识
A.1 恒等式和不等量
A.2 渐进表示法
A.3 概率论简介
A.4 “ 生日 ” 问题
附录B算法数论补充知识
B.1 整数算术
B.2 模算术
B.3 寻找一个循环群的生成元
参考文献和扩展阅读材料介绍
练习
参考文献

《现代密码学》

精彩短评

1、瞅一眼中文版……作者是用google翻译翻的吗？！……这种翻译质量也能出版？！
2、质量很好，到货很及时，内容也很详尽，有助于对这方面兴趣的的发展。
3、其实内容与想象的相差不少
4、看E文版吧。对翻译本来就不应该抱有什么期待。。。
5、翻译不好，语序都没调整，不适合入门。
6、纸质非常一般。基础内容可以看william stalling的那本。这书里的一些现代公钥签名方案可以从目录跳着看。
7、用译者的语言风格，我对这本书的评价就是：这吓到了我 that 翻译烂像这样
8、内容艰深，看的吃力。

看了几节coursera的cryptography来看这书，翻译确实有点烂，不过倒是能轻松从翻译推断出英文原文是什么词。可能也找不到信达雅的描述吧。譬如练习3.7，the scheme need not to be "natural"->该方案不必是“ 天然的 ”。
9、好好的书，翻译得跟屎一样

《现代密码学》

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:www.tushu000.com