

<<密码学与网络安全>>

图书基本信息

书名：<<密码学与网络安全>>

13位ISBN编号：9787302099673

10位ISBN编号：7302099677

出版时间：2005-1

出版时间：第1版 (2005年1月1日)

作者：卡哈特

页数：435

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>

<<密码学与网络安全>>

内容概要

本书清晰易懂地介绍了密码学和网络安全的基本概念和实际问题，探讨了加密、解密、对称和不对称密钥，详细分析和解释了各种主要密码算法，包括数据加密标准（DES），国际数据加密算法（IDEA），RC5，Blowfish，先进加密标准（AES），RSA，数字签名算法（DSA）等，并讨论了主要用于机构的防火墙和虚拟专用网络（VPN）技术，数字签名，公钥基础设施（PKI）和XML安全性，安全套接协议层（SSL），安全超文本传输协议（SHTTP），安全电子交易（SET），3D安全，PGP，PEM，S/MIME等。

在无线安全方面研究了WAP、GSM、3G、身份认证、单点登录（SSO）等技术。

本书还介绍了拒绝服务（DoS）攻击，联机银行交易等一些案例研究。

本书每章后面给出了多项选择题、复习题、编程练习题等。

本书不仅对于普及IT专业人员的网络安全知识、提高普通用户的安全意识会大有裨益，也是本科生和研究生的一本不错的参考书。

书籍目录

1 Introduction to the Concepts of Security 1.1 Introduction 1 1.2 The Need for Security 2 1.3 Security Approaches 3 1.4 Principles of Security 4 1.5 Types of Attacks 8 Outline of the Book 23 Multiple-choice Questions 25 Review Questions 26 Design/Programming Exercises 272 Cryptographic Techniques 2.1 Introduction 28 2.2 Plain Text and Cipher Text 29 2.3 Substitution Techniques 31 2.4 Transposition Techniques 36 2.5 Encryption and Decryption 40 2.6 Symmetric and Asymmetric Key Cryptography 43 2.7 Steganography 53 2.8 Key Range and Key Size 54 2.9 Possible Types of Attacks 57 Chapter Summary 58 Key Terms and Concepts 59 Multiple-choice Questions 59 Review Questions 60 Design/Programming Exercises 61 Contents 3 Computer-based SYmmetric Key Cryptographic Algorithms 3.1 Introduction 63 3.2 Algorithm Types and Modes 63 3.3 An Overview of Symmetric Key Cryptography 73 3.4 Data Encryption Standard (DES) 75 3.5 International Data Encryption Algorithm (IDEA) 90 3.6 RC5 98 3.7 Blowfish 105 3.8 Advanced Encryption Standard (AES) 107 3.9 Differential and Linear Cryptanalysis 109 Chapter Summary 110 Key Terms and Concepts 110 Multiple-choice Questions 110 Review Questions 111 Design/Programming Exercises 114 4 Computer-based Asymmetric Key Cryptographic Algorithms 4.1 Introduction 112 4.2 Brief History of Asymmetric Key Cryptography 112 4.3 An Overview of Asymmetric Key Cryptography 113 4.4 The RSA Algorithm 115 4.5 Symmetric and Asymmetric Key Cryptography Together 119 4.6 Digital Signatures 125 4.7 Knapsack Algorithm 154 4.8 Some Other Algorithms 154 Chapter Summary 157 Key Terms and Concepts 158 Multiple-choice Questions 158 Review Questions 159 Design/Programming Exercises 159 5 Public Key Infrastructure (PKI) 5.1 Introduction 161 5.2 Digital Certificates 162 5.3 Private Key Management 194 5.4 The PKIX Model 196 5.5 Public Key Cryptography Standards (PKCS) 198 5.6 XML, PKI and Security 204 Chapter Summary 208 Key Terms and Concepts 208 Multiple-choice Questions 209 Review Questions 210 Design/Programming Exercises 210 6 Internet Security Protocols 6.1 Basic Concepts 211 6.2 Secure Socket Layer (SSL) 218 6.3 Secure HyperText Transfer Protocol (SHTTP) 229 6.4 Time Stamping Protocol (TSP) 230 6.5 Secure Electronic Transaction (SET) 231 6.6 SSL Versus SET 244 6.7 3-D Secure Protocol 244 6.8 Electronic Money 245 6.9 Email Security 250 6.10 Wireless Application Protocol (WAP) Security 263 6.11 Security in GSM 266 Chapter Summary 268 Key Terms and Concepts 269 Multiple-choice Questions 269 Review Questions 270 Design/Programming Exercises 270 7 User Authentication Mechanisms 7.1 Introduction 271 7.2 Authentication Basics 271 7.3 Passwords 272 7.4 Authentication Tokens 286 7.5 Certificate-based Authentication 297 7.6 Biometric Authentication 303 7.7 Kerberos 304 7.8 Single Sign On (SSO) Approaches 309 Chapter Summary 310 Key Terms and Concepts 311 Multiple-choice Questions 311 Review Questions 312 Design/Programming Exercises 312 8 Practical Implementations of Cryptography/Security 8.1 Cryptographic Solutions Using Java 314 8.2 Cryptographic Solutions Using Microsoft 322 8.3 Cryptographic Toolkits 324 8.4 Security and Operating Systems 325 Chapter Summary 330 Key Terms and Concepts 330 Multiple-choice Questions 330 Review Questions 331 Design/Programming Exercises 331 Contents 9 Network Security 9.1 Brief Introduction to TCP/IP 332 9.2 Firewalls 338 9.3 IP Security 349 9.4 Virtual Private Networks (VPN) 365 Chapter Summary 368 Key Terms and Concepts 368 Multiple-choice Questions 369 Review Questions 369 10 Case Studies on Cryptography and Security 10.1 Introduction 371 10.2 Cryptographic Solutions--A Case Study 371 10.3 Single Sign On (SSO) 379 10.4 Secure Inter-branch Payment Transactions 382 10.5 Denial of Service (DOS) Attacks 385 10.6 IP Spoofing Attacks 388 10.7 Cross Site Scripting Vulnerability (CSSV) 389 10.8 Contract Signing 391 10.9 Secret Splitting 392 10.10 Virtual Elections 394 10.11 Secure Multiparty Calculation 395 Appendix A-Mathematical Background Appendix B-Number Systems Appendix C-Information Theory Appendix D-Real-life Tools Appendix E-Web Resources Appendix F-A Brief Introduction to ASN, BER, DER Appendix G-Modern Security Trends Answers to Multiple-choice Questions Glossary References Index

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>