<<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：9787302197966

10位ISBN编号：7302197962

出版时间：2009-5

出版时间：清华大学出版社

作者：卡哈特

页数：534

前言

Having worked in the area of information Technology for about six years （in 2001）, I had read a lot abouto worked in the area of information Technology for about six years （in 2001）, I had read a lot aboutinformation securitV, and how to achieve it. However, my concepts were vague, and I knew theJ, and how to achieve it. However, my concepts were vague, and I knew thetechnology of security in bits and pieces. This was quite annoying, as it never gave a feeling ofioJ J in bits and pieces. This was quite annoying, as it never gave a feeling ofsatisfaction. It was as if I did not know the complete pictllre. For example, I did know that numbersystems played an important role in cryptography, but did not know how much I should know aboutthem to understand the concepts thoroughly. Similarly, I knew that digital certificates and Public KeyInfrastructure （PKI） were quite wonderful technologies, but knew only to some extent as to how theyworked. Numerous other examples can be given.Then I got an opportunity to lead an information security project in i-flex solutions limited. I knewo pportunity to lead an information security project in i-flex solutions limited. I knewthat I could learn a lot simply by working on that project. However, I also felt very strongly that until Iwas thorouZh with all the aSDects of comDUter securitV/crVptoZraDhv myself. I would not be able to doo poets of computer security/cryptography myself, I would not be able to do..true lustice to this project. It was for this reason that I took up the task of studying each and every aspectJ ustice to this project. It was for this reason that I took up the task of studying each and every aspectof these technologies. Unfortllnately, there were a lot of hurdles. The main hurdle was that there was noto j, Lllere were a lot of hurdles.

<<密码学与网络安全>>

内容概要

本书以清晰的脉络、简洁的语言，介绍了各种加密技术、网络安全协议与实现技术等内容，包括各种对称密钥算法与AES，非对称密钥算法、数字签名与RSA，数字证书与公钥基础设施，Internet安全协议，用户认证与Kerberos，Java、.NET和操作系统的加密实现，网络安全、防火墙与VPN，并给出了具体的加密与安全的案例实现分析，是一本关于密码学与网络安全的理论结合实践的优秀教材。

作者简介

Atul Kahate在印度和世界IT业中已经有12年的工作经验，他取得了统计学学士学位和计算机系统专业的MBA学位。
他与他人为Tata McGraw-Hill出版公司合著了多部著作，不少书被用作教材或全世界的大学/学院/IT公司用作参考书。
Atul Kahate还在印度和国外获得过多个奖项，过去曾就职

<<密码学与网络安全>>

书籍目录

Preface to the Second Editon jace to the Second Editon Preface to the First Editon jace to the First Editon Important Terms andAbbreviations 1. Attacks on Computers and Computer Security 1.1 intfoduction 1 1.2 The Need for Security 1.3 SecuritV Approaches 1.4 Principles of Security 1.5 TVves of Attacks Summary Multiple-choice Ouestions pie-choice Questions Exercises Design/Programming Exercises 2. Cryptography: Concepts and Techniques 2.1 Intfoduction 2.2 Plain Text and Cipher Text 2.3 Substitution Techniques 2.4 Transposition Techniques 2.5 EncrVption and DecrVption 2.6 Symmetric and AsVmmetric Key Cryptography 2.7 Steganography 2.8 Key Range and Key Size 2.9 Possible TVves of Attacks Summary Multiple-choice Ouestions pie-choice Questions Exercises Design/Programming Exercises 3. Symmetric Key Algorithms and AES 3.1 Introduction 3.2 Algorithm Types and Modes 3.3 An Overview of Symmetric Key Cryptography 3.4 Data Encryption Standard (DES) 3.5 International Data Encryption Algorithm (IDEA) 3.6 RC4 3.7 RCS 3.8 Blowfish 3.9 Advanced Encryption Standard (AES) Summary Multiple-choice Questions Exercises Design/Programming Exercises 4. Asymmetric Key Algorithms, Digital Signatures and RSA 4.1 Introduction 4.2 Brief History of Asymmetric Key Cryptography 4.3 An Overview of Asymmetric Key Cryptography 4.4 The RSA Algorithm 4.5 Symmetric and Asymmetric Key Cryptography Together 4.6 Digital Signatures 4.7 KnapsackAlgorithm 4.8 Some Other Algorithms Summary Multiple--choice Questions Exercises Design/Programming Exercises 5. Digital Certificates and Public Key infrastructure (PKI) 5.1 Introduction 5.2 Digital Certificates 5.3 Private Key Management 5.4 The PKIX Model 5.5 Public Key Cryptography Standards (PKCS) 5.6 XML, PKI and Security 5.7 Creating Digital Certificates Using Java Summary Multiple-choice Questions Exercises Design/Programming Exercises 6. Internet Security Protocols 7. User Authentication and Kerberos 8. Cryptography in lava, .NET and Operating Systems 9. Network Security, Firewalls and Virtual Private Networks (VPN) 10. Case Studies on Cryptography and Security APPendixA: Mathematical Background APPendix B: Number Systems APPendix C: Information Theory APPendixD: Real-ide TOols APPendix E: Web Resources APPendix F: A Brief introduction tO ASN, BER, DER References

章节摘录

插图：It is said that a random number generator based purely on deterministic computational techniquecannot really be considered as a perfect random number generator. This is because its output ispredictable. Distinguishing between true and seemingly true random numbers is not easy. Most computer programming languages provide support for random number generators in the formof library functions. They are usually so designed that they can provide a random byte or a floating pointnumber uniformly distributed between the range of 0 and 1. These library functions are often found tohave poor statistical properties and some will repeat patterns after a few cycles. They are usuallyinitialized using a computer's clock as the seed. These functions may provide enough randomness forcertain simple tasks （e.g. computer-based games）, but they are not recommended in situations thatdemand high-quality randomness. Examples of these situations are cryptographic applications,statistical applications or numerical applications. Hence, specialized random number generators are alsoavailable on a majority of operating systems. We might feel that computers can generate random numbers. In fact, many programming languagesprovide facilities to generate random numbers. However, this is not quite correct. Random numbersgenerated by computers are not truly randomover a period of time, we can predict them. This issimply because computers are rulebased machines, which have a finite range for generating （the socalled） random numbers. Therefore, we must make computers generate random numbers by usingsome external means. This process is called as psuedorandom number generation.

编辑推荐

《密码学与网络安全(第2版)》语言表达流畅、简洁，使《密码学与网络安全(第2版)》的阅读不再枯燥。
全书多达425幅插图，极大地方便了读者的学习和理解。
全书提供了丰富的多项选择题、练习题、设计与编程题，有利于加深读者对所学知识的理解和掌握。

版权说明