1. Record Nr. UNINA9910151655203321

Autore	Stallings William
Titolo	Cryptography and network security : principles and practice / / William Stallings ; contributions by Mohit P. Tahiliani
Pubbl/distr/stampa	Boston, [Massachusetts] : , : Pearson, , 2014 ©2014
ISBN	9781488682957 9780273793359 1-4886-8295-X 0-273-79376-4
Edizione	[Sixth edition.]
Descrizione fisica	1 online resource (755 pages) : illustrations
Collana	Always Learning
Disciplina	005.8
Soggetti	Computer networks - Security measures Data encryption (Computer science) Coding theory
Lingua di pubblicazione	Inglese
Formato	Multimedia
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Cover -- Contents -- Notation -- Preface -- Chapter 0 Guide for Readers and Instructors -- 0.1 Outline of This Book -- 0.2 A Roadmap for Readers and Instructors -- 0.3 Internet and Web Resources -- 0.4 Standards -- Chapter 1 Overview -- 1.1 Computer Security Concepts -- 1.2 The OSI Security Architecture -- 1.3 Security Attacks -- 1.4 Security Services -- 1.5 Security Mechanisms -- 1.6 A Model for Network Security -- 1.7 Recommended Reading -- 1.8 Key Terms, Review Questions, and Problems -- PART ONE: SYMMETRIC CIPHERS -- Chapter 2 Classical Encryption Techniques -- 2.1 Symmetric Cipher Model -- 2.2 Substitution Techniques -- 2.3 Transposition Techniques -- 2.4 Rotor Machines -- 2.5 Steganography -- 2.6 Recommended Reading -- 2.7 Key Terms, Review Questions, and Problems -- Chapter 3 Block Ciphers and the Data Encryption Standard -- 3.1 Traditional Block Cipher Structure -- 3.2 The Data Encryption Standard -- 3.3 A DES Example -- 3.4 The Strength of DES -- 3.5 Block Cipher Design Principles -- 3.6 Recommended Reading -- 3.7 Key Terms, Review Questions, and Problems -- Chapter 4 Basic Concepts in Number

Theory and Finite Fields -- 4.1 Divisibility and the Division Algorithm -- 4.2 The Euclidean Algorithm -- 4.3 Modular Arithmetic -- 4.4 Groups, Rings, and Fields -- 4.5 Finite Fields of the Form GF(p) -- 4.6 Polynomial Arithmetic -- 4.7 Finite Fields of the Form GF(2(Sup[n])) -- 4.8 Recommended Reading -- 4.9 Key Terms, Review Questions, and Problems -- Appendix 4A The Meaning of mod -- Chapter 5 Advanced Encryption Standard -- 5.1 Finite Field Arithmetic -- 5.2 AES Structure -- 5.3 AES Transformation Functions -- 5.4 AES Key Expansion -- 5.5 An AES Example -- 5.6 AES Implementation -- 5.7 Recommended Reading -- 5.8 Key Terms, Review Questions, and Problems -- Appendix 5A Polynomials with Coefficients in GF(2(Sup[8])) -- Appendix 5B Simplified AES.
Chapter 6 Block Cipher Operation -- 6.1 Multiple Encryption and Triple DES -- 6.2 Electronic Code book -- 6.3 Cipher Block Chaining Mode -- 6.4 Cipher Feedback Mode -- 6.5 Output Feedback Mode -- 6.6 Counter Mode -- 6.7 XTS-AES Mode for Block-Oriented Storage Devices -- 6.8 Recommended Reading -- 6.9 Key Terms, Review Questions, and Problems -- Chapter 7 Pseudorandom Number Generation and Stream Ciphers -- 7.1 Principles of Pseudorandom Number Generation -- 7.2 Pseudorandom Number Generators -- 7.3 Pseudorandom Number Generation Using a Block Cipher -- 7.4 Stream Ciphers -- 7.5 RC4 -- 7.6 True Random Number Generators -- 7.7 Recommended Reading -- 7.8 Key Terms, Review Questions, and Problems -- PART TWO: ASYMMETRIC CIPHERS -- Chapter 8 More Number Theory -- 8.1 Prime Numbers -- 8.2 Fermat's and Euler's Theorems -- 8.3 Testing for Primality -- 8.4 The Chinese Remainder Theorem -- 8.5 Discrete Logarithms -- 8.6 Recommended Reading -- 8.7 Key Terms, Review Questions, and Problems -- Chapter 9 Public-Key Cryptography and RSA -- 9.1 Principles of Public-Key Cryptosystems -- 9.2 The RSA Algorithm -- 9.3 Recommended Reading -- 9.4 Key Terms, Review Questions, and Problems -- Appendix 9A The Complexity of Algorithms -- Chapter 10 Other Public-Key Cryptosystems -- 10.1 Diffie-Hellman Key Exchange -- 10.2 Elgamal Cryptographic System -- 10.3 Elliptic Curve Arithmetic -- 10.4 Elliptic Curve Cryptography -- 10.5 Pseudorandom Number Generation Based on an Asymmetric Cipher -- 10.6 Recommended Reading -- 10.7 Key Terms, Review Questions, and Problems -- PART THREE: CRYPTOGRAPHIC DATA INTEGRITY ALGORITHMS -- Chapter 11 Cryptographic Hash Functions -- 11.1 Applications of Cryptographic Hash Functions -- 11.2 Two Simple Hash Functions -- 11.3 Requirements and Security -- 11.4 Hash Functions Based on Cipher Block Chaining -- 11.5 Secure Hash Algorithm (SHA).
11.6 SHA-3 -- 11.7 Recommended Reading -- 11.8 Key Terms, Review Questions, and Problems -- Chapter 12 Message Authentication Codes -- 12.1 Message Authentication Requirements -- 12.2 Message Authentication Functions -- 12.3 Requirements for Message Authentication Codes -- 12.4 Security of MACs -- 12.5 MACs Based on Hash Functions: HMAC -- 12.6 MACs Based on Block Ciphers: DAA and CMAC -- 12.7 Authenticated Encryption: CCM and GCM -- 12.8 Key Wrapping -- 12.9 Pseudorandom Number Generation using Hash Functions and MACs -- 12.10 Recommended Reading -- 12.11 Key Terms, Review Questions, and Problems -- Chapter 13 Digital Signatures -- 13.1 Digital Signatures -- 13.2 Elgamal Digital Signature Scheme -- 13.3 Schnorr Digital Signature Scheme -- 13.4 NIST Digital Signature Algorithm -- 13.5 Elliptic Curve Digital Signature Algorithm -- 13.6 RSA-PSS Digital Signature Algorithm -- 13.7 Recommended Reading -- 13.8 Key Terms, Review Questions, and Problems -- PART FOUR: MUTUAL TRUST -- Chapter 14 Key Management and Distribution

-- 14.1 Symmetric Key Distribution Using Symmetric Encryption -- 14.2 Symmetric Key Distribution Using Asymmetric Encryption -- 14.3 Distribution of Public Keys -- 14.4 X.509 Certificates -- 14.5 Public-Key Infrastructure -- 14.6 Recommended Reading -- 14.7 Key Terms, Review Questions, and Problems -- Chapter 15 User Authentication -- 15.1 Remote User-Authentication Principles -- 15.2 Remote User-Authentication Using Symmetric Encryption -- 15.3 Kerberos -- 15.4 Remote User Authentication Using Asymmetric Encryption -- 15.5 Federated Identity Management -- 15.6 Personal Identity Verification -- 15.7 Recommended Reading -- 15.8 Key Terms, Review Questions, and Problems -- PART FIVE: NETWORK AND INTERNET SECURITY -- Chapter 16 Network Access Control and Cloud Security -- 16.1 Network Access Control.
16.2 Extensible Authentication Protocol -- 16.3 IEEE 802.1X Port-Based Network Access Control -- 16.4 Cloud Computing -- 16.5 Cloud Security Risks and Countermeasures -- 16.6 Data Protection in the Cloud -- 16.7 Cloud Security as a Service -- 16.8 Recommended Reading -- 16.9 Key Terms, Review Questions, and Problems -- Chapter 17 Transport-Level Security -- 17.1 Web Security Considerations -- 17.2 Secure Sockets Layer -- 17.3 Transport Layer Security -- 17.4 HTTPS -- 17.5 Secure Shell (SSH) -- 17.6 Recommended Reading -- 17.7 Key Terms, Review Questions, and Problems -- Chapter 18 Wireless Network Security -- 18.1 Wireless Security -- 18.2 Mobile Device Security -- 18.3 IEEE 802.11 Wireless LAN Overview -- 18.4 IEEE 802.11i Wireless LAN Security -- 18.5 Recommended Reading -- 18.6 Key Terms, Review Questions, and Problems -- Chapter 19 Electronic Mail Security -- 19.1 Pretty Good Privacy -- 19.2 S/MIME -- 19.3 DomainKeys Identified Mail -- 19.4 Recommended Reading -- 19.5 Key Terms, Review Questions, and Problems -- Appendix 19A Radix-64 Conversion -- Chapter 20 IP Security -- 20.1 IP Security Overview -- 20.2 IP Security Policy -- 20.3 Encapsulating Security Payload -- 20.4 Combining Security Associations -- 20.5 Internet Key Exchange -- 20.6 Cryptographic Suites -- 20.7 Recommended Reading -- 20.8 Key Terms, Review Questions, and Problems -- APPENDICES -- Appendix A Projects for Teaching Cryptography and Network Security -- A.1 Sage Computer Algebra Projects -- A.2 Hacking Project -- A.3 Block Cipher Projects -- A.4 Laboratory Exercises -- A.5 Research Projects -- A.6 Programming Projects -- A.7 Practical Security Assessments -- A.8 Firewall Projects -- A.9 Case Studies -- A.10 Writing Assignments -- A.11 Reading/Report Assignments -- A.12 Discussion Topics -- Appendix B Sage Examples -- B.1 Linear Algebra and Matrix Functionality.
B.2 Chapter 2: Classical Encryption -- B.3 Chapter 3: Block Ciphers and the Data Encryption Standard -- B.4 Chapter 4: Basic Concepts in Number Theory and Finite Fields -- B.5 Chapter 5: Advanced Encryption Standard -- B.6 Chapter 6: Pseudorandom Number Generation and Stream Ciphers -- B.7 Chapter 8: Number Theory -- B.8 Chapter 9: Public-Key Cryptography and RSA -- B.9 Chapter 10: Other Public-Key Cryptosystems -- B.10 Chapter 11: Cryptographic Hash Functions -- B. 11 Chapter 13: Digital Signatures -- References -- Credits -- Index.

Sommario/riassunto

For one-semester, undergraduate- or graduate-level courses in Cryptography, Computer Security, and Network Security A practical survey of cryptography and network security with unmatched support for instructors and students In this age of universal electronic connectivity, viruses and hackers, electronic eavesdropping, and electronic fraud, security is paramount. This text provides a practical survey of both the principles and practice of cryptography and network security. First, the basic issues to be addressed by a network security

capability are explored through a tutorial and survey of cryptography and network security technology. Then, the practice of network security is explored via practical applications that have been implemented and are in use today. An unparalleled support package for instructors and students ensures a successful teaching and learning experience. Teaching and Learning Experience To provide a better teaching and learning experience, for both instructors and students, this program will: Support Instructors and Students: An unparalleled support package for instructors and students ensures a successful teaching and learning experience. Apply Theory and/or the Most Updated Research: A practical survey of both the principles and practice of cryptography and network security. Engage Students with Hands-on Projects: Relevant projects demonstrate the importance of the subject, offer a real-world perspective, and keep students interested.