1.

Record Nr.	UNINA9910154943503321
Autore	Stallings William
Titolo	Cryptography and network security : principles and practice / / William Stallings
Pubbl/distr/stampa	Boston : , : Pearson, , [2017] ©2017
ISBN	9781292158594 9781292158587
Edizione	[Seventh, global edition.]
Descrizione fisica	1 online resource (766 pages) : illustrations ;
Collana	Always learning
Disciplina	005.82
Soggetti	Data encryption (Computer science) Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Cover -- Notation -- Preface -- Contents -- About the Author -- Part One: Background -- Chapter 1 Computer and Network Security Concepts -- 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 Fundamental Security Design Principles -- 1.7 Attack Surfaces and Attack Trees -- 1.8 A Model for Network Security -- 1.9 Standards -- 1.10 Key Terms, Review Questions, and Problems -- Chapter 2 Introduction to Number Theory -- 2.1 Divisibility and the Division Algorithm -- 2.2 The Euclidean Algorithm -- 2.3 Modular Arithmetic -- 2.4 Prime Numbers -- 2.5 Fermat's and Euler's Theorems -- 2.6 Testing for Primality -- 2.7 The Chinese Remainder Theorem -- 2.8 Discrete Logarithms -- 2.9 Key Terms, Review Questions, and Problems -- Appendix 2A The Meaning of Mod -- Part Two: Symmetric Ciphers -- Chapter 3 Classical Encryption Techniques -- 3.1 Symmetric Cipher Model -- 3.2 Substitution Techniques -- 3.3 Transposition Techniques -- 3.4 Rotor Machines -- 3.5 Steganography -- 3.6 Key Terms, Review Questions, and Problems -- Chapter 4 Block Ciphers and the Data Encryption Standard -- 4.1 Traditional Block Cipher Structure -- 4.2 The Data Encryption Standard -- 4.3 A DES Example -- 4.4 The Strength of DES -- 4.5 Block Cipher Design Principles -- 4.6 Key Terms, Review Questions, and Problems --

Chapter 5 Finite Fields -- 5.1 Groups -- 5.2 Rings -- 5.3 Fields -- 5.4 Finite Fields of the Form GF(p) -- 5.5 Polynomial Arithmetic -- 5.6 Finite Fields of the Form GF(2n) -- 5.7 Key Terms, Review Questions, and Problems -- Chapter 6 Advanced Encryption Standard -- 6.1 Finite Field Arithmetic -- 6.2 AES Structure -- 6.3 AES Transformation Functions -- 6.4 AES Key Expansion -- 6.5 An AES Example -- 6.6 AES Implementation -- 6.7 Key Terms, Review Questions, and Problems -- Appendix 6A Polynomials with Coefficients in GF(28) -- Chapter 7 Block Cipher Operation -- 7.1 Multiple Encryption and Triple DES -- 7.2 Electronic Codebook -- 7.3 Cipher Block Chaining Mode -- 7.4 Cipher Feedback Mode -- 7.5 Output Feedback Mode -- 7.6 Counter Mode -- 7.7 XTS-AES Mode for Block-Oriented Storage Devices -- 7.8 Format-Preserving Encryption -- 7.9 Key Terms, Review Questions, and Problems -- Chapter 8 Random Bit Generation and Stream Ciphers -- 8.1 Principles of Pseudorandom Number Generation -- 8.2 Pseudorandom Number Generators -- 8.3 Pseudorandom Number Generation Using a Block Cipher -- 8.4 Stream Ciphers -- 8.5 RC4 -- 8.6 True Random Number Generators -- 8.7 Key Terms, Review Questions, and Problems -- Part Three: Asymmetric Ciphers 283 -- Chapter 9 Public-Key Cryptography and RSA -- 9.1 Principles of Public-Key Cryptosystems -- 9.2 The RSA Algorithm -- 9.3 Key Terms, Review Questions, and Problems -- 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 Key Terms, Review Questions, and Problems -- Part Four: 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 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 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 Key Terms, Review Questions, and Problems -- Part Five: 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 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 Key Terms, Review Questions, and Problems -- Part Six: 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 Addressing Cloud Computing Security Concerns -- 16.9 Key Terms, Review Questions, and Problems -- Chapter 17 Transport-Level Security -- 17.1 Web Security Considerations -- 17.2 Transport Layer Security -- 17.3 HTTPS -- 17.4 Secure Shell (SSH) -- 17.5 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 Key Terms, Review Questions, and Problems -- Chapter 19 Electronic Mail Security -- 19.1 Internet Mail Architecture -- 19.2 Email Formats -- 19.3 Email Threats and Comprehensive Email Security -- 19.4 S/MIME -- 19.5 Pretty Good Privacy -- 19.6 DNSSEC -- 19.7 DNS-Based Authentication of Named Entities -- 19.8 Sender Policy Framework -- 19.9 DomainKeys Identified Mail -- 19.10 Domain-Based Message Authentication, Reporting, and Conformance -- 19.11 Key Terms, Review Questions, and Problems -- 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 Key Terms, Review Questions, and Problems -- APPENDICES 696 -- 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: Number Theory -- B.3 Chapter 3: Classical Encryption -- B.4 Chapter 4: Block Ciphers and the Data Encryption Standard -- B.5 Chapter 5: Basic Concepts in Number Theory and Finite Fields -- B.6 Chapter 6: Advanced Encryption Standard -- B.7 Chapter 8: Pseudorandom Number Generation and Stream Ciphers -- 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

Sommario/riassunto

For courses in Cryptography, Computer Security, and Network Security   The Principles and Practice of Cryptography and Network Security Stallings' Cryptography and Network Security introduces students to the compelling and evolving field of cryptography and network security. In an age of viruses and hackers, electronic eavesdropping, and electronic fraud on a global scale, security is paramount. The purpose of this book is to provide a practical survey of both the principles and practice of cryptography and network security. In the first part of the book, the basic issues to be addressed by a network security capability are explored by providing a tutorial and survey of cryptography and network security technology. The latter part of the book deals with the practice of network security: practical applications that have been implemented and are in use to provide network security.   This edition streamlines subject matter with new and updated material -- including Sage, one of the most important features of the book. Sage is an open-source, multiplatform, freeware package that implements a very powerful, flexible, and easily learned mathematics and computer algebra system. It provides hands-on experience with cryptographic algorithms and supporting homework assignments. With Sage, students learn a powerful tool that can be used for virtually any mathematical application. The book also provides an unparalleled degree of support

for instructors and students to ensure a successful teaching and learning experience. The full text downloaded to your computer With eBooks you can: search for key concepts, words and phrases make highlights and notes as you study share your notes with friends eBooks are downloaded to your computer and accessible either offline through the Bookshelf (available as a free download), available online and also via the iPad and
Android apps. Upon purchase, you will receive via email the code and instructions on how to access this product. Time limit The eBooks products do not have an expiry date. You will continue to access your digital ebook products whilst you have your Bookshelf installed.