1. Record Nr. UNINA9910795990003321

Autore	Musa Sarhan M
Titolo	Network Security and Cryptography
Pubbl/distr/stampa	Bloomfield : , : Mercury Learning & Information, , 2022 ©2022
ISBN	9781683928829 9781683928836
Edizione	[2nd ed.]
Descrizione fisica	1 online resource (611 pages)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Cover -- Half-Title -- Title -- Copyright -- Dedication -- Contents -- Preface -- Chapter 1: Overview of Computer Networks -- 1.1 Introduction -- 1.2 Open Systems Interconnection (OSI) Model -- 1.3 Transmission Control Protocol/Internetworking Protocol (TCP/IP) Model -- 1.4 Hierarchical Model -- 1.5 Computer Network Equipment -- 1.6 Computer Network Types -- 1.7 Computer Network Topology -- 1.8 Exercises -- Chapter 2: Mathematical Foundations for Computer Networks -- 2.1 Introduction -- 2.2 Probability Fundamentals -- 2.2.1 Simple Probability -- 2.2.2 Joint Probability -- 2.2.3 Conditional Probability -- 2.2.4 Statistical Independence -- 2.3 Random Variables -- 2.3.1 Cumulative Distribution Function -- 2.3.2 Probability Density Function -- 2.3.3 Joint Distribution -- 2.4 Discrete Probability Models -- 2.4.1 Bernoulli Distribution -- 2.4.2 Binomial Distribution -- 2.4.3 Geometric Distribution -- 2.4.4 Poisson Distribution -- 2.5 Continuous Probability Models -- 2.5.1 Uniform Distribution -- 2.5.2 Exponential Distribution -- 2.5.3 Erlang Distribution -- 2.5.4 Hyperexponential Distribution -- 2.5.5 Gaussian Distribution -- 2.6 Transformation of a Random Variable -- 2.7 Generating Functions -- 2.8 Central Limit Theorem -- 2.9 Classification of Random Processes -- 2.9.1 Continuous versus Discrete Random Process -- 2.9.2 Deterministic versus Non-Deterministic Random Process -- 2.9.3 Stationary versus Nonstationary Random Process -- 2.9.4 Ergodic versus Nonergodic

Random Process -- 2.10 Statistics of Random Processes and Stationarity -- 2.11 Time Averages of Random Processes and Ergodicity -- 2.12 Multiple Random Processes -- 2.13 Sample Random Processes -- 2.13.1 Random Walks -- 2.13.2 Markov Processes -- 2.13.3 Birth-and-Death Processes -- 2.13.4 Poisson Processes -- 2.14 Renewal Processes -- 2.15 Kendall's Notation -- 2.16 Little's Theorem. 2.17 M/M/1 Queue -- 2.18 M/M/1 Queue With Bulk Arrivals/Service -- 2.18.1 Mx/M/1 (Bulk Arrivals) System -- 2.18.2 M/MY/1 (Bulk Service) System -- 2.18.3 M/M/1/k Queueing System -- 2.18.4 M/M/k Queueing System -- 2.18.5 M/M/ Queueing System -- 2.19 M/G/1 Queueing SYSTEM -- 2.20 M/Ek/1 Queueing SYSTEM -- 2.21 Networks of Queues -- 2.21.1 Tandem Queues -- 2.21.2 Queueing System with Splitting -- 2.21.3 Queueing System with Feedback -- 2.22 Jackson Networks -- 2.23 Exercises -- Chapter 3: Overview of Cryptography -- 3.1 Introduction -- 3.2 Basic Terms Related to Cryptography -- 3.2.1 Cryptographic Primitives -- 3.2.2 Cryptographic Protocols -- 3.2.3 Encryption (at the Sender's End) -- 3.2.4 Decryption (at the Recipient's End) -- 3.3 Requirements of Secure Communication -- 3.4 Osi Security Architecture X.800 -- 3.4.1 Security Attacks -- 3.4.2 Security Services -- 3.4.3 Security Mechanisms -- 3.5 Categories of Cryptographic Systems -- 3.6 Symmetric (or Conventional) Encryption Model -- 3.6.1 Types of Attacks on a Conventional Encryption Scheme -- 3.6.2 Conventional Encryption for Confidentiality -- 3.6.3 Link Encryption -- 3.7 Exercises -- Chapter 4: Mathematical Foundations for Cryptography -- 4.1 Introduction -- 4.2 Introduction to Groups, Rings, and Fields -- 4.2.1 Groups -- 4.2.2 Ring -- 4.2.3 Field -- 4.3 Modular Arithmetic -- 4.3.1 Residue Classes (mod n) -- 4.3.2 Properties of Zn -- 4.3.3 Multiplication within Set Zn -- 4.4 Introduction to Primes and Co-Primes -- 4.4.1 Prime Numbers -- 4.4.2 Co-Prime Numbers or Relatively Prime Numbers -- 4.5 Euclid's Algorithm To Determine GCD -- 4.6 Extended Euclid's Algorithm -- 4.7 Galols Finite Fields -- 4.7.1 GF (p) -- 4.7.2 Set Z*p -- 4.7.3 Galois Finite Fields of Order 2n -- 4.7.4 Arithmetic Operations within GF (2n) -- 4.7.5 Addition (+) Operation within GF (23) -- 4.7.6 Addition Inverse of GF (23). 4.7.7 Multiplication (x) Operation within GF (23) Using m(x) = x3 + x2 + 1 for Reducing the Polynomials -- 4.7.8 Multiplication Inverse within GF (23) -- 4.7.9 Multiplicative Inverses of All Integers in GF (23) -- 4.8 Fermat's Little Theorem -- 4.8.1 A Corollary of Fermat's Little Theorem -- 4.9 Euler's Totient Function -- 4.9.1 General Formula for Computation of Totient Function (n) -- 4.10 Euler's Theorem -- 4.10.1 A Corollary of Euler's Theorem -- 4.11 Prime Numbers -- 4.11.1 Primitive Roots -- 4.12 Discrete Logarithms -- 4.12.1 Difficulty of Computing Discrete Logarithms -- 4.12.2 Algorithm to Determine the Primitive Roots of a Number n -- 4.12.3 Another Method of Determining the Primitive Roots of a Number n -- 4.13 Primality Testing -- 4.13.1 Miller and Rabin's Method -- 4.14 Chinese Remainder Theorem -- 4.14.1 Alternate Interpretation of the Chinese Remainder Theorem -- 4.15 Exercises -- Chapter 5: Classical Cipher Schemes -- 5.1 Introduction -- 5.2 Classical Substitution Ciphers -- 5.2.1 Caesar Cipher -- 5.2.2 Mono-Alphabetic Cipher -- 5.2.3 Hill Cipher -- 5.2.4 Play-Fair Cipher -- 5.2.5 Poly-Alphabetic Cipher (Vigenere Cipher) -- 5.2.6 One-Time Pad -- 5.3 Transposition Ciphers -- 5.3.1 Rail-Fence Cipher -- 5.3.2 Rectangular Transposition Cipher -- 5.4 Steganography -- 5.4.1 Limitation of Steganography -- 5.4.2 Steganography Combined with Cryptography -- 5.5 Exercises -- Chapter 6: Modern Symmetric Ciphers -- 6.1 Introduction -- 6.2 Some Basic Concepts for Symmetric Ciphers -- 6.2.1 Concept of Binary Block Substitution -- 6.2.2 Strength of the Substitution Cipher -- 6.2.3 Key

Size for the Simple Substitution Cipher -- 6.3 Claude Shannon's Theory of Diffusion and Confusion -- 6.3.1 Diffusion -- 6.3.2 Confusion -- 6.4 Feistel Cipher -- 6.4.1 Strength of the Feistel Cipher -- 6.5 Data Encryption Standard (DES).
6.5.1 Description of the Critical Functions of Each Round of DES -- 6.5.2 S-Box Transformation -- 6.5.3 Generation of Sub-Keys (K1... K16) -- 6.5.4 DES Decryption Algorithm -- 6.6 Avalanche Effect -- 6.6.1 Strength of DES -- 6.6.2 Possible Attacks on DES -- 6.6.3 Differential Cryptanalysis vs. Linear Cryptanalysis -- 6.7 Multiple Des -- 6.7.1 Double DES -- 6.7.2 Triple DES -- 6.7.3 Block Cipher vs. Stream Cipher -- 6.7.4 Block/Stream Cipher Modes of Operation -- 6.8 International Data Encryption Algorithm (IDEA) -- 6.8.1 Description of IDEA -- 6.8.2 Generation of Sub-Keys in IDEA -- 6.8.3 IDEA Modes of Operation -- 6.9 Advanced Encryption Standard (AES) -- 6.9.1 Processing of Plaintext -- 6.10 Key Management: Symmetric Encryption -- 6.10.1 Secure Distribution of Keys -- 6.10.2 Key Distribution Schemes -- 6.11 Pseudo-Random Number Generators -- 6.11.1 Pseudo-Random Number Generation (PRNG) Algorithms -- 6.12 Exercises -- Chapter 7: Public-Key Cryptography for Data Confidentiality -- 7.1 Introduction -- 7.2 Requirements of Public-Key Cryptography -- 7.3 Data Confidentiality Using Public-Key Cryptography -- 7.4 RSA Algorithm -- 7.4.1 Main Components -- 7.4.2 Strength of RSA -- 7.5 Key Management Using Public-Key Cryptography -- 7.5.1 Diffie-Hellman Algorithm for Key Distribution -- 7.5.2 Global Parameters -- 7.5.3 Strength of Diffie-Hellman Key-Exchange Scheme -- 7.5.4 Types of Attacks against Diffie-Hellman -- 7.6 El-Gamal Encryption Scheme -- 7.6.1 Determination of Private Key and Public Key (by User "A") -- 7.7 Elliptic Curve Cryptography (ECC) -- 7.7.1 Elliptic Curves -- 7.7.2 Elliptic Curves in Cryptography (ECC) -- 7.7.3 Prime Elliptic Curves -- 7.7.4 Prime Elliptic Curve Set -- 7.7.5 Computation of Elliptic Curve Set E11 (1, 1) -- 7.7.6 Rules for Addition (+) Operation over EP (a, b) -- 7.7.7 Multiplication over the Set EP (a, b).
7.7.8 Strength of ECC-Based Schemes -- 7.7.9 ECC-Based Key-Exchange Algorithm -- 7.7.10 Strength of ECC Key-Exchange Algorithm -- 7.7.11 ECC-Based Encryption/Decryption Scheme -- 7.7.12 Strength of ECC-based Encryption/Decryption Scheme -- 7.7.13 ECC Encryption/Decryption vs. RSA -- 7.7.14 Efficient Hardware Implementation -- 7.8 Exercises -- Chapter 8: Authentication Schemes -- 8.1 Introduction -- 8.2 What is Message Authentication? -- 8.3 Types of Authentication Services -- 8.3.1 Different Techniques of Message Authentication -- 8.3.2 Digital Signatures Using Public-Key Cryptography -- 8.3.3 Message Authentication Code (MAC) -- 8.3.4 Many-to-One Relationship between Messages and MAC Values -- 8.3.5 Use of MAC for Message Authentication -- 8.3.6 Chosen Plaintext Attack on MAC -- 8.3.7 Hash Function -- 8.4 Application Modes of Digital Signatures -- 8.4.1 Direct Digital Signature -- 8.4.2 Arbitrated Digital Signature -- 8.5 Authentication Protocols -- 8.5.1 Mutual Authentication -- 8.5.2 Symmetric Encryption Approaches -- 8.5.3 Needham Schroeder Protocol -- 8.5.4 Denning Protocol -- 8.5.5 NEUM Protocol -- 8.5.6 Public-Key Encryption Approaches -- 8.5.7 One-Way Authentication -- 8.5.8 Symmetric Encryption Approach -- 8.5.9 Public Key Encryption Approach -- 8.5.10 The Birthday Paradox -- 8.5.11 Probability of Two Sets Overlapping -- 8.5.12 Mathematical Basis for Birthday Attack -- 8.5.13 Birthday Attack -- 8.5.14 Verification of the Digital Signature at the Recipient End -- 8.5.15 How to Create Many Variants of a Message -- 8.5.16 Weak Collision Resistance -- 8.5.17 Strengths of Hash Functions -- 8.6 Message Digest (Hash Function)

Algorithms -- 8.6.1 MD5 Message Digest Algorithm -- 8.6.2 Sequence of Use of Message Words in Various Rounds -- 8.6.3 Primitive Logical Functions Used in Various Rounds -- 8.6.4 Strength of MD5.
8.7 Secure Hash Algorithm (SHA-1).

Sommario/riassunto

This new edition introduces the basic concepts in computer networks, blockchain, and the latest trends and technologies in cryptography and network security. The book is a definitive guide to the principles and techniques of cryptography and network security, and introduces basic concepts in computer networks such as classical cipher schemes, public key cryptography, authentication schemes, pretty good privacy, and Internet security. It features a new chapter on artificial intelligence security and the latest material on emerging technologies, related to IoT, cloud computing, SCADA, blockchain, smart grid, big data analytics, and more. Primarily intended as a textbook for courses in computer science, electronics & communication, the book also serves as a basic reference and refresher for professionals in these areas. FEATURES:Includes a new chapter on artificial intelligence security, the latest material on emerging technologies related to IoT, cloud computing, smart grid, big data analytics, blockchain, and moreFeatures separate chapters on the mathematics related to network security and cryptographyIntroduces basic concepts in computer networks including classical cipher schemes, public key cryptography, authentication schemes, pretty good privacy, Internet security services, and system securityIncludes end of chapter review questions