1. Record Nr. UNINA9910811938103321

| | |
|---|---|
| Autore | Oppliger Rolf |
| Titolo | Cryptography 101 : From Theory to Practice |
| Pubbl/distr/stampa | Norwood : , : Artech House, , 2021<br>©2021 |
| Edizione | [1st ed.] |
| Descrizione fisica | 1 online resource (679 pages) |
| Disciplina | 005.824 |
| Soggetti | Data encryption (Computer science)<br>Cryptography |
| Lingua di pubblicazione | Inglese |
| Formato | Materiale a stampa |
| Livello bibliografico | Monografia |
| Nota di contenuto | Intro -- Cryptography 101: From Theory to Practice -- Contents -- Foreword -- Preface -- References -- Acknowledgments -- Chapter 1 Introduction -- 1.1 CRYPTOLOGY -- 1.2 CRYPTOGRAPHIC SYSTEMS -- 1.2.1 Classes of Cryptographic Systems -- 1.2.2 Secure Cryptographic Systems -- 1.3 HISTORICAL BACKGROUND INFORMATION -- 1.4 OUTLINE OF THE BOOK -- References -- Chapter 2 Cryptographic Systems -- 2.1 UNKEYED CRYPTOSYSTEMS -- 2.1.1 Random Generators -- 2.1.2 Random Functions -- 2.1.3 One-Way Functions -- 2.1.4 Cryptographic Hash Functions -- 2.2 SECRET KEY CRYPTOSYSTEMS -- 2.2.1 Pseudorandom Generators -- 2.2.2 Pseudorandom Functions -- 2.2.3 Symmetric Encryption -- 2.2.4 Message Authentication -- 2.2.5 Authenticated Encryption -- 2.3 PUBLIC KEY CRYPTOSYSTEMS -- 2.3.1 Key Establishment -- 2.3.2 Asymmetric Encryption Systems -- 2.4 FINAL REMARKS -- References -- Part I UNKEYEDC RYPTOSYSTEMS -- Chapter 3 Random Generators -- 3.1 INTRODUCTION -- 3.2 REALIZATIONS AND IMPLEMENTATIONS -- 3.2.1 Hardware-Based Random Generators -- 3.2.2 Software-Based Random Generators -- 3.2.3 Deskewing Techniques -- 3.3 STATISTICAL RANDOMNESS TESTING -- References -- Chapter 4 Random Functions -- 4.1 INTRODUCTION -- 4.2 IMPLEMENTATION -- 4.3 FINAL REMARKS -- Chapter 5 One-Way Functions -- 5.1 INTRODUCTION -- 5.2 CANDIDATE ONE-WAY FUNCTIONS -- 5.2.1 Discrete Exponentiation |

Function -- 5.2.2 RSA Function -- 5.2.3 Modular Square Function -- 5.3 INTEGER FACTORIZATION ALGORITHMS -- 5.3.1 Special-Purpose Algorithms -- 5.3.2 General-Purpose Algorithms -- 5.3.3 State of the Art -- 5.4 ALGORITHMS FOR COMPUTING DISCRETE LOGARITHMS -- 5.4.1 Generic Algorithms -- 5.4.2 Nongeneric (Special-Purpose) Algorithms -- 5.4.3 State of the Art -- 5.5 ELLIPTIC CURVE CRYPTOGRAPHY -- 5.6 FINAL REMARKS -- References -- Chapter 6 Cryptographic Hash Functions -- 6.1 INTRODUCTION.
6.2 MERKLE-DAMGARD CONSTRUCTION -- 6.4 EXEMPLARY HASH FUNCTIONS -- 6.4.1 MD4 -- 6.4.2 MD5 -- 6.4.3 SHA-1 -- 6.4.4 SHA-2 Family -- 6.4.5 KECCAK and the SHA-3 Family -- 6.5 FINAL REMARKS -- Part II SECRET KEY CRYPTOSYSTEMS -- Chapter 7 Pseudorandom Generators -- 7.1 INTRODUCTION -- 7.2 EXEMPLARY CONSTRUCTIONS -- 7.3 CRYPTOGRAPHICALLY SECURE PRGs -- 7.3.1 Blum-Micali PRG -- 7.3.2 RSA PRG -- 7.3.3 BBS PRG -- 7.4 FINAL REMARKS -- References -- Chapter 8 Pseudorandom Functions -- 8.1 INTRODUCTION -- 8.2 SECURITY OF A PRF -- 8.3 RELATIONSHIP BETWEEN PRGs AND PRFs -- 8.3.1 PRF-Based PRG -- 8.3.2 PRG-Based PRF -- 8.4 RANDOM ORACLE MODEL -- 8.5 FINAL REMARKS -- References -- Chapter 9 Symmetric Encryption -- 9.1 INTRODUCTION -- 9.1.1 Block and Stream Ciphers -- 9.1.2 Attacks -- 9.2 HISTORICAL PERSPECTIVE -- 9.3 PERFECTLY SECURE ENCRYPTION -- 9.3 PERFECTLY SECURE ENCRYPTION -- 9.4 COMPUTATIONALLY SECURE ENCRYPTION -- 9.5 STREAM CIPHERS -- 9.5.1 LFSR-Based Stream Ciphers -- 9.5.2 Other Stream Ciphers -- 9.6 BLOCK CIPHERS -- 9.6.1 DES -- 9.6.2 AES -- 9.7 MODES OF OPERATION -- 9.7.1 ECB -- 9.7.2 CBC -- 9.7.3 CFB -- 9.7.4 OFB -- 9.7.5 CTR -- 9.8 FINAL REMARKS -- References -- Chapter 10 Message Authentication -- 10.1 INTRODUCTION -- 10.2 INFORMATION-THEORETICALLY SECURE MESSAGE AUTHENTICATION -- 10.3 COMPUTATIONALLY SECURE MESSAGE AUTHENTICATION -- 10.3.1 MACs Using A Symmetric Encryption System -- 10.3.2 MACs Using Keyed Hash Functions -- 10.3.3 Carter-WegmanMACs -- 10.4 FINAL REMARKS -- References -- Chapter 11 Authenticated Encryption -- 11.1 INTRODUCTION -- 11.2 AEAD CONSTRUCTIONS -- 11.2.1 CCM -- 11.2.2 GCM -- 11.3 FINAL REMARKS -- References -- Part III PUBLIC KEY CRYPTOSYSTEMS -- Chapter 12 Key Establishment -- 12.1 INTRODUCTION -- 12.2 KEY DISTRIBUTION -- 12.2.1 Merkle's Puzzles -- 12.2.2 Shamir's Three-Pass Protocol.
12.2.3 Asymmetric Encryption-Based Key Distribution Protocol -- 12.3 KEY AGREEMENT -- 12.4 QUANTUM CRYPTOGRAPHY -- 12.4.1 Basic Principles -- 12.4.2 Quantum Key Exchange Protocol -- 12.4.3 Historical and Recent Developments -- 12.5 FINAL REMARKS -- References -- Chapter 13 Asymmetric Encryption -- 13.1 INTRODUCTION -- 13.2 PROBABILISTIC ENCRYPTION -- 13.2.1 Algorithms -- 13.2.2 Assessment -- 13.3 ASYMMETRIC ENCRYPTION SYSTEMS -- 13.3.1 RSA -- 13.3.2 Rabin -- 13.3.3 Elgamal -- 13.3.4 Cramer-Shoup -- 13.4 IDENTITY-BASED ENCRYPTION -- 13.5 FULLY HOMOMORPHIC ENCRYPTION -- 13.6 FINAL REMARKS -- References -- Chapter 14 Digital Signatures -- 14.1 INTRODUCTION -- 14.2 DIGITAL SIGNATURE SYSTEMS -- 14.2.1 RSA -- 14.2.2 PSS and PSS-R -- 14.2.3 Rabin -- 14.2.4 Elgamal -- 14.2.5 Schnorr -- 14.2.6 DSA -- 14.2.7 ECDSA -- 14.2.8 Cramer-Shoup -- 14.3 IDENTITY-BASED SIGNATURES -- 14.4 ONE-TIME SIGNATURES -- 14.5 VARIANTS -- 14.5.1 Blind Signatures -- 14.5.2 Undeniable Signatures -- 14.5.3 Fail-Stop Signatures -- 14.5.4 Group Signatures -- 14.6 FINAL REMARKS -- References -- Chapter 15 Zero-Knowledge Proofs of Knowledge -- 15.1 INTRODUCTION -- 15.2 ZERO-KNOWLEDGE AUTHENTICATION PROTOCOLS -- 15.2.1 Fiat-Shamir -- 15.2.2 Guillou-Quisquater --

15.2.3 Schnorr -- 15.3 NONINTERACTIVE ZERO-KNOWLEDGE -- 15.4 FINAL REMARKS -- References -- Part IV CONCLUSIONS -- Chapter 16 Key Management -- 16.1 INTRODUCTION -- 16.1.1 Key Generation -- 16.1.2 Key Distribution -- 16.1.3 Key Storage -- 16.1.4 Key Destruction -- 16.2 SECRET SHARING -- 16.2.1 Shamir's System -- 16.2.2 Blakley's System -- 16.2.3 Verifiable Secret Sharing -- 16.2.4 Visual Cryptography -- 16.3 KEY RECOVERY -- 16.4 CERTIFICATE MANAGEMENT -- 16.4.1 Introduction -- 16.4.2 X.509 Certificates -- 16.4.3 OpenPGP Certificates -- 16.4.4 State of the Art -- 16.5 FINAL REMARKS -- References -- Chapter 17 Summary.
17.1 UNKEYED CRYPTOSYSTEMS -- 17.2 SECRET KEY CRYPTOSYSTEMS -- 17.3 PUBLIC KEY CRYPTOSYSTEMS -- 17.4 FINAL REMARKS -- Chapter 18 Outlook -- 18.1 THEORETICAL VIEWPOINT -- 18.2 PRACTICAL VIEWPOINT -- 18.3 PQC -- 18.3.1 Code-based Cryptosystems -- 18.3.2 Hash-based Cryptosystems -- 18.3.3 Lattice-based Cryptosystems -- 18.3.4 Isogeny-based Cryptosystems -- 18.3.5 Multivariate-based Cryptosystems -- 18.4 CLOSING REMARKS -- References -- Appendix A Discrete Mathematics -- A.1 ALGEBRAIC BASICS -- A.1.1 Preliminary Remarks -- A.1.2 Algebraic Structures -- A.1.3 Homomorphisms -- A.1.4 Permutations -- A.2 INTEGER ARITHMETIC -- A.2.1 Integer Division -- A.2.2 Common Divisors and Multiples -- A.2.3 Euclidean Algorithms -- A.2.4 Prime Numbers -- A. 2.5 Factorization -- A.2.6 Euler's Totient Function -- A.3 MODULAR ARITHMETIC -- A.3.1 Modular Congruence -- A.3.2 Modular Exponentiation -- A.3.3 Chinese Remainder Theorem -- A.3.4 Fermat's Little Theorem -- A.3.5 Euler's Theorem -- A.3.6 Finite Fields Modulo Irreducible Polynomials -- A.3.7 Quadratic Residuosity -- A.3.8 Blum Integers -- References -- Appendix B Probability Theory -- B.1 BASIC TERMS AND CONCEPTS -- B.2 RANDOM VARIABLES -- B.2.1 Probability Distributions -- B.2.2 Marginal Distributions -- B.2.3 Conditional Probability Distributions -- B.2.4 Expectation -- B.2.5 Independence of Random Variables -- B.2.6 Markov's Inequality -- B.2.7 Variance and Standard Deviation -- B.2.8 Chebyshev's Inequality -- References -- Appendix C  Information Theory -- C.1 INTRODUCTION -- C.2 ENTROPY -- C.2.1 Joint Entropy -- C.2.2 Conditional Entropy -- C.2.3 Mutual Information -- C.3 REDUNDANCY -- C.4 KEY EQUIVOCATION AND UNICITY DISTANCE -- References -- Appendix D Complexity Theory -- D.1 PRELIMINARY REMARKS -- D.2 INTRODUCTION -- D.3 ASYMPTOTIC ORDER NOTATION -- D.4 EFFICIENT COMPUTATIONS -- D.5 COMPUTATIONAL MODELS.
D.6 COMPLEXITY CLASSES -- D.6.1 Complexity Class P -- D.6.2 Complexity Classes NP and coNP -- D.6.3 Complexity Class PP and Its Subclasses -- D.7 FINAL REMARKS -- References -- List of Symbols -- Abbreviations and Acronyms -- About the Author -- Index.