

|                         |   |
|-------------------------|---|
| 1. Record Nr.           | UNINA9910139648303321   |
| Autore                  | Stamp Mark  |
| Titolo                  | Information security [[electronic resource] ] : principles and practice // Mark Stamp   |
| Pubbl/distr/stampa      | Hoboken, NJ, : Wiley, c2011   |
| ISBN                    | 1-283-13887-5<br>9786613138873<br>1-118-02796-5<br>1-118-02797-3<br>1-118-02795-7   |
| Edizione                | [2nd ed.]   |
| Descrizione fisica      | 1 online resource (608 p.)  |
| Classificazione         | COM053000   |
| Disciplina              | 005.8   |
| Soggetti                | Computer security<br>Data protection<br>Electronic books.   |
| Lingua di pubblicazione | Inglese   |
| Formato                 | Materiale a stampa  |
| Livello bibliografico   | Monografia  |
| Note generali           | Description based upon print version of record.   |
| Nota di bibliografia    | Includes bibliographical references (p. 531-571) and index.   |
| Nota di contenuto       | Information Security: Principles and Practice; Contents; Preface; About The Author; Acknowledgments; 1 Introduction; 1.1 The Cast of Characters; 1.2 Alice's Online Bank; 1.2.1 Confidentiality, Integrity, and Availability; 1.2.2 Beyond CIA; 1.3 About This Book; 1.3.1 Cryptography; 1.3.2 Access Control; 1.3.3 Protocols; 1.3.4 Software; 1.4 The People Problem; 1.5 Principles and Practice; 1.6 Problems; I Crypto; 2 Crypto Basics; 2.1 Introduction; 2.2 How to Speak Crypto; 2.3 Classic Crypto; 2.3.1 Simple Substitution Cipher; 2.3.2 Cryptanalysis of a Simple Substitution; 2.3.3 Definition of Secure 2.3.4 Double Transposition Cipher2.3.5 One-Time Pad; 2.3.6 Project VENONA; 2.3.7 Codebook Cipher; 2.3.8 Ciphers of the Election of 1876; 2.4 Modern Crypto History; 2.5 A Taxonomy of Cryptography; 2.6 A Taxonomy of Cryptanalysis; 2.7 Summary; 2.8 Problems; 3 Symmetric Key Crypto; 3.1 Introduction; 3.2 Stream Ciphers; 3.2.1 A5/1; 3.2.2 RC4; 3.3 Block Ciphers; 3.3.1 Feistel Cipher; 3.3.2 DES; 3.3.3 Triple DES; 3.3.4 AES; 3.3.5 Three More Block Ciphers; 3.3.6 TEA; 3.3.7 Block Cipher Modes; 3.4 Integrity; 3.5 Summary; 3.6 Problems; 4 Public Key |

Crypto; 4.1 Introduction; 4.2 Knapsack; 4.3 RSA  
 4.3.1 Textbook RSA Example 4.3.2 Repeated Squaring; 4.3.3 Speeding  
 Up RSA; 4.4 Diffie-Hellman; 4.5 Elliptic Curve Cryptography; 4.5.1  
 Elliptic Curve Math; 4.5.2 ECC Diffie-Hellman; 4.5.3 Realistic Elliptic  
 Curve Example; 4.6 Public Key Notation; 4.7 Uses for Public Key Crypto;  
 4.7.1 Confidentiality in the Real World; 4.7.2 Signatures and Non-  
 repudiation; 4.7.3 Confidentiality and Non-repudiation; 4.8 Public Key  
 Infrastructure; 4.9 Summary; 4.10 Problems; 5 Hash Functions++; 5.1  
 Introduction; 5.2 What is a Cryptographic Hash Function?; 5.3 The  
 Birthday Problem; 5.4 A Birthday Attack  
 5.5 Non-Cryptographic Hashes 5.6 Tiger Hash; 5.7 HMAC; 5.8 Uses for  
 Hash Functions; 5.8.1 Online Bids; 5.8.2 Spam Reduction; 5.9  
 Miscellaneous Crypto-Related Topics; 5.9.1 Secret Sharing; 5.9.2  
 Random Numbers; 5.9.3 Information Hiding; 5.10 Summary; 5.11  
 Problems; 6 Advanced Cryptanalysis; 6.1 Introduction; 6.2 Enigma;  
 6.2.1 Enigma Cipher Machine; 6.2.2 Enigma Keyspace; 6.2.3 Rotors;  
 6.2.4 Enigma Attack; 6.3 RC4 as Used in WEP; 6.3.1 RC4 Algorithm;  
 6.3.2 RC4 Cryptanalytic Attack; 6.3.3 Preventing Attacks on RC4; 6.4  
 Linear and Differential Cryptanalysis; 6.4.1 Quick Review of DES  
 6.4.2 Overview of Differential Cryptanalysis 6.4.3 Overview of Linear  
 Cryptanalysis; 6.4.4 Tiny DES; 6.4.5 Differential Cryptanalysis of TDES;  
 6.4.6 Linear Cryptanalysis of TDES; 6.4.7 Implications Block Cipher  
 Design; 6.5 Lattice Reduction and the Knapsack; 6.6 RSA Timing  
 Attacks; 6.6.1 A Simple Timing Attack; 6.6.2 Kocher's Timing Attack;  
 6.7 Summary; 6.8 Problems; II Access Control; 7 Authentication; 7.1  
 Introduction; 7.2 Authentication Methods; 7.3 Passwords; 7.3.1 Keys  
 Versus Passwords; 7.3.2 Choosing Passwords; 7.3.3 Attacking Systems  
 via Passwords; 7.3.4 Password Verification  
 7.3.5 Math of Password Cracking

## Sommario/riassunto

Now updated-your expert guide to twenty-first century information  
 security Information security is a rapidly evolving field. As businesses  
 and consumers become increasingly dependent on complex  
 multinational information systems, it is more imperative than ever to  
 protect the confidentiality and integrity of data. Featuring a wide array  
 of new information on the most current security issues, this fully  
 updated and revised edition of Information Security: Principles and  
 Practice provides the skills and knowledge readers need to tackle any  
 information security challenge. Taking a pract