1. Record Nr. UNINA9910143434303321

Autore	Konheim Alan G. <1934->
Titolo	Computer security and cryptography [[electronic resource] /] / Alan G. Konheim
Pubbl/distr/stampa	Hoboken, N.J., : Wiley-Interscience, c2007
ISBN	1-280-82189-2 9786610821891 0-470-08398-0 0-470-08397-2
Edizione	[1st edition]
Descrizione fisica	1 online resource (541 p.)
Disciplina	005.8
Soggetti	Computer security Cryptography 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 and index.
Nota di contenuto	COMPUTER SECURITY AND CRYPTOGRAPHY; CONTENTS; FOREWORD; PREFACE; ACKNOWLEDGMENTS; ABOUT THE AUTHOR; CHAPTER 1 APERITIFS; 1.1 The Lexicon of Cryptography; 1.2 Cryptographic Systems; 1.3 Cryptanalysis; 1.4 Side Information; 1.5 Thomas Jefferson and the M-94; 1.6 Cryptography and History; 1.7 Cryptography and Computers; 1.8 The National Security Agency; 1.9 The Giants; 1.10 No Sex, Money, Crime or . . . Love; 1.11 An Example of the Inference Process in Cryptanalysis; 1.12 Warning!; CHAPTER 2 COLUMNAR TRANSPOSITION; 2.1 Shannon's Classification of Secrecy Transformations 2.2 The Rules of Columnar Transposition Encipherment2.3 Cribbing; 2.4 Examples of Cribbing; 2.5 Plaintext Language Models; 2.6 Counting k-Grams; 2.7 Deriving the Parameters of a Markov Model from Sliding Window Counts; 2.8 Markov Scoring; 2.9 The ADFGVX Transposition System; 2.10 CODA; 2.11 Columnar Transposition Problems; CHAPTER 3 MONOALPHABETIC SUBSTITUTION; 3.1 Monoalphabetic Substitution; 3.2 Caesar's Cipher; 3.3 Cribbing Using Isomorphs; 3.4 The x(2)-Test of a Hypothesis; 3.5 Pruning from the Table of Isomorphs; 3.6 Partial

Maximum Likelihood Estimation of a Monoalphabetic Substitution
3.7 The Hidden Markov Model (HMM)3.8 Hill Encipherment of ASCII N-Grams; 3.9 Gaussian Elimination; 3.10 Monoalphabetic Substitution Problems; CHAPTER 4 POLYALPHABETIC SUBSTITUTION; 4.1 Running Keys; 4.2 Blaise de Vigenere; 4.3 Gilbert S. Vernam; 4.4 The One-Time Pad; 4.5 Finding the Key of Vernam-Vigenere Ciphertext with Known Period by Correlation; 4.6 Coincidence; 4.7 Venona; 4.8 Polyalphabetic Substitution Problems; CHAPTER 5 STATISTICAL TESTS; 5.1 Weaknesses in a Cryptosystem; 5.2 The Kolmogorov-Smirnov Test; 5.3 NIST's Proposed Statistical Tests; 5.4 Diagnosis
5.5 Statistical Tests ProblemsCHAPTER 6 THE EMERGENCE OF CIPHER MACHINES; 6.1 The Rotor; 6.2 Rotor Systems; 6.3 Rotor Patents; 6.4 A Characteristic Property of Conjugacy; 6.5 Analysis of a 1-Rotor System: Ciphertext Only; 6.6 The Displacement Sequence of a Permutation; 6.7 Arthur Scherbius; 6.8 Enigma Key Distribution Protocol; 6.9 Cryptanalysis of the Enigma; 6.10 Cribbing Enigma Ciphertext; 6.11 The Lorenz Schlusselzusatz; 6.12 The SZ40 Pin Wheels; 6.13 SZ40 Cryptanalysis Problems; 6.14 Cribbing SZ40 Ciphertext; CHAPTER 7 THE JAPANESE CIPHER MACHINES; 7.1 Japanese Signaling Conventions
7.2 Half-Rotors7.3 Components of the RED Machine; 7.4 Cribbing RED Ciphertext; 7.5 Generalized Vowels and Consonants; 7.6 "Climb Mount Itaka" - War!; 7.7 Components of the PURPLE Machine; 7.8 The PURPLE Keys; 7.9 Cribbing PURPLE: Finding the V-Stepper; 7.10 Cribbing PURPLE: Finding the C-Steppers; CHAPTER 8 STREAM CIPHERS; 8.1 Stream Ciphers; 8.2 Feedback Shift Registers; 8.3 The Algebra of Polynomials over Z(2); 8.4 The Characteristic Polynomial of a Linear Feedback Shift Register; 8.5 Properties of Maximal Length LFSR Sequences; 8.6 Linear Equivalence
8.7 Combining Multiple Linear Feedback Shift Registers

Sommario/riassunto

Gain the skills and knowledge needed to create effective data security systems This book updates readers with all the tools, techniques, and concepts needed to understand and implement data security systems. It presents a wide range of topics for a thorough understanding of the factors that affect the efficiency of secrecy, authentication, and digital signature schema. Most importantly, readers gain hands-on experience in cryptanalysis and learn how to create effective cryptographic systems. The author contributed to the design and analysis of the Data Encryption Standard (DES), a w