1.

Record Nr.	UNINA9910793156703321
Autore	Padhye Sahadeo
Titolo	Introduction to cryptography / / Sahadeo Padhye, Rajeev A. Sahu, Vishal Saraswat
Pubbl/distr/stampa	Boca Raton, FL : , : CRC Press, Taylor & Francis Group, , [2018] ©2018
ISBN	1-351-62815-1 1-315-11459-3 1-351-62813-5
Descrizione fisica	1 online resource (278 pages)
Disciplina	003/.54
Soggetti	Cryptography - Mathematics Number theory Algorithms
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	"A science publishers book."
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Notation Types of algorithm Complexity Classes Exercise Classical Cryptosystems Classification of Classical Cryptosystem Block Cipher Stream Cipher Cryptanalysis of Cryptosystems Exercise Block Ciphers Introduction Modes of Operation Padding Design Considerations Data Encryption Standard Advanced Encryption Standard Exercise Hash Function Compression and Hash Functions Hash function for cryptography Random Oracle Model Cryptographic Hash Functions Exercise Public Key Cryptosystem Introduction Diffie-Hellman Key Exchange Protocol RSA Cryptosystem Rabin Cryptosystem ElGamal Cryptosystem Elliptic Curve Cryptosystem Exercises Digital Signature Formal Definitions Attack Goals for Digital. Cover; Title Page; Copyright Page; Dedication; Foreword; Preface; Table of Contents; 1 Overview of Cryptography; 1.1 Introduction; 1.2 Goals of Cryptography; 1.3 Classification of Cryptosystem; 1.4 Practically Useful Cryptosystem; 1.4.1 Confusion and Diffusion; 1.5 Cryptanalysis; 1.5.1 Types of Attackers; 1.5.2 Types of Attacks; 1.5.3 Security Notions; 2 Basic Algebra; 2.1 Group; 2.2 Ring; 2.3 Field; 2.3.1 Finite Field; 2.3.2 Field Construction; 2.3.3 Field Construction using Irreducible

Polynomial; 2.3.4 Galois Field GF(2n); 2.3.4.1 Integer Representation of Finite Field Elements.

2.3.5 Field Construction using Generator2.4 Exercises; 3 Number Theory; 3.1 Prime Numbers; 3.2 Cardinality of Primes; 3.3 Extended Euclidean Algorithm; 3.4 Congruences; 3.4.1 Solving Linear Congruence in Zn; 3.4.2 Chinese Remainder Theorem (CRT); 3.5 Integer Factorization Problem; 3.5.1 Trial Division Method; 3.5.2 Fermat's Method; 3.5.3 Pollard's p -- 1 Method; 3.5.4 Pollard's Rho Method; 3.5.5 Quadratic Sieve; 3.5.6 Number Field Sieve; 3.6 Primality Testing; 3.6.1 Sieve of Eratosthenes; 3.6.2 Divisibility Algorithm; 3.6.3 AKS Algorithm; 3.6.4 Fermat Test; 3.6.5 Miller-Rabin Algorithm.

3.7 Quadratic Congruence3.7.1 Quadratic Residue or Non-Residue; 3.7.2 Legendre Symbol and Jacobi Symbol; 3.8 Exponentiation and Logarithm; 3.8.1 Square and Multiply Method; 3.9 Discrete Logarithm Problem; 3.9.1 Shank's Baby-Step Giant-Step Algorithm; 3.9.2 Pollard's Rho Algorithm; 3.9.3 Pohlig-Hellman Algorithm; 3.9.4 Index Calculus Algorithm; 3.10 Exercises; 4 Probability and Perfect Secrecy; 4.1 Basic Concept of Probability; 4.2 Birthday Paradox; 4.3 Perfect Secrecy; 4.4 Vernam One-Time Pad; 4.5 Random Number Generation; 4.6 Pseudo-random Number Generator; 4.7 Exercises; 5 Complexity Theory.

5.1 Running Time and Size of Input5.2 Big-O Notation; 5.2.1 Big-O and Growth Rate; 5.2.2 Properties of Order Notation; 5.3 Types of Algorithm; 5.4 Complexity Classes; 5.5 Exercises; 6 Classical Cryptosystems; 6.1 Classification of Classical Cryptosystem; 6.2 Block Cipher; 6.2.1 Substitution Cipher; 6.2.1.1 Shift Cipher; 6.2.1.2 Affine Cipher; 6.2.1.3 Substitution Cipher; 6.2.1.4 Vigenere Cipher; 6.2.1.5 Hill Cipher; 6.2.2 Transposition Cipher; 6.2.2.1 Scytale; 6.2.2.2 The Rail Fence Cipher; 6.3 Stream Cipher; 6.3.1 Synchronous Stream Cipher.

6.3.1.1 Vigenere Cipher as Synchronous Stream Cipher6.3.2 Linear Feedback Shift Register (LFSR); 6.3.3 Non-Synchronous Stream Cipher; 6.3.3.1 Autokey Cipher; 6.4 Cryptanalysis of Cryptosystems; 6.4.1 Frequency Analysis; 6.4.2 Cryptanalysis of Affine Cipher; 6.4.3 Cryptanalysis of Substitution Cipher; 6.4.4 Cryptanalysis of Vigenere Cipher; 6.4.5 Cryptanalysis of Hill Cipher; 6.4.6 Cryptanalysis of LFSR Stream Cipher; 6.5 Exercises; 7 Block Ciphers; 7.1 Introduction; 7.1.1 Notations; 7.2 Modes of Operation; 7.2.1 Electronic Code Book (ECB); 7.2.1.1 ECB Properties.

Sommario/riassunto

"Electronic communication and financial transactions have assumed massive proportions today. But they comprise high risks too. Achieving cyber security has become a top priority, and has become one of the most crucial areas of study and research in IT.?This book introduces readers to perhaps the most effective tool in achieving a secure environment, i.e. cryptography. Students who have elementary knowledge of mathematics, will be introduced to mathematical notions relevant to cryptography, and the design and analysis of the cryptographic schemes. More advanced students who have already a background of algebra, number theory, probability and algorithms; will be able to review the applications of secure systems and will be introduced to cryptographic primitives and current research, besides being exposed to scope of future research addressing the open problems in related area. This book gives more solved examples than most books on the subject, it includes state of the art topics and discusses the scope of future research."--Provided by publisher.