1. Record Nr. UNINA9910503003203321

Autore	Mihailescu Marius Iulian
Titolo	Cryptography and cryptanalysis in MATLAB : creating and programming advanced algorithms / / Marius Iulian Mihailescu, Stefania Loredana Nita
Pubbl/distr/stampa	New York, NY : , : Apress, , [2021] ©2021
ISBN	1-4842-7334-6
Descrizione fisica	1 online resource (201 pages)
Disciplina	005.8
Soggetti	Cryptography - Standards Cryptography
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Table of Contents -- About the Authors -- About the Technical Reviewer -- Chapter 1: Getting Started in Cryptography and Cryptanalysis -- Cryptography and Cryptanalysis -- Book Structure -- Conclusion -- References -- Chapter 2: MATLAB Cryptography Functions -- Conclusion -- References -- Chapter 3: Conversions Used in MATLAB for Cryptography -- Conclusion -- References -- Chapter 4: Basic Arithmetic Foundations -- Euclid's Division Lemma -- Greatest Common Divisor (gcd) -- Euclid's Algorithm -- The Extended Euclidean Algorithm -- Practical Implementations -- The Extended Euclidean Algorithm -- Prime Factors in MATLAB -- Computing the Modular Inverse -- Conclusion -- References -- Chapter 5: Number Theory -- Primality and Factorization -- Prime Numbers -- The Prime Number Theorem -- Congruency -- Inverse -- Chinese Remainder Theorem -- Primality Tests -- The Wilson Primality Test -- The Little Fermat Primality Test -- The Miller-Rabin Primality Test -- Algebraic Structures -- Conclusion -- References -- Chapter 6: Classic Cryptography -- Symmetric Cryptography -- Classic Ciphers -- The Caesar Cipher -- Example -- Mathematical Background -- Cryptanalysis -- Implementing the Caesar Cipher -- The Vigenère Cipher -- Example -- Mathematical Background -- Implementing the Vigenère Cipher -- The Hill Cipher -- Example -- Cryptanalysis --

Implementing the Hill Cipher -- Conclusion -- References -- Chapter 7: Pseudo-Random Number Generators -- Simple PRNGs -- Linear Congruential Generators -- Ranrot Generators -- Blum-Blum-Shub Generator -- Linear Circuit PRNGs -- Other PRNGs -- Practical Implementations -- Conclusion -- References -- Chapter 8: Hash Functions -- Security of Hash Functions -- Cryptographic Hash Functions -- Birthday Attack -- MD4 Function -- MD4 Function Description -- Cryptanalysis of MD4 -- MD5 Function -- SHA1 Function.
Implementing Hash Functions -- Implementing SHA-1/256/368/512, MD2, and MD5 -- Conclusion -- References -- Chapter 9: Block Ciphers: DES and AES -- Preliminaries -- Networks Based on Substitution and Permutation -- Attacks Based on Linear Cryptanalysis -- Attacks Based on Differential Cryptanalysis -- The Data Encryption Standard (DES) -- DES Description -- Implementation of DES -- The Advanced Encryption System (AES) -- SubBytes Operations -- The ShiftRows Operation -- The MixColumn Operation -- The AddRoundKey Operation -- Key Expansion -- InvSubBytes Operation -- InvShiftRows Operation -- InvMixColumns Operation -- Conclusion -- References -- Chapter 10: Asymmetric Encryption Schemes -- RSA -- ElGamal -- Merkle-Hellman -- Knapsack Approach -- The Algorithms -- Conclusion -- References -- Chapter 11: Formal Techniques for Cryptography -- Probability Theory -- Random Variables -- Birthday Problem -- Entropy -- Randomness in Cryptography -- Conclusion -- References -- Chapter 12: Visual Cryptography -- Conclusion -- References -- Chapter 13: Chaos-Based Cryptography -- Chaos Maps and Functions -- Logistic Map -- Chaos Theory in Cryptography -- Sensitivity to Initial Conditions -- Conclusion -- References -- Chapter 14: Steganography -- Algorithms and Methods for Different Steganography Types -- Steganography for Image Files -- Steganography for Audio Files -- Steganography for Video Files -- Practical Implementation -- Implementing the Least Significant Bit (LSB) Method -- Implementing the Histogram Analysis Method -- Conclusion -- References -- Index.