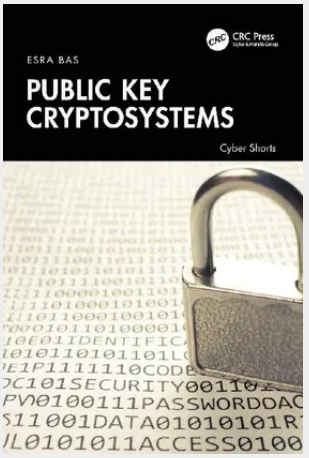
Bas

Public Key Cryptosystems



This book is a short book about public key cryptosystems, digital signature algorithms, and their basic cryptanalysis which are provided at a basic level so that it can be easy to understand for the undergraduate engineering students who can be defined as the core audience. To provide the necessary background, Chapters 1 and 2 are devoted to the selected fundamental concepts in cryptography mathematics and selected fundamental concepts in cryptography. Chapter 3 is devoted to discrete logarithm problem (DLP), DLP-related public key cryptosystems, digital signature algorithms, and their cryptanalysis. In this chapter, the elliptic curve counterparts of the algorithms and the basic algorithms for the solution of DLP are also given. In Chapter 4, RSA public key cryptosystem, RSA digital signature algorithm, the basic cryptanalysis approaches, and the integer factorization methods are provided. Chapter 5 is devoted to GGH and NTRU public key cryptosystems, GGH and NTRU digital signature algorithms, and the basic cryptanalysis approaches, whereas Chapter 6 covers other topics including knapsack cryptosystems, identity-based public key cryptosystems, identity-based digital signature algorithms, Goldwasser-Micali probabilistic public key cryptosystem, and their cryptanalysis. The book's distinctive features: - The book provides some fundamental mathematical and conceptual preliminaries required to understand the core parts of the book. - The book comprises the selected public key cryptosystems, digital signature algorithms, and the basic cryptanalysis approaches for these cryptosystems and algorithms. - The cryptographic algorithms and most of the solutions of the examples are provided in a structured table format to support easy learning. - The concepts and algorithms are illustrated with examples, some of which are revisited multiple times to present alternative approaches. - The details of the topics covered in the book are intentionally not presented; however, several references are provided at the end of each chapter so that the reader can read those references for more details.

This book is a short book about public key cryptosystems, digital signature algorithms, and their basic cryptanalysis which are provided at a basic level so that it can be easy to understand for the undergraduate engineering students who can be defined as the core audience.

76,00 €
76,00 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9781032846231
Medium: Buch
ISBN: 978-1-032-84623-1
Verlag: CRC Press
Erscheinungstermin: 30.12.2024
Sprache(n): Englisch
Auflage: 1. Auflage 2024
Serie: Cyber Shorts
Produktform: Kartoniert
Gewicht: 278 g
Seiten: 174
Format (B x H): 156 x 234 mm

Kundenservice Verlag Dr. Otto Schmidt KG
Neumannstraße 10, 40235 Düsseldorf | kundenservice@otto-schmidt.de | 0221-93738-997 (Inland)