Review of the book

"Introduction to Cryptography"

by Alexander Stanoyevetich

CRC Press, Taylor & Francis Group, 2011

ISBN: 978-1-4398-1763-6

S. V. Nagaraj
RMK Engineering College

2011-04-22

1 What the book is about

The book offers an introduction to cryptography with focus on its mathematical foundations and computer implementations. The book is published under the Chapman and Hall / CRC Press series on Discrete Mathematics and its Applications.

The book is made up of twelve chapters and five appendices.

Chapter 1 (An Overview of the Subject) is an introduction to the subject matter discussed in the book. Some key definitions and general concepts of cryptography are introduced. There are inspiring photographs of some cryptographers. These and other details contained in the chapter provide some insights into the historical aspects of cryptography.

Chapter 2 (Divisibility and Modular Arithmetic) discusses Euclid's algorithm, the extended Euclidean algorithm, modular arithmetic, congruences, and the Chinese remainder theorem.

Chapter 3 (The Evolution of Codemaking until the Computer Era) discusses the evolution of code making before computers came into existence. Ancient codes, affine ciphers, steganography, and the Enigma machines are described.

Chapter 4 (Matrices and the Hill Cryptosystem) discusses matrix operations including matrix addition, subtraction, and multiplication. Techniques for computing determinants, the inverse and the transpose of matrices are also studied. The Hill cryptosystem is introduced. This cryptosystem makes use of modular matrix multiplication by invertible matrices.

Chapter 5 (The Evolution of Codebreaking until the Computer Era) describes frequency analysis and its use in ciphertext only attacks on substitution ciphers. Ciphertext only attacks on the Vignere cipher and attacks on Enigma are also discussed.

Chapter 6 (Representation and Arithmetic of Integers in Different Bases) deals with ways of representing integers in different bases. Arithmetic operations using such bases are also covered.

Chapter 7 (Block Cryptosystems and the Data Encryption Standard (DES)) discusses the rise and fall of the Data Encryption Standard. Triple DES and modes of operation for block cryptosystems are studied.

Chapter 8 (Some Number Theory and Algorithms) contains information about the prime number theorem, Fermat's little theorem, the Euler Phi function, primitive roots, Fermat's primality test, Carmichael numbers, the Miller-Rabin primality test, and the Pollard's $p-1$ factoring algorithm.

Chapter 9 (Public Key Cryptography) describes the Diffie-Hellman key exchange protocol, the Rivest Shamir Adleman cryptosystem, the ElGamal cryptosystem, and the Merkle-Hellman knapsack cryptosystem.

Chapter 10 (Finite Fields in General, and GF(2^8) in Particular) discusses topics such as rings, fields, divisibility in rings, and the Euclidean algorithm for polynomials. Special mention is made about GF(2^n) in general and GF(2^8) in particular.

Chapter 11 (The Advanced Encryption Standard (AES) Protocol) mentions about the calls that were made for a replacement to the DES. A scaled down version of the AES, decryption in that version, and the AES encryption and decryption algorithms are described. The security of AES is briefly looked at.

Chapter 12 (Elliptic Curve Cryptography) discusses elliptic curves over the reals, modular elliptic curves, the discrete logarithm problem on modular elliptic curves, elliptic curve versions of the Difie-Hellman key exchange and the ElGamal cryptosystem. There is also a description of a factoring algorithm using elliptic curves.

The book includes appendices on sets and basic counting principles, randomness and probability, solutions to all exercises for the reader, answers and brief solutions to selected odd-numbered exercises, and suggestions for further reading. The book includes a short list of references to the literature. The book includes three indices. One index covers corollaries, lemmas, propositions, and theories. Whereas the second index is for algorithms discussed in the book and the third index is a subject index.

2 What is the book like (style)?

The book is very readable and therefore suitable for teaching undergraduate students. Cryptography is a hot topic these days and familiarity with its basics will be helpful for students with varied backgrounds. It will be suitable for students of mathematics as well as computer science. The author has kept the prerequisites to a bare minimum. The author tries to make the book interesting by including historical details. The style of presentation is pleasant. The details have been presented in a manner students will find absorbing. Adequate examples, tables and illustrations make understanding difficult concepts easy. The chapters of the book include exercises as well as computer implementations and exercises based on them. The appendices contain useful information. They include solutions to all exercises for the reader as well as answers and brief solutions to selected odd-numbered exercises. Some suggestions for further reading have also been included in an appendix. The author has provided some references to the literature. However, my feeling is that a more comprehensive list of references would have been more helpful. The author has provided a supporting Web site that includes an extensive set of sample programs and downloadable platform-independent applet pages. The book is more or less self-contained. The coverage of elliptic curve cryptography is laudable. Algorithms have been presented using readable pseudo-code. There are many books in the market that cover topics discussed in the book, however, this book is very readable and stimulating.

3 Would you recommend this book?

This book is a very comprehensible introduction to cryptography. It will be very suitable for undergraduate students. There is adequate material in the book for teaching one or two courses on cryptography. The author has provided many mathematically oriented as well as computer-based exercises. I strongly recommend this book as an introductory book on cryptography for undergraduates.

The reviewer is a Professor at the CSE Dept., RMK Engg. College, Kavaraipettai, Tamil Nadu, India