Review of the book

"Introduction to Modern Cryptography"

by Jonathan Katz and Yehuda Lindell

Chapman & Hall CRC, 2008

ISBN: 1-58488-551-3, 978-1-584-885-511

Ladan Mahabadi
McGill University

February 2011

1 Summary of the review

The following reviews **Introduction to Modern Cryptography** by Jonathan Katz and Yehuda Lindell. It is the goal of this review to provide a brief, general overview of this book and advocate for its use. This review highlights topics covered, their significance in the global context of cryptography and the text's potential audience.

2 Summary of the book

The influence of digital computation and communications in daily lives is undeniable. It is this ubiquitous technological presence that has made cryptography - a rigorous study of security, authentication and data integrity - both relevant and indispensable.

The Katz-Lindell book was received very well by the cryptographic research community, and soon after its publication, it became well known as one of the *it* books in this field. Currently, it is considered by many experts in the field to be a thorough reference for cryptographic notions and algorithms.

By highlighting the significance of mathematical definitions and providing rigorous proofs, the authors demystify cryptography as not a field of ad-hoc procedures but rather a field enriched by beautiful theoretical concepts and algorithms. This emphasis of the mathematical framework that has shaped cryptography in the past few decades, is perhaps one of the most significant contributions of this book. The authors, in essence, highlight the fundamental tenets of cryptography: rigorous definitions, clear statement of assumptions and thorough proofs.

3 What is the book like (style)?

Katz and Lindell provide a very intuitive approach to some of the most fundamental and abstract notions of cryptography. Moreover, while emphasizing the need for proofs, they also highlight applications of these notions or algorithms whenever possible.

The book starts by providing a brief history of cryptography, the first ciphers and their crypt-analysis. It moves on to mathematically define the notion of security. It does so by introducing concepts first introduced by Shannon (perfect security) followed by a more computationally feasible approach (semantic security).

The task of securing information is achieved through encryption algorithms which are divided into private and public key categories each of which receives ample attention and coverage. Private-key security (symmetric security) is followed by data integrity. Here, message authentication codes and collision-resistant hash functions are introduced and studied. Of course, cryptography without randomness will appear limited, and so the text devotes two chapters to the construction (both theoretical and practical) of pseudorandom generators. Then, focus is shifted to public-key cryptography.

Public-key cryptography (asymmetric security) applies fundamental notions of number theory to construct encryption algorithms that are provably secure (while making certain hardness or feasibility assumptions) and yet free of certain constraints of symmetric security, making them great candidates for data security and privacy in many applications and settings. The authors start by introducing the needed number theoretical notions and proceed to key management algorithms followed by commonly used encryption algorithms (such as the RSA).

Finally, the authors discuss data integrity techniques in the public-key setting. These are algorithms that enable senders to sign the data, and the receivers to verify that the sender is indeed the appropriate individual and that the data has not been manipulated during transmission. The book ends with supplementary notes on probability and algorithmic number theory.

4 Would you recommend this book?

The authors masterfully create a balance between mathematical formalism and application throughout this book. It is precisely this balance that makes this text accessible to a large audience. The topics covered are fundamental topics relevant to any researcher being introduced to cryptography, and at the same time the coverage is sufficiently thorough to make the book a reference for more advanced researchers or graduate students.

The intuitive approach of the text makes introduction to the fundamental issues of cryptography easy to grasp for new researchers and graduate students, and the rigorous definitions and proofs, followed by applications or open questions posed throughout the text, will appeal to more advanced researchers both new to or experienced in cryptography.

Cryptographic notions such as security may appear to be abstract or purely conceptual to many, however, the authors here, by providing intuitive and yet precise definitions and proofs, make the journey to better understanding and devising cryptographic protocols and algorithms enjoyable.

In my view, emphasizing the need for precise definitions, clear statements of assumptions and rigorous proofs throughout the book is its most valuable virtue since it teaches the principles of research to graduate students commencing their research careers in cryptography.

This book hopefully will not only introduce researchers to cryptography, but also inspire them for further rigorous advancements. As a young researcher in cryptography, I found the book very intuitive, and recommend the book to others both as an introductory and a reference book.

The reviewer is PhD candidate in Computer Science at McGill University.