Review of the book

"Introduction to Modern Cryptography"

by Jonathan Katz, Yehuda Lindell

Chapman & Hall/CRC, 2008

ISBN: 978-1-58488-551-1

Maria Cristina Onete
CASED (TU Darmstadt)

1 What the book is about

This book is a comprehensive, rigorous introduction to what the authors name "Modern" Cryptography, or in other words, the science — rather than the art — of cryptography, relying on: concrete definitions of security; formal, precise, as-few-as-possible assumptions; and rigorous proofs of security. In itself, this definition-based structure represents a novel approach to how cryptography is taught, replacing the older, construction-based approach. The book, though by no means complete, presents a thorough overview of the following subjects: block ciphers, symmetric encryption, message authentication, hash functions, (pseudo)randomness, hardness assumptions for asymmetric public key cryptography, key management, public key encryption schemes, digital signatures, the random oracle model, and a selection of cryptanalysis methods for factoring and finding discrete logarithms. To this end, the authors also give an overview of the necessary mathematical background and of the tools used in cryptography, amongst which I mention: probability notions, the Birthday problem, integer and modular arithmetic number-theory notions, and the problem of finding generators of cyclic groups. Though the authors mention some basic notions of side-channel attacks and general hardware issues, these topics are not considered in the scope of the book.

The treatment of each subject is extensive; nonetheless each of the thirteen chapters also offers good suggestions for additional reading, and exercises meant to both stimulate the student's capacity of using the theoretical knowledge he has gained, and to show concretely how this theory based approach may be put into practice. The authors specifically designed this book such that it presents what they feel are the core areas of cryptography, while several further, in-depth reading topics are marked with a star ("*").

The book is divided in three parts: an Introduction, the Symmetric Setting, and the Asymmetric Setting. A more interesting division is the one between what is considered to be core course material, and more advanced contents (marked with a star). This division is also shown in detail in the Preface, and is suc-

cinctly described below:

- Core contents:
  - Chapters 1-4: notions of classical and modern cryptography, the basic tools of public key cryptography;
  - Chapter 5: basic design principles for block ciphers; presentation of DES and AES;
  - Chapter 7: hard problems; concrete assumptions for RSA, Diffie-Hellman, and ElGamal constructions;
  - Chapters 9,10: the public key setting, and a discussion of public key encryption;
  - Chapter 12: digital signatures;
  - Sections 13.1, 13.3: the random oracle model, and the RSA-FDH signature scheme.
- More advanced contents:
  - Theoretic cryptography:
    - Section 3.2.2: semantic security for encryption;
    - Sections 4.8, 4.9: stronger security notions for encryption;
    - Chapter 6: one-way functions, hardcore bits, constructions of pseudorandom generators, functions, and permutations, starting from one-way permutations;
    - Section 10.7: public key encryption schemes from trapdoor permutations.
  - Applications:
    - Section 4.7: HMAC;
    - Chapter 13: further digital signature constructions in the random oracle model.
  - Mathematics:
    - Chapter 7: Chinese remainder theorem, elliptic curve groups;
    - Chapter 8: algorithms for factoring and for finding discrete logarithms;
    - Chapter 11: further encryption schemes due to Goldwasser-Micali, Rabin, Paillier.

2 What is the book like (style)?

Though quite a bit denser than the average introduction to cryptography, this book is not overwhelming. The concepts are clearly stated, both in an intuitive fashion and formally. The importance of precision and rigorousness is explained

and exemplified, so that a potential student may also understand the benefits of this approach and start thinking about cryptography in a structured, precise manner. This book is not suitable for the industry; indeed, it is not meant for such use. The reader must be familiar with some basic mathematical concepts and the science of proving statements. However, even a versed cryptographer will benefit from the rigorous and complete treatment of the mentioned topics.

Though the authors' approach is not construction-driven, but rather based on security definitions and models, several constructions of encryption, authentication, and digital signature schemes are presented and discussed. The writing is clear and fluent, and though there is some chapter inter-dependency, the writers make sure to briefly review the important concepts that will be used in a new chapter. One should count on reading passages of this book several times before they fully understand or place them into perspective. The authors prefer to delve into a smaller number of subjects rather deeply, than to give more shallow overviews of more subjects; therefore, the reader is recommended to use this book as a starting point and as a reference only, using the further reading suggestions to continue their studies.

One of the book's best qualities is the remarkably logical and systematic style in which the authors present several cryptographic primitives and constructions. Tremendous care has gone into including sufficient information to make this a thorough and interesting book, while at the same time not confusing or flooding the reader with information. It is also remarkable that even a reader with a good understanding of some cryptographic topics will find this book useful, both as a reference for future reading, and as an index of known results presented in a logical fashion.

A disadvantage of this book in my opinion is that it does not delve deeper into cryptographic methods such as authentication with limited resources, such as RFID, or PUF-based authentication. Quantum cryptography methods are not mentioned, nor explained. While the random oracle model is thoroughly explained, perhaps one could also include, in a starred section, the disadvantages of using the random oracle model and some constructions that are secure in the standard model. While a lot of care goes in proofs of security, the matter of privacy is not really introduced. Some references could also perhaps be made to areas of cryptography such as lattice, code-based, and multivariate cryptography. One should, however, take into account that these topics are slightly beyond the scope of an introductory book on cryptography, and as such, it is tricky to add this information without confusing the reader.

One of the best traits of this book is that it gives a unitary overview of the topics listed above in a logical fashion, such that the information becomes easy to process and the concepts have the time to settle properly after the reader has had the time to understand them. It is particularly useful for students to use this book as a guideline, as it has the capacity to improve one's analytical skills, channelling them towards a rigorous way of thinking about cryptography. Each subject is treated linearly: the authors begin by introducing a set of concepts; then, as the reader becomes familiar with them, these concepts are broadened to more generalised and more precise terminology and constructions. Occasionally,

the writers also give a list of "most popular wrong answers", in order to motivate their systematic approach and in order to show lapses in judgement. The light, and at the same time precise, way of writing is appealing and accurate. In this way, the knowledge at the end of each chapter is rounded and well built, and the reader may go on.

3 Would you recommend this book?

I would heartily recommend this book to anyone who is interested in cryptography. Apart from the intrinsic theory, the writing style involved presents quite a few proof methods and definitions that are useful in general in this domain. In addition, the exercises are challenging and interesting, and can benefit readers of all academic levels.

However, in order to make full use of the information presented here, the reader must have a good mathematical background and some analytical skills. One should be prepared to spend some time on understanding the more dense subsections and paragraphs, and I would recommend actually studying some of the suggested further readings, particularly in order to broaden the perspective that is given in the core sections of this piece of work.

The reviewer is a Ph.D. student at the Center for Advanced Security Research Darmstadt (CASED).