Review of the book

"Introduction to Cryptography, Principles and Applications Second Edition "

by Hans Delfs and Helmut Knebl
Springer, 2007

ISBN: 978-3-540-49243-6

Hasan Mirjalili
EPFL, Switzerland

1 Summary of the book

The book is divided into two parts. Chapters 1 to 4 cover basic concepts such as symmetric and asymmetric encryption, digital signatures and cryptographic protocols. The second part, Chapters 5 to 10, focus on more advanced topics and explain formally and precisely (with proofs) the concepts introduced in the first part.

Chapter 1 is an introduction to the concepts such as encryption and the objectives of cryptography, different types of attacks on encryption schemes, cryptographic protocols, and provable security. This chapter introduces the basics and gives pointer to the chapters where the concepts are explained in detail.

Chapter 2 describes block and stream ciphers and gives details about DES and AES algorithms and their modes of operation.

In Chapter 3, public-key cryptography is introduced. Mathematical concepts for understanding the idea behind public key cryptosystems are discussed including modular arithmetic, primes and factorization in adequate detail. These concepts make the reader ready for understanding RSA encryption/signature in next sections. Then a list of attacks against RSA is explained. Before opening the discussion about signature schemes, hash functions which are used in signature schemes are explained. The construction of Hash functions, their security requirement, attacks, and compression functions. Some hash functions such as SHA-1 and MD5 are briefly mentioned with their history and known attacks. Message authentication codes are discussed too. In the next topic of this chapter, discrete logarithm problem, ElGamal encryption and signature and DSS that are based on discrete logarithm problem are explained in detail. At the end Rabin's encryption and signature are discussed.

After describing cryptographic primitives in Chapters 1-3, the reader has adequate information for understanding cryptographic protocols in Chapter 4. This chapter covers five categories of cryptographic protocols: Key Exchange and Entity Authentication; Identification Schemes; Commitment Schemes; Electronic Elections; and Digital Cash protocols.

Chapter 5 explains probabilistic algorithms including Monte Carlo and Las Vegas algorithms to start discussing the subsequent chapters dealing with provable security and precise definition of the concepts mentioned in previous chapters. One-way functions and

the security assumptions behind public key cryptography are covered in Chapter 6. Bit security of the discrete logarithm, RSA function, and Square family with mathematical proofs are explained in detail in Chapter 7. Since computationally perfect pseudorandom bit generators can be derived from one-way permutations, in Chapter 8, the relation of one-way functions and pseudo-randomness is discussed including Yao's Theorem.
Chapter 9 and 10 cover provable security. Chapter 9 covers provably secure encryption cryptosystems and in Chapter 10, provably secure digital signatures are discussed. These two chapters explain mathematical proofs that show how a given cryptosystem resists certain types of attacks. Each chapter gives examples of provably secure encryption and signature schemes with their security proofs.

2 What is the book like (style)?

Given the title of the book "Introduction to Cryptography", one may expect an overview of all basic concepts of cryptography as it is customary in other introductory books, which start with history, definitions and key concepts. Reader may expect general information and not necessarily mathematical proofs and concepts behind cryptography. The book does not provide, for instance, the construction of well known hash functions SHA-1 or MD5, and there is no explanation about PKI, Elliptic Curve Cryptography, and quantum cryptography. Therefore the book may not satisfy someone who wants to have general information about cryptography. The book indicates in Preface, it is intended for advanced undergraduate and graduate students in computer science, mathematics and electrical engineering. The book includes exercises at the end of each chapter which are good for students. Some exercises are easy and some challenging. Chapters start with simple and clear introduction that makes the reader ready for diving into the subject of the chapter. Authors have attempted rigorously to explain every keyword and technical phrase and to give cross-reference to any topic used in a chapter which has been explained in other chapters. Hence, if a reader starts from a particular chapter and not from the beginning, he/she always has a pointer for finding more in other chapters. The focus of the book is rather on asymmetric cryptography, security proofs, and mathematical foundations and provable security.

3 Would you recommend this book?

I really enjoyed reading this book and I recommend it for students who have very basic understanding of cryptography and want to know more about mathematical basis and deeper concepts underlying cryptography. It has been written fluent, coherent and concise. There is almost no figure in the book and to my opinion, adding some figures would help readers particularly beginners to better understand subjects, e.g., figures for encryption algorithms or cryptographic protocols. The book targets people who are interested to know principles of security proofs and provably secure schemes. People who are focused more on topics like security management, system security, and network security are suggested to look for other books for introduction to cryptography.

The reviewer is a Ph.D. student at EPFL (École Polytechnique Fédérale de Lausanne).