Review of the book

"Introduction to Cryptography (Second Edition)"

by Johannes Buchmann

Springer, 2004

ISBN: 0-387-21156-X

by

Mohamed Saied Emam Mohamed

Technical University of Darmstadt (TUD), Germany

1 What the book is about

As the title states the book by Johannes Buchmann provides an introduction to cryptography. Buchmann's text in only 324 pages (excluding the appendices) presents a stand alone introduction to some modern cryptographic methods.

The book begins with the mathematical background that will be used as foundation for the cryptographic methods discussed in this book. Chapter one explains the important properties of integers and the extended Euclidean algorithm. Chapter two includes some important algebraic definitions (groups, residue class, ring, fields,...). Also, it contains algorithms for fast evaluation of power products and the Chinese remainder theorem. Probability theory and Shannon's view of perfect secrecy are presented in chapter 4.

There are three chapters discussing symmetric cryptography and to be more specific they are devoted to block ciphers. Chapter 3 explains the meaning of cryptosystems and gives some different encryption schemes. For the symmetric cryptography the author just defines the structure of stream ciphers and provides two examples, whereas he explains the block cipher in more details. Moreover chapter 5 and chapter 6 represent a complete study to the most famous block ciphers DES and AES, respectively.

In the next four chapters, the author discusses asymmetric cryptography (public key cryptography). Since many public key cryptosystems use large prime numbers, the author gives more additional mathematical preliminaries for the prime number generation and some algorithms used for testing the primality of large numbers in chapter 7. The idea of public key cryptosystems and a description to the most important schemes are given in chapter 8, for examples RSA and ElGamal. The security of RSA is based on the difficulty of the factorization problem and is studied in chapter 9. It is focusing on the quadratic sieve algorithm and providing an estimation to the efficiency of it and some other factoring algorithms. Similarly, in chapter 10 the security analysis of ElGamal cryptosystem is discussed by analyzing the algorithms that solve the discrete logarithm problem.

In the next part of this text, cryptographic hash functions and digital signatures are discussed. Chapter 11 explains the structure of hash functions and their application in cryptography. It gives SHA-1 as an example. The idea of digital signature and its security are found in chapter 12. The author uses RSA, ElGamal, and DSA as examples to digital signature schemes. Simply he describes the key generation, the signature generation, and the verification of each example. He studies the efficiency and some attack scenarios for each one of them. Also he presents an example of a special purpose digital signature, so-called blind signatures. Two different protocols are given (Chaum and Okamoto-Schnorr). In the last part of this book, the author briefly introduces some other topics. In less than three pages he defines the elliptic curves. Identification, secret charing, and public key infrastructure are just explained in a very brief way.

2 Summary

I like the structure of this book. It gives a general mathematical background in the beginning and particular mathematical preliminaries just at the time you need them to understand some specific cryptographic method. It provides a clearly detailed presentation of some selected methods in cryptography. The focus of this book is on number theoretic algorithms that are used in cryptography like primality testing, factorization and discrete logarithms. It also provides a detailed description of block ciphers as an example of symmetric cryptography. Explanations of some basic particular cryptography such as digital signatures, hash functions, secret sharing, and certificate authentications are provided. The brief description of some important methods in cryptography represents one of the drawbacks of this book, for example the part that is dealing with elliptic curve. Also the definitions of O-notation and Ω-notation are not clear.

3 Recommendation

As the author mentioned this book is based on courses in cryptography that have been taught by the author himself at the Technical University of Darmstadt. So I would recommend this text for undergraduate students or readers who want to get an overview of some modern cryptographic methods and their mathematical preliminaries, like for example RSA and DES. The text is just 324 pages, so it is focusing on some cryptographic methods like number theoretical cryptographic techniques and just touches some other methods like elliptic curves. For readers that need texts with more wide details in cryptography, I recommend these books:

- Oded Goldreich "Foundations of Cryptography: Volume 1 and 2"
- Doug Stinson "Cryptography: theory and practice"
- Wenbo Mao "Modern cryptography: theory and practice"

The reviewer is a Ph.D. student at the Technical University of Darmstadt, Germany.