Review of the book

" A Classical Introduction to Cryptography Exercise Book"

by Baigneres, Th., Junod, P., Lu, Y., Monnerat, J., Vaudenay, S.

Springer, 2006

ISBN: 978-0-387-27934-3

Abdelhak Azhari
Hassan II University, Casablanca

1 Summary of the book

In the last decade, cryptography has been employed in various applications of our daily lives: Authentication, Digital Signatures, and Electronic Money, bank operations, Electronic Voting, Electronic Commerce, TV, cell phone, smart card, Secure Network Communications, etc... Cryptography is used to protect data and sensitive communications. Today governments, academies, industries and practitioners use sophisticated methods of coding and decoding messages. Cryptography is an indispensable tool for protecting information in computer systems and the ability to securely store and transfer sensitive information has proved a critical factor in success in military and business transactions. Today, the Internet has allowed the spread of powerful programs and the underlying techniques of cryptography, so that the most advanced cryptosystems and ideas are in the public domain.

The book under review is an exercises book on cryptography and its application in secure communications. It proposes various aspects of cryptography starting from prehistory to modern cryptography. This includes conventional cryptography such as DES and 3DES, security protocols such as Woo-lam Protocol, Bluetooth Pairing Protocol and UNIX passwords.

Chapter 6 proposes a study of algorithmic algebra such as primitive roots, quadratic residues, AES, discrete logarithm and elliptic curves on finite fields. Moreover, chapter 7 proposes various exercises on algorithmic number theory including factorization, Pollard's rho method, prime numbers, strong prime numbers and complexity of Eratosthenes' sieve method as well as hash functions based on arithmetic.

Chapter 9 is devoted to the study of public key crypotography. Some cryptosystems are studied in details such as Okamoto-Uchiyama, RSA, Rabin, Paillier and Naccache-Stern.

Chapters 10 and 11 propose various exercises on Digital Signatures and cryptographic Protocols such blind signature protocol, Fiat-Shamir signature, authenticated Diffie-Hellman key agreement protocol and a key distribution system.

Chapter 12, untitled From Cryptography to Communication Security, proposes a study of a hybrid cryptosystem using RSA and DES. It also proposes some exercises on SSL/TLS cryptography and Secure Shell (SSH) and Forging X.509 Certificates.

All the proposed exercises contain hints and solutions and are based on various notions of mathematics. This helps the reader to be more familiar with many aspects in cryptography.

2 What is the book like (style)?

The book was developed after graduate courses in cryptography done at EPFL between 2000 and 2005. The main objective is to show how some mathematical notions such as calculus, algebra, as well as computer science are used to study the security of various cryptosystems or to break some them.

3 Would you recommend this book?

The book is suitable for advanced undergraduate and graduate students as well as students in computer science and engineering. It is also a good reference for practitioners who want to understand the mathematical techniques of cryptography.

As a companion book of Vaudenay's book untitled A Classical Introduction to Cryptography, it contains a carefully revised version of most of the material used in teaching by the authors or given as examinations at EPFL from 2000 to mid-2005.

The book covers most of the modern cryptography protocols, based on various exercises. We wish the reader a wonderful trip in the exciting world of cryptology!!

The reviewer is a Professor at Hassan II University, Casablanca.