Hans Delfs
Helmut Knebl

Introduction to Cryptography

Principles and Applications

Springer

IST 2842

BIBLIOTHEQUE DU CERIST

BIBLIOTHEQUE DU CERIST

Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Tokyo

BIBLIOTHEQUE DU CERIST

Hans Delfs · Helmut Knebl

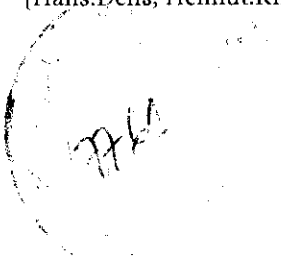
Introduction to Cryptography

Principles and Applications

Springer

Prof. Dr. Hans Delfs
Prof. Dr. Helmut Knebl

Georg-Simon-Ohm University of Applied Sciences Nürnberg
Department of Computer Science
Keßlerplatz 12
90489 Nürnberg
Germany
{Hans.Delfs, Helmut.Knebl}@fh-nuernberg.de



BIBLIOTHEQUE DU CERIST

Library of Congress Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek – CIP-Einheitsaufnahme
Delfs, Hans:
Introduction to cryptography: principles and applications / H. Delfs ; H. Knebl. – Berlin; Heidelberg; New York; Barcelona; Hong Kong; London; Milan; Paris; Tokyo: Springer, 2002
(Information security and cryptography)
ISBN 3-540-42278-1

ACM Computing Classification (1998): E.3

ISBN 3-540-42278-1 Springer-Verlag Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilm or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German copyright law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

Springer-Verlag Berlin Heidelberg New York,
a member of BertelsmannSpringer Science+Business Media GmbH
http://www.springer.de

© Springer-Verlag Berlin Heidelberg 2002
Printed in Germany

The use of general descriptive names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

Cover design: KünkelLopka, Heidelberg
Typesetting: Camera-ready by authors
Printed on acid-free paper SPIN: 10838447 45/3142 GF– 5 4 3 2 1 0

Preface

BIBLIOTHEQUE DU CERIST

The rapid growth of electronic communication means that issues in information security are of increasing practical importance. Messages exchanged over worldwide publicly accessible computer networks must be kept confidential and protected against manipulation. Electronic business requires digital signatures that are valid in law, and secure payment protocols. Modern cryptography provides solutions to all these problems.

This book originates from courses given for students in computer science at the Georg-Simon-Ohm University of Applied Sciences, Nürnberg. It is intended as a course on cryptography for advanced undergraduate and graduate students in computer science, mathematics and electrical engineering.

In its first part (Chapters 1–4), it covers - at an undergraduate level – the key concepts from symmetric and asymmetric encryption, digital signatures and cryptographic protocols, including, for example, identification schemes, electronic elections and digital cash. The focus is on asymmetric cryptography and the underlying modular algebra. Since we avoid probability theory in the first part, we necessarily have to work with informal definitions of, for example, one-way functions and collision-resistant hash functions.

It is the goal of the second part (Chapters 5–10) to show, using probability theory, how basic notions like the security of cryptographic schemes and the one-way property of functions can be made precise, and which assumptions guarantee the security of public-key cryptographic schemes such as RSA. More advanced topics, like the bit security of one-way functions, computationally perfect pseudorandom generators and the close relation between the randomness and security of cryptographic schemes, are addressed. Typical examples of provably secure encryption and signature schemes and their security proofs are given.

Though particular attention is given to the mathematical foundations and, in the second part, precise definitions, no special background in mathematics is presumed. An introductory course typically taught for beginning students in mathematics and computer science is sufficient. The reader should be familiar with the elementary notions of algebra, such as groups, rings and fields, and, in the second part, with the basics of probability theory. Appendix A contains an exposition of the results from algebra and number theory necessary for an understanding of the cryptographic methods. It includes proofs

and covers, for example, basics like Euclid's algorithm and the Chinese Remainder Theorem, but also more advanced material like Legendre and Jacobi symbols and probabilistic prime number tests. The concepts and results from probability and information theory, which are applied in the second part of the book, are given in full in Appendix B. To keep the mathematics easy, we do not address elliptic curve cryptography. We illustrate the key concepts of public-key cryptography by the classical examples like RSA in the quotient rings $\mathbb{Z}_n$ of the integers $\mathbb{Z}$.

The book starts with an introduction into classical symmetric encryption in Chapter 2. The principles of public-key cryptography and their use for encryption and digital signatures are discussed in detail in Chapter 3. The famous and widely used RSA, ElGamal's methods and the digital signature standard, Rabin's encryption and signature schemes serve as the outstanding examples. The underlying one-way functions – modular exponentiation, modular powers and modular squaring – are used throughout the book, also in the second part.

Chapter 4 presents typical cryptographic protocols, including key exchange, identification and commitment schemes, electronic cash and electronic elections.

The following chapters focus on a precise definition of the key concepts and the security of public-key cryptography. Attacks are modeled by probabilistic polynomial algorithms (Chapter 5). One-way functions as the basic building blocks and the security assumptions underlying modern public-key cryptography are studied in Chapter 6. In particular, the bit security of the RSA function, the discrete logarithm and the Rabin function is analyzed in detail (Chapter 7). The close relation between one-way functions and computationally perfect pseudorandom generators meeting the needs of cryptography is explained in Chapter 8. Provable security properties of encryption schemes are the central topic of Chapter 9. It is clarified that randomness is the key to security. We start with the classical notions of provable security originating from Shannon's work on information theory. Typical examples of more recent results on the security of public-key encryption schemes are given, taking into account the computational complexity of attacking algorithms. A short introduction to cryptosystems, whose security can be proven by information-theoretic methods without any assumptions on the hardness of computational problems ("unconditional security approach"), supplements the section. Finally, we discuss in Chapter 10 the levels of security of digital signatures and give examples of signature schemes, whose security can be proven solely under standard assumptions like the factoring assumption, including a typical security proof.

Each chapter (except Chapter 1) closes with a collection of exercises. Answers to the exercises are provided on the Web page for this book: www.informatik.fh-nuernberg.de/DelfsKnebl/Cryptography.

BIBLIOTHEQUE DU CERIST

We thank our colleagues and students for pointing out errors and suggesting improvements. In particular, we express our thanks to Jörg Schwenk, Harald Stieber and Rainer Weber. We are grateful to Jimmy Upton for his comments and suggestions, and we are very much indebted to Patricia Shiroma-Brockmann for proof-reading the English copy. Finally, we would like to thank Alfred Hofmann at Springer-Verlag for his support during the writing and publication of this book.

Nürnberg, December 2001 Hans Delfs, Helmut Knebl

BIBLIOTHEQUE DU CERIST

BIBLIOTHEQUE DU CERIST

Contents

BIBLIOTHEQUE DU CERIST

BIBLIOTHEQUE DU CERIST

BIBLIOTHEQUE DU CERIST