Preface to the Third, Extended Edition

The third edition is a substantive extension. This is reflected in a considerable increase in pages. A number of new topics have been included. They supplement and extend the material covered in the previous editions. The major extensions and enhancements follow:

- We added a description of the new SHA-3 algorithm for cryptographic hash functions, Keccak, and the underlying sponge construction (Section 2.2.2).
- As a further important example of homomorphic encryption algorithms, Paillier encryption is introduced in Section 3.6.2.
- ElGamal encryption in a prime-order subgroup of a finite field is studied in detail in Section 3.4.4.
- An introduction to elliptic curve cryptosystems including Diffie–Hellman key exchange, ElGamal encryption and the elliptic curve digital signature standard ECDSA is given in Section 3.7.
- The basics of plane curves and elliptic curves that are necessary to understand elliptic curve cryptography are explained in Appendix A.11.
- Additional concepts of interactive proof systems, such as the special honest-verifier zero-knowledge property and the OR-combination of Σ-proofs, are addressed in Section 4.5.
- The exposition of cryptographic protocols for electronic elections and Internet voting has been substantially extended (Sections 4.6 and 4.7).
- Decryption and re-encryption mix nets and shuffles as the basic tools to anonymize communication are discussed in Section 4.6. A complete zero-knowledge proof for the correctness of a re-encryption shuffle is given. Such proofs are indispensable in critical applications of mix nets, such as electronic voting systems. The correct operations of the mix net must be publicly verifiable, without compromising the confidentiality of individual votes.
- Receipt-free and coercion-resistant elections are studied in Section 4.7. Various techniques that are useful in the design of cryptographic protocols are explained here, such as designated-verifier proofs, diverted proofs, untappable channels and plaintext equivalence tests.
- Unconditionally secure cryptographic schemes are not based on the practical infeasibility of a computational task. Their security is proven by using

methods from information theory. Unconditionally secure schemes are now addressed in an extra chapter, Chapter 10.
- Unconditional security is not achievable without an unconditionally secure authentication of the communication partners. Suitable message authentication codes are constructed from almost universal classes of hash functions in Section 10.3.
- Privacy amplification is one of the essential techniques to derive an unconditionally secure shared secret key from information that is publicly exchanged. We give a proof of the Privacy Amplification Theorem and explain the basic properties of Rényi entropy.
- In Section 10.5, we present an introduction to quantum cryptography. We describe, in detail, the famous BB84 protocol of Bennett and Brassard for quantum key distribution and prove its security, assuming intercept-and-resend attacks.

The description of cryptographic hash functions has been moved to Chapter 2, which is now headlined "Symmetric-Key Cryptography". Moreover, errors and inaccuracies have been corrected, and in some places, the exposition has been clarified.

Some exercises have been added. Answers to all exercises are provided on the webpage www.in.th-nuernberg.de/DelfsKnebl/Cryptography.

We thank our readers and our students for their comments and hints. Again, we are greatly indebted to our colleague Patricia Shiroma-Brockmann for proof-reading the English copy of the new and revised chapters. Finally, we would like to thank Ronan Nugent at Springer for his support.

Nürnberg, July 2015 Hans Delfs, Helmut Knebl

Preface to the Second, Extended Edition

New topics have been included in the second edition. They reflect recent progress in the field of cryptography and supplement the material covered in the first edition. Major extensions and enhancements are the following.

- A complete description of the Advanced Encryption Standard AES is given in Chapter 2.1 on symmetric encryption.
- In Appendix A, there is a new section on polynomials and finite fields. There we offer a basic explanation of finite fields, which is necessary to understand the AES.
- The description of cryptographic hash functions in Chapter 3 has been extended. It now also includes, for example, the HMAC construction of message authentication codes.[1]
- Bleichenbacher's 1-Million-Chosen-Ciphertext Attack against schemes that implement the RSA encryption standard PKCS#1 is discussed in detail in Chapter 3. This attack proves that adaptively-chosen-ciphertext attacks can be a real danger in practice.
- In Chapter 9 on provably secure encryption we have added typical security proofs for public-key encryption schemes that resist adaptively-chosen-ciphertext attacks. Two prominent examples are studied – Boneh's simple-OAEP, or SAEP for short, and Cramer–Shoup's public-key encryption.
- Security proofs in the random oracle model are now included. Full-domain-hash RSA signatures and SAEP serve as examples.

Furthermore, the text has been updated and clarified at various points. Errors and inaccuracies have been corrected.

We thank our readers and our students for their comments and hints, and we are indebted to our colleague Patricia Shiroma-Brockmann and Ronan Nugent at Springer for proof-reading the English copy of the new and revised chapters.

Nürnberg, December 2006 Hans Delfs, Helmut Knebl

[1] In the 3rd edition, the description of hash functions has been moved to Chapter 2.

Preface

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 5–11) 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 that 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.[2] 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 to classical symmetric encryption in Chapter 2.[3] 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 11 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.

[2] Elliptic curve cryptography has been included in the 3rd edition.
[3] Chapter 2 now covers symmetric encryption and cryptographic hash functions.

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

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