Preface

Why is cryptography interesting? Firstly, cryptography is a classical subject with a fascinating history. Encryption techniques have been used since ancient times, but the protection against exposure was sometimes dubious and many ciphers were broken. The design of new ciphers and the capability to analyze and break them co-evolved over time. Since then, the techniques have been adapted to progress in cryptanalysis and to the computing power available. Modern cryptography goes beyond confidentiality, also addressing aspects such as data integrity, authentication, non-repudiation and other security objectives. The subject now includes all mathematical techniques relating to information security.

Secondly, cryptography is closely connected to several fields of mathematics and computer science, providing interesting applications for many theoretical results and stimulating mathematical research. Cryptography, which we use as an umbrella term for the field including cryptanalysis, is linked to aspects of discrete mathematics, number theory, algebra, probability theory, statistics, information and coding theory.

Thirdly, cryptography has become a key technology that is used ubiquitously in computer systems from small devices to large servers and networks. The multitude of security threats is driving the trend to protect data whenever possible, be it for storage or during transmission over networks. The reader should be warned, however, that real-world security is a complex process in which cryptography contributes "only" the primitives, algorithms and schemes. In practice, attacks often exploit protocol or implementation flaws, weak passwords or negligent users. Furthermore, the security guarantees offered by cryptography cannot be unconditional. The security provided depends on the power of adversaries, their computing resources and the time available for an attack, as well as on underlying computational problems which are believed to be hard.

The aim of this book is to explain the current cryptographic primitives and schemes and to outline the essential mathematics required to understand the building blocks and assess their security. We cover the widespread schemes, but we also want to address some of the recent developments in post-quantum cryptography. The mathematical and, in particular, algebraic and number-theoretical foundations of cryptography are explained in detail. The mathematical theory is presented with a focus on cryptographic applications and we do not strive for maximal generality. We look at a selection of cryptographic algorithms according to their current and supposed future relevance, while leaving out several historic schemes. Since cryptography is a very active field, some uncertainty regarding future developments will of course remain.

Why write *yet another* textbook on cryptography? We hope to convince potential readers by listing some of the unique features of this book:

- The fundamentals of cryptography are presented with rigorous definitions while being accessible to undergraduate students in science, engineering and mathematics;
- Formal definitions of security as used in the modern literature on cryptography;
- Focus on widely used methods and on prospective cryptographic schemes;
- Introduction to quantum computing and post-quantum cryptography;
- Numerical examples and SageMath (Python) code.

Cryptography can easily be underestimated by mathematicians. Several textbooks contain excellent descriptions of the mathematical theory, but fall short of explaining how to use these algorithms in practice. In fact, the main purpose of cryptography is to achieve security objectives such as confidentiality and integrity in the presence of powerful adversaries. Well-known schoolbook algorithms like RSA can be insecure without adaptations, for example, by incorporating random data.

This book follows the *provable security* approach which is adopted in the modern literature. Well-defined experiments (games) are used in which the success probability of potential attackers determines the security. Secure schemes have the property that an adversary with restricted resources can do little better than randomly guess the secret information. Using this approach, the security is reduced to standard assumptions that are generally believed to be true. In this book, we give exact security definitions and some proofs, but refer to the literature for more advanced proofs and techniques, for example, using the sequence of games approach.

We find that examples are very helpful and include computations using the open source mathematics software SageMath (aka Sage) [**Sag18**]. SageMath contains many algebraic and number theoretic functions which can be easily used and extended. Although the software might be better known among mathematicians than scientists and engineers, it is easily accessible and very suitable for cryptographic computations. SageMath is based on Python and contains other open source software as, for example, Singular, Maxima, PARI, GAP, NumPy, SciPy, SymPy and R. In recent years, Python

has gained immense popularity among scientists. One of its advantages is that results can be obtained quickly without much programming overhead. In this book, we opt for SageMath instead of plain Python since SageMath has much better support for algebraic computations, which are often needed in modern cryptography. SageMath also has a convenient user interface and supports the popular Jupyter browser notebooks.

Numerical examples can be used to help understand cryptographic constructions and their underlying theory. Toy examples, in which the numbers and bit-lengths are too small for any real-world security, can still be useful in this respect. The reader is encouraged to perform computations and to write their own SageMath functions. We also provide exercises with both theoretical and numerical problems.

The book should be accessible to mathematics, science or engineering students after completing a first year's undergraduate course in mathematics (calculus and linear algebra). The material originates from several courses on cryptography for computer scientists and communication engineers which the author has taught. Since the previous knowledge can be quite heterogeneous, we decided to include several elementary topics. In the author's teaching experience, abstract algebra as well as linear algebra over general fields deserves special attention. Linear maps over finite fields play an important role in many cryptographic constructions. This book should be largely self-contained and requires no previous knowledge of discrete mathematics, algebra, number theory or cryptography. We do not strive for greatest generality and frequently refer to more specialized textbooks or articles.

Cryptography can be taught at different levels and to different audiences. This book can be used in bachelor's and master's courses, as well as by practitioners, and is suitable for a general audience wanting to understand the fundamentals of modern cryptography. Many mathematics and computer science students may already have the necessary background in discrete mathematics, elementary number theory and probability and can therefore skip Chapters 1 and 3. Chapter 4 provides the necessary algebraic constructions and is recommended to all readers without solid knowledge of abstract algebra. From my teaching experience, algebra can be a major stumbling block and should not be underestimated. Chapters 1, 3 and 4 thus provide the mathematical background of cryptography.

We decided to begin with the core cryptographic content as early as possible, so Chapter 2 deals with encryption schemes and the modern definitions of security. This chapter requires only basic discrete mathematics, complexity and probability theory and is recommended for most readers, even if they have some prior knowledge of cryptography. Understanding the provable security approach is crucial for the subsequent chapters of this book. Chapter 5 deals with block ciphers and AES in particular, which is a crucial part of every modern course on cryptography. Chapter 6 explores stream ciphers, which form a natural complement, but it is also possible to omit this chapter if you are short on time. We have already mentioned that modern cryptography goes beyond encryption. Integrity protection is another major objective, and hash functions

and message authentication codes play a crucial role in this. These topics are addressed in Chapters 7 and 8. Chapters 9, 10 and 11, which are on public-key encryption, key establishment and signatures, introduce the fundamentals of public-key cryptography. We explain RSA and Diffie-Hellman in particular and discuss their security, which is based on hard number-theoretic problems.

We therefore think that Chapters 2, 5, 7, 8, 9, 10 and 11, along with the necessary mathematical preparations (Chapters 1, 3 and 4), should be covered in every first course on cryptography. A one-semester bachelor's module might end after Chapter 11, but whenever possible, we recommend including Chapter 12 on elliptic curve cryptography. This has been the topic of intensive research in the last few decades but has now become part of well-established cryptography and is implemented by every Internet browser, for example. We believe the basics of elliptic curves are accessible to readers after the preparatory work in Chapters 3 and 4. There are, however, more advanced topics in elliptic curves that are not treated here.

Chapters 13, 14 and 15 provide an introduction to the new field of post-quantum cryptography. In Chapter 13, we explore the basics of quantum computing and explain why quantum computers can break classic public-key schemes like RSA. Chapters 14 and 15 deal with two major types of post-quantum systems that are based on lattices and error-correcting codes, respectively. We focus on the foundations and several selected encryption schemes. Note that there are other post-quantum systems, for example, cryptosystems from isogenies of elliptic curves or multivariate-quadratic-equations signatures, which are not covered in this book. Chapters 13–15 are more challenging with respect to the level of calculus and abstract algebra. However, we spend some time on examples (many of them using SageMath) and we hope that the content of these three chapters is accessible for master's or advanced bachelor's students. We expect that quantum computing and post-quantum schemes will become increasingly important in the future.

I would be happy to receive feedback and suggestions for improvement. Please email your comments to `heiko.knospe@th-koeln.de`. Updates and additional material, for example, solutions to selected exercises and SageMath code, are available on the following website: `https://github.com/cryptobook`.

Finally, I would like to thank my colleagues and my students for their valuable feedback on my cryptography course and on earlier versions of the manuscript.