# Introduction

The object of this book is threefold. First, we explore how non-commutative groups which are typically studied in combinatorial group theory can be used in *public-key cryptography*. Second, we show that there is a remarkable feedback from cryptography to combinatorial group theory because some of the problems motivated by cryptography appear to be new to group theory, and they open many interesting research avenues within group theory. In particular, we put a lot of emphasis on studying *search problems*, as compared to *decision problems*, traditionally studied in combinatorial group theory. Yet another purpose of this book is to survey recent developments in combinatorial and computational group theory that are or can potentially be useful to cryptography. This includes generic properties of groups, subgroups and elements, generic- and average-case complexity of group-theoretic algorithms, asymptotically dominant properties, compressed words, etc.

We emphasize that our focus in this book is on public-key (or asymmetric) cryptography. "Classical" (or symmetric) cryptography generally uses a single key which allows both for the encryption and decryption of messages. This form of cryptography is usually referred to as symmetric key cryptography because the same algorithm or procedure or key is used not only to encode a message but also to decode that message. The key being used then is necessarily private and known only to the parties involved in communication. This method for transmission of messages was basically the only way until 1976 when W. Diffie and M. Hellman introduced an ingenious new way of transmitting information, which has led to what is now known as public-key cryptography. The basic idea is quite simple. It involves the use of a so-called one-way function $f$ to encrypt messages. Very informally, a one-way function $f$ is a function such that it is easy to compute the value of $f(x)$ for each argument $x$ in the domain of $f$, but it is very hard to compute the value of $f^{-1}(y)$ for "most" $y$ in the range of $f$. The most celebrated one-way function, due to Rivest, Shamir and Adleman, gives rise to the protocol called RSA, which is the most common public-key cryptosystem in use today. It is employed, for instance, in the browsers Firefox and Internet Explorer. Thus it plays a critical and increasingly important role in all manner of secure electronic communication and transactions that use the Internet. It depends in its efficacy, as do many of other cryptosystems, on the complexity of finite abelian (or commutative) groups. Such algebraic structures are very special examples of *finitely generated groups*. Finitely generated groups have been intensively studied for over 150 years and they exhibit extraordinary complexity. Although the security of the Internet does not appear to be threatened at this time because of the weaknesses of the existing protocols such as RSA, it seems prudent to explore possible enhancements and replacements

of such protocols which depend on finite abelian groups. This is one of the basic objectives of this book.

The idea of using the complexity of infinite non-abelian groups in cryptography goes back to Wagner and Magyarik [**180**] who in 1985 devised a public-key protocol based on the unsolvability of the word problem for finitely presented groups (or so they thought). Their protocol now looks somewhat naive, but it was pioneering. More recently, there has been an increased interest in applications of non-abelian group theory to cryptography (see for example [**5, 161, 257**]). Most suggested protocols are based on search problems that grew out of more traditional *decision problems* of combinatorial group theory. Protocols based on search problems fit in with the general paradigm of a public-key protocol based on a one-way function. We therefore dub the relevant area of cryptography *canonical cryptography* and explore it in Chapter 4 of our book.

On the other hand, employing decision problems in public-key cryptography allows one to depart from the canonical paradigm and construct cryptographic protocols with new properties, impossible in the canonical model. In particular, such protocols can be secure against some "brute force" attacks by computationally unbounded adversary. There is a price to pay for that, but the price is reasonable: a legitimate receiver decrypts correctly with probability that can be made very close to 1, but not equal to 1. We discuss this and some other new ideas in Chapter 15.

In Chapter 8, we describe several new ideas in public-key authentication. The problem of secure public-key authentication is, arguably, the most intriguing one in public-key cryptography since it can be put "between" the two principal problems: (1) the existence of one-way functions; (2) the existence of a secure public-key cryptosystem (or, equivalently, the existence of a secure key exchange protocol). Namely, the existence of a secure public-key cryptosystem obviously implies the existence of a secure public-key authentication scheme, and the latter implies the existence of one-way functions. However, the reverse implications may not hold. We describe in this book a number of authentication schemes based on different ideas, some of them coming from group theory and some from other areas of mathematics. Independently interesting is a related concept of a "zero-knowledge" proof that we also discuss in Chapter 8.

There were attempts, so far rather isolated, to provide a rigorous mathematical justification of security for protocols based on infinite groups, as an alternative to the security model known as *semantic security* [**102**], which is widely accepted in the "finite case". It turns out, not surprisingly, that to introduce such a model one would need to define a suitable probability measure on a given infinite group. This delicate problem has been addressed in [**29, 28, 167**] for some classes of groups, but this is just the beginning of the work required to build a solid mathematical foundation for assessing security of cryptosystems based on infinite groups. Another, related, area of research studies *generic* behavior of infinite groups with respect to various properties (see [**146**] and its references). It is becoming clear now that, as far as security of a cryptographic protocol is concerned, the appropriate measure of computational hardness of a group-theoretic problem in the core of such a cryptographic protocol should take into account the "generic" case of the problem, as opposed to the worst case or average case traditionally studied in mathematics and theoretical computer science. Generic-case performance of various algorithms on

groups has been studied in [**146, 148**], [**149**], and many other papers. It is the focus of Part 3 of this book.

We have to make a disclaimer though that we do *not* address here security properties (e.g. semantic security) that are typically considered in "traditional" cryptography. They are extensively treated in cryptographic literature; here we single out a forthcoming monograph [**104**] because it also studies how group theory may be used in cryptography, but the focus there is quite different from ours; in particular, the authors of [**104**] do not consider infinite groups, but they do study "traditional" security properties thoroughly. To avoid misunderstanding, we stress that we do not mean any disrespect for semantic security; it is just that in the present book, we place strong emphasis on discussing new ideas and the intuition behind them. One other thing to keep in mind is that here we deal mostly with *infinite* groups as platforms for cryptographic primitives, and possible ramifications and generalizations of semantic security to infinite platforms are yet to be explored, although we do make some inroads into that area in this book.

We also have to point out that, in comparison with some other books on cryptography, our book is less implementation-oriented. In particular, we usually avoid giving specific parameters for cryptographic protocols that we describe; instead, we focus on new ideas and new research avenues.

In Part 4 of our book, we use the ideas and machinery from Part 3 to study *asymptotically dominant properties* of some infinite groups that have been used in public-key cryptography so far. Informally, the point is that "most" elements, or tuples of elements, or subgroups, or whatever, of a given group have some "smooth" properties which make them misfits for being used (as private or public keys, say) in a cryptographic scheme. Therefore, for a relevant cryptographic scheme to be secure, it is essential that keys are actually sampled (i.e., randomly selected) from a "small" (relative to the whole group, say) subset rather than from the whole group. Detecting these subsets ("black holes") for a particular cryptographic scheme is usually a very challenging problem, but it holds the key to creating secure cryptographic primitives based on infinite non-abelian groups.

Parts 5 and 6 are not about cryptography *per se*, but about complexity of various algorithmic problems in combinatorial group theory, notably of search problems, motivated by cryptography. Part 5 offers an in-depth study, from a computational perspective, of two major search problems in group theory: the word search and the conjugacy search problems. Chapter 18 of Part 6 describes new interesting developments in the algorithmic theory of solvable, in particular metabelian, groups. It may come as a surprise that in a free metabelian group where standard algorithmic problems are efficiently solvable, the *bounded geodesic problem* (i.e., deciding whether for a given word and a given integer $k$, there is another word of length $\leq k$ representing the same element) is **NP**-complete. Chapter 19 describes yet another spectacular new development related to complexity of group-theoretic problems. Based on the ideas of *compressed words* and straight-line programs coming from computer science, it is possible to design polynomial-time algorithms for some problems in group theory that were previously thought to be computationally intractable including, for example, the word problem in the automorphism group of a free group.

In the Appendix, yet another probabilistic approach to cryptanalysis is introduced. Specifically, a particular example of a group-based authentication protocol,

due to Sibert et al. [**256**], is used to illustrate how the "strong law of large numbers" can be adapted for graphs and then employed in cryptanalysis of group-based cryptographic schemes.

Finally, we note that this book is a substantial extension of our earlier introductory book [**194**] that was based on lecture notes for the Advanced Course on Group-Based Cryptography held at the CRM, Barcelona in May 2007.