Preface

In this book, we explore "non-commutative ideas" in cryptography that have appeared in the literature over the last decade or so. Since all three authors have backgrounds in combinatorial and computational group theory, we pay particular attention to what can be called group-based cryptography, i.e., cryptography that uses non-commutative group theory one way or another. However, we also discuss some ideas from other areas of mathematics, especially when we address the problem of authentication, which is one of the most important areas of applications of modern cryptography.

We also show that there is remarkable feedback from cryptography to combinatorial and computational 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. Then, we employ complexity theory, notably *generic-case complexity* of algorithms, for cryptanalysis of various cryptographic protocols based on infinite groups. We also use the ideas and machinery from the theory of generic-case complexity to study *asymptotically dominant properties* of some infinite groups that have been used in public-key cryptography so far. It turns out that for a relevant cryptographic scheme to be secure, it is essential that keys are selected from a "very 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 non-commutative groups.

A substantial part of the book deals with new directions in computational group theory itself, notably with search problems motivated by cryptography. We also study complexity of more traditional decision problems (like the word and conjugacy problems) in some groups that have been suggested as platforms for cryptographic protocols.

Acknowledgments. It is a pleasure for us to thank our colleagues who have directly or indirectly contributed to this book. In particular, we would like to thank M. Anshel, G. Baumslag, Y. Bryukhov, M. Elder, N. Fazio, B. Fine, R. Gilman, D. Grigoriev, Yu. Gurevich, G. Havas, D. Kahrobaei, I. Kapovich, L. Makar-Limanov, A. D. Miasnikov, A. A. Mikhalev, A. V. Mikhalev, D. Osin, G. Rosenberger, T. Riley, V. Roman'kov, A. Rybalov, M. Sapir, W. Skeith, R. Steinwandt, B. Tsaban, A. Vershik, G. Zapata for numerous helpful comments and insightful discussions.

We are also grateful to our home institutions, the City College of New York and Stevens Institute of Technology for a stimulating research environment. A. G. Myasnikov and A. Ushakov acknowledge support by the NSF grant DMS-0914773 during their work on this book. A. G. Myasnikov was also supported by an NSERC grant. V. Shpilrain acknowledges support by the NSF grant DMS-0914778.

Finally, we are indebted to S. I. Gelfand for his encouragement and patience during our work on this project, and to C. Thivierge and L. Cole for their help during the production process.

Alexei Myasnikov
Vladimir Shpilrain
Alexander Ushakov

New York