To Galina

Preface

Cryptology is nowadays one of the most important subjects of applied mathematics. Not only the task of keeping information secret is important, but also the problems of integrity and of authenticity, i.e., one wants to avoid that an adversary can change the message into a fraudulent one without the receiver noticing it, and on the other hand the receiver of a message should be able to be sure that the latter has really been sent by the authorized person (electronic signature). A big impetus on modern cryptology was the invention of so-called public-key cryptosystems in the 1970's by Diffie, Hellman, Rivest, Shamir, Adleman, and others. In particular in this context, deep methods from number theory and algebra began to play a decisive role. This aspect of cryptology is explained in, for example, the monograph "Algebraic Aspects of Cryptography" by Koblitz (1999). The goal of these notes was to write a treatment focusing rather on the stochastic (i.e., probabilistic and statistical) aspects of cryptology. As this direction also consists of a huge literature, only some glimpses can be given, and by no means are we always at the frontier of the current research. The book is rather intended as an invitation for students, researchers, and practitioners to study certain subjects further. We have tried to be as self-contained as reasonably possible, however we suppose that the reader is familiar with some fundamental notions of probability and statistics. It is our hope that we have been able to communicate the fascination of the subject and we would be delighted if the book encouraged further theoretical and practical research.

Let me give my gratitude to my colleagues in the Cryptology Section in the Ministry of Defense of Switzerland for the excellent and stimulating working atmosphere. Many thanks are also due to Werner Schindler from the German "Bundesamt für Sicherheit in der Informationstechnik" for helpful discussions. Furthermore, I am indebted to Springer-Verlag, Heidelberg for the agreeable cooperation. However, the most important thanks goes to my wife Galina for her constant moral support of my scientific activities. Without her asking "How is your book?" from time to time, the latter would certainly not yet be finished!

Bern, February 2004 Daniel Neuenschwander