Preface

This book is an entirely self-contained sophomore-level text on the exciting subject of cryptography, which is the science of achieving secure communication over insecure channels. It was carefully designed to accommodate a wide variety of both mathematics and computer science courses, ranging from a ground-level course with minimal prerequisites to a follow-up course to a standard number theory course. The author began teaching cryptography as a special topic in more general courses that included both mathematics and computer science majors (for example, in discrete structures, in abstract algebra, and even in finite mathematics) starting about 12 years ago. Rather than aiming at an encyclopedic treatment of almost all topics in cryptography, this book provides a focused tour of the central and evergreen topics and concepts of cryptography, following the exciting history of its development from ancient times to the present day. Cryptography is a very important subject in both mathematics and computer science, and it serves as an ideal melting pot, where the subjects, students, and practitioners can draw on each other and become stronger in the process. The fact that cryptography is heavily relied on by business, government, and industry, coupled with the increasing new technologies for transferring data, guarantees that it will play a permanent role in research and development, as its architects and hackers continue to battle for the upper hand.

Each chapter is written in an engaging and easy-going, yet rigorous style. Important concepts are introduced with clear definitions and theorems, the proofs are written in a style that students find appealing. Numerous examples are provided to illustrate key points, and figures and tables are used to help illustrate the more difficult or subtle concepts. The first chapter gives an overview of the subject, provides a road map for the rest of the book, and lays out some terminology of the subject. Some of the concepts and definitions can only be informally defined in such a preliminary chapter, but the subsequent chapters follow a more rigorous path, and additional details for some topics introduced in the overview chapter will be revisited later on in the text with more formal treatments. Chapters 2 through 12 basically develop cryptography in chronological order, with mathematical concepts being developed as they are needed. The text proper of each chapter is punctuated with "Exercises for the Reader" that provide the readers with regular opportunities to test their understanding of their reading (and help them to become more active readers). The exercises for the reader range in difficulty from routine to more involved, but appendices at the end of the book include detailed solutions to all of them. In addition to these exercises for the reader, each chapter has an extensive and well-crafted set of exercises that range in difficulty from routine to nontrivial. An appendix contains answers or brief solutions to most of the odd-numbered exercises. A separate instructor's manual has been prepared for the corresponding solutions of the even-numbered exercises. Every chapter concludes with a Computer Implementation and Exercises section, which guides interested readers through the process of writing their own programs for the cryptographic concepts of each chapter.

There is more than enough material included in this text for a one-semester course, and a variety of different courses could be created from it. Since the computer implementation material is separated from the main text, the book can be used without computers. A useful set of platform-independent applet pages has been created to perform many of the core algorithms of this book; these can be freely downloaded along with other relevant materials from the book's Web page. Rather than print the URL of the Web page, which may change as servers get updated or as (the author's physical or electronic) addresses may change, the easiest way to access this page is through the author's homepage, which can be obtained by a simple Web search of the author's last name. The Web page should also be navigable via the publisher's Web site. There is a sufficient amount of number theory in the book to satisfy the number theory credential requirement for students studying to be secondary math teachers in the State of California, providing an exciting option to replace the standard number theory course with a more applied version. After all, cryptography is largely responsible for reenergizing the traditionally very pure subject of number theory into a practical one. The book also contains a decent amount of abstract algebra, presented in a concrete and applied fashion, which should help students to better understand the motivations and purpose of this subject. A chapter dependence chart is provided following this Preface to help instructors design their own courses.

About the Author

Alexander Stanoyevitch completed his doctorate in mathematical analysis at the University of Michigan–Ann Arbor, has held academic positions at the University of Hawaii and the University of Guam, and is presently a professor at California State University–Dominguez Hills. He has published several articles in leading mathematical journals and has been an invited speaker at numerous lectures and conferences in the United States, Europe, and Asia. His research interests include areas of both pure and applied mathematics, and he has taught many upper-level classes to mathematics students as well as computer science students.

Dependency Chart

The following chart should be helpful to readers or instructors aiming to plan courses with this book. Major dependencies are indicated with solid arrows, minor ones with dashed arrows. The two minor dependencies stemming from Chapter 3 rely on only the general function/cryptosystem concepts, not on any of the specific cryptosystems that are introduced in that chapter.

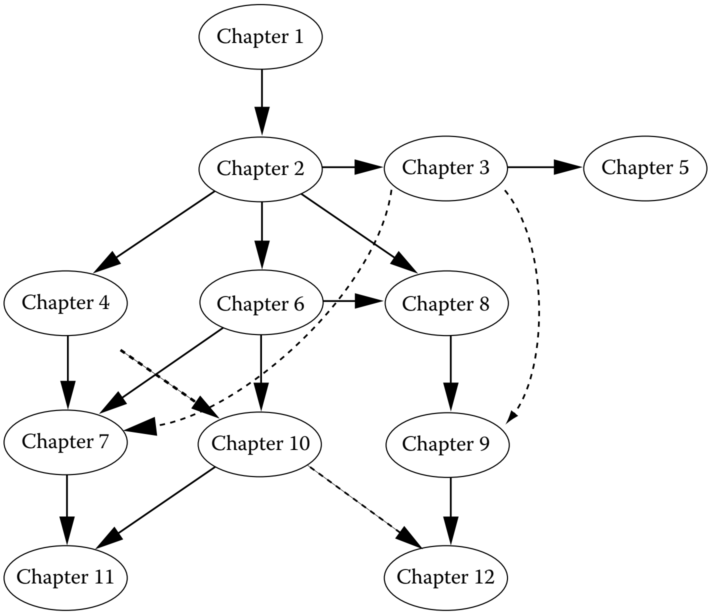

Figure 1 The material surrounding Algorithm 6.2 through Algorithm 6.4, although helpful in gaining understanding of the concepts, is not used in subsequent chapters.

Acknowledgments

Creating such a substantial book could not have been done so effectively without the help and encouragement of many individuals. I am generally grateful to my departments for encouraging and allowing me to work cryptography into my classes, first as topics, and eventually as complete courses. I am grateful to my students, who signed up for these classes although they were not always required to, for their useful feedback on early drafts. I am particularly grateful to my former student Eric Flior; he has carefully read over the entire book and provided some very useful suggestions. Moreover, he has designed the very nice platform-independent applet pages that correspond to several of the core chapters of this book and are available on the author's Web page. I am enormously grateful to my colleague George Jennings, who has also carefully read over the whole book and has provided many useful suggestions and scholarly observations. In addition, George has done a superb job with the task of preparing an instructor's solutions manual that contains completely worked-out solutions for all of the even-numbered exercises (instructors should contact CRC Press to obtain a copy of this manual). I am also grateful to my neighboring colleague Will Murray at California State University–Long Beach, who has read over portions of this book and has provided useful feedback. I thank Yumi Nishimura for creating some of the technical drawings. I thank my mother, Christa Stanoyevitch, for her continued encouragement and very careful proofreading of the entire book. I am grateful to my editor, Sunil Nair, who has provided much insightful guidance, advice, and support throughout the project. Tara Nieuwesteeg, the project editor of this book, has been extremely conscientious and a pleasure to work with throughout the production process. I also wish to express my gratitude to CRC series editor Ken Rosen, who has read over much of the book and has provided me with some very illuminating comments and suggestions. Initial feedback from the anonymous reviewers of the book has also been very helpful. Librarian Rene Stein of the National Cryptographic Museum (located at the NSA headquarters) has provided me with a great deal of historical information and assistance with photographs. I am delighted to express my sincere appreciation to the following illustrious cryptographers who have either provided me with personal photographs or helped me to secure permission for other's photographs of them: Leonard Adleman, Clifford Cocks, Whit Diffie, Joan Daemen, and Vincent Rijmen. I extend special thanks also to the widow of James Ellis for providing me with several photographs.