# Preface

*I can't understand why a person will take a year to write a novel*
*when he can easily buy one for a few dollars.*
— Fred Allen

The first moral question that we faced (like most authors) is: "Why another book?" Available textbooks on public-key cryptography (or cryptography in general) are many [37, 74, 113, 114, 145, 152, 153, 194, 209, 262, 283, 288, 291, 296]. In the presence of all these books, writing another may sound like a waste of energy and effort.

Fortunately, we have a big answer. Most cryptography textbooks today, even many of the celebrated ones, essentially take a narrative approach. While such an approach may be suitable for beginners at an undergraduate level, it misses the finer details in this rapidly growing area of applied mathematics. The fact that public-key cryptography *is* mathematical is hard to deny and a mathematical subject would be better treated in the mathematical way.

This is precisely the point that this book addresses, that is, it proceeds in a canonically mathematical way while revealing cryptographic concepts. This mathematics is often not so simple (and that is why other textbooks didn't bother to mention it), but we plan to stick to mathematical sophistication as far as possible. A typical feature of this book is that it does not rely on anything other than the readers' mathematical intuitions; it develops all the mathematical abstractions starting from scratch. Although computer science and mathematics students nowadays do undergo some courses on discrete structures somewhere in their curricula, we do not assume this; instead we develop the algebra starting at the level of set operations. Simpler structures like groups, rings and fields are followed by more complex concepts like finite fields, algebraic curves, number fields and $p$-adic numbers. The resulting (long) compilation of abstract mathematical tools tends to relieve cryptography students and researchers from consulting many mathematics books for understanding the background concepts. We are happy to offer this self-sufficient treatment complete with proofs and other details. The only place where we had to be somewhat sketchy is the discussion on elliptic and hyperelliptic curves. The mathematics here seems to be too vast to fit in a few pages and we opted for a deliberate simplification of these topics.

A big problem with discrete mathematics is that many of its proofs are existential. However, in order to make things work in a practical environment one must undergo algorithmic studies of algebra and number theory. This is what our book does next. While many algorithmic issues in this area are settled favourably, there remain some problems whose best known algorithmic complexities are still poor. Some of these so-called computationally difficult problems are used to build *secure* public-key cryptosystems. The security of these systems are assumed (rather than proven) and so we extensively deal with the algorithms known till date to solve these difficult problems. This is precisely the point that utilizes the mathematics developed in earlier chapters, to a great extent.

In Chapter 5, we eventually hit upon the culmination of all these mathematical and algorithmic studies in the design of public-key systems for achieving various cryptographic goals. Under the theoretical base developed in earlier chapters, Chapter 5 turns out to be an easy chapter. This is our way of looking into the problem, namely, a formal bottom–up approach. We claim to be different from most textbooks in this regard. Our discussion of mathematics is not for its own sake, but to develop the foundation of cryptographic primitives.

We then turn to some purely implementation and practical issues of public-key cryptography. Standards proposed by organizations such as IEEE and RSA Security Inc. promote interoperability of using crypto primitives in Internet applications. We then look at some small applications of the crypto basics. Some indirect ways of cryptanalysis are described next. These techniques (side-channel and backdoor attacks) give the book a strong practical flavour in tandem with its otherwise formal appearance.

As an eleventh-hour decision, we added a final chapter to our book, a chapter on quantum computation and its implications on public-key cryptography. Although somewhat theoretical at this point, quantum computation exhibits important ramifications in public-key cryptography. The mathematics behind quantum mechanics and computation are never discussed earlier just to highlight the distinctive nature of this chapter, which may perhaps be titled *cryptography in future*.

This schematic description of this book perhaps makes it clear that this book is better suited as a graduate-level textbook. A one- or two-semester graduate or advanced undergraduate course can run based on the contents of this book. Self-studying this book is also possible at an advanced graduate or research level, but is expected to be difficult at an undergraduate level. We highlight the importance of classroom teaching, if an undergraduate course is to be based on this textbook.

We rated different items in the book by their levels of difficulty and/or mathematical sophistication. Unstarred items can be covered even in undergraduate courses. Items marked by single stars can be taken seriously for a second course or a second reading. Doubly starred items, on the other hand, are research-level materials and can be pursued only in really advanced courses or for undergoing research. Inclusion of a good amount of these advanced topics marks another distinction of this book compared to other available textbooks.

The book comes with plenty of exercises. We have two-fold motivations behind these exercises. In the first place, they help the readers deepen their understanding of the matter discussed in the text. In the second place, some of these exercises build additional theory that we omit in the text proper. We occasionally make use of these additional topics in proving and/or explaining results in the text. We do not classify the exercises into easy and difficult ones, but specify hints, some of which are pretty explicit, for intellectually challenging parts. We separate out the hints in an appendix near the end of this book and leave the marker **[H]** in appropriate locations of the statements of the exercises. This practice prevents a reader from accidentally seeing a hint. Only when the reader gets stuck, (s)he can look at the hints at the end. We believe that the exercises, together with our discussion on algorithms and implementation issues, will offer serious students many ways to carry out substantial implementation work to further their research and development in cryptography.

Every chapter ends with annotated references for further studies. We do not claim to be encyclopaedic in this respect. Instead we mention only those references that, we feel, are directly related to the topics dealt with in the respective chapters.

As a trade-off between bulk and coverage, we had to leave many issues untouched. For example, we were limited by constraints of space to present symmetric-key cryptography in detail. However, in view of its importance today, we include brief discussions in an appendix on block ciphers, stream ciphers and hash functions. We also do not discuss anything about formal security of public-key protocols. The issues related to *provable security* are at the minimum theoretically important in the study of cryptography, but are entirely left out here. Only a brief discussion on the implication of complexity theory on the security of public-key protocols is included in another appendix. The *Handbook of Applied Cryptography* [194] by Menezes et al. can supplement this book for learning symmetric techniques, whereas the book by Delfs and Knebl [74] or those by Goldreich [113, 114] can be consulted for formal security issues.

We are indebted to everybody whose criticism, encouragement and support made this project materializable. Special thanks go to Bimal Roy, Chandan Mazumdar, C. Pandurangan, Debdeep Mukhopadhyay, Dipanwita Roychowdhury, Gagan Garg, Hartmut Wiebe, H. V. Kumar Swamy, Indranil Sengupta, Kapil Paranjape, Manindra Agarwal, Palash Sarkar, Rajesh Pillai, Rana Barua, R. Balasubramanian, Sanjay Barman, Shailesh, Satrajit Ghosh, Souvik Bhattacherjee, Srihari Vavilapalli, Subhamoy Maitra, Surjyakanta Mohapatro, and Uwe Storch. This book has been tested in postgraduate courses in the Indian Institute of Science, Bangalore, and in the Indian Institute of Technology Kharagpur. We sincerely thank all our students for pointing out many errors and suggesting several improvements. We express our deep gratitude to our family members for their constant understanding and moral support. We are also indebted to our institutes for providing the wonderful intellectual climate for completing this work.

A. D.
C. E. V. M.