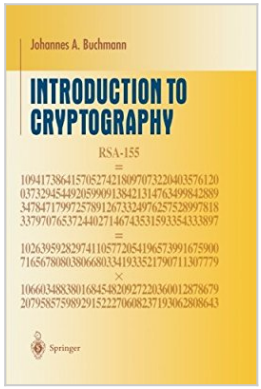

Introduction to Cryptography (Undergraduate Texts in Mathematics)

By Johannes Buchmann

Introduction to Cryptography (Undergraduate Texts in Mathematics) By Johannes Buchmann

Cryptography is a key technology in electronic security systems. Modern cryptograpic techniques have many uses, such as to digitally sign documents, for access control, to implement electronic money, and for copyright protection. Because of these important uses it is necessary that users be able to estimate the efficiency and security of cryptographic techniques. It is not sufficient for them to know only how the techniques work. This book is written for readers who want to learn about mod ern cryptographic algorithms and their mathematical foundation but who do not have the necessary mathematical background. It is my goal to explain the basic techniques of modern cryptography, including the necessary mathematical results from linear algebra, algebra, number theory, and probability theory. I assume only basic mathematical knowledge. The book is based on courses in cryptography that I have been teaching at the Technical University, Darmstadt, since 1996. I thank all students who attended the courses and who read the manuscript carefully for their interest and support. In particular, I would like to thank Harald Baier, Gabi Barking, Manuel Breuning, Sa fuat Hamdy, Birgit Henhapl, Michael Jacobson (who also corrected my English), Andreas Kottig, Markus Maurer, Andreas Meyer, Stefan v vi Preface Neis, Sachar Paulus, Thomas Pfahler, Marita Skrobic, Edlyn Thske, Patrick Theobald, and Ralf-Philipp Weinmann. I also thank the staff at Springer-Verlag, in particular Martin Peters, Agnes Herrmann, Claudia Kehl, Ina Lindemann, and Thrry Kornak, for their support in the preparation of this book.

Introduction to Cryptography (Undergraduate Texts in Mathematics)

By Johannes Buchmann

Introduction to Cryptography (Undergraduate Texts in Mathematics) By Johannes Buchmann

Cryptography is a key technology in electronic security systems. Modern cryptograpic techniques have many uses, such as to digitally sign documents, for access control, to implement electronic money, and for copyright protection. Because of these important uses it is necessary that users be able to estimate the efficiency and security of cryptographic techniques. It is not sufficient for them to know only how the techniques work. This book is written for readers who want to learn about mod ern cryptographic algorithms and their mathematical foundation but who do not have the necessary mathematical background. It is my goal to explain the basic techniques of modern cryptography, including the necessary mathematical results from linear algebra, algebra, number theory, and probability theory. I assume only basic mathematical knowledge. The book is based on courses in cryptography that I have been teaching at the Technical University, Darmstadt, since 1996. I thank all students who attended the courses and who read the manuscript carefully for their interest and support. In particular, I would like to thank Harald Baier, Gabi Barking, Manuel Breuning, Sa fuat Hamdy, Birgit Henhapl, Michael Jacobson (who also corrected my English), Andreas Kottig, Markus Maurer, Andreas Meyer, Stefan v vi Preface Neis, Sachar Paulus, Thomas Pfahler, Marita Skrobic, Edlyn Thske, Patrick Theobald, and Ralf-Philipp Weinmann. I also thank the staff at Springer-Verlag, in particular Martin Peters, Agnes Herrmann, Claudia Kehl, Ina Lindemann, and Thrry Kornak, for their support in the preparation of this book.

Introduction to Cryptography (Undergraduate Texts in Mathematics) By Johannes Buchmann Bibliography

- Sales Rank: #11272698 in Books
- Brand: Brand: Springer
- Published on: 2001-01-01
- Original language: English
- Number of items: 1
- Dimensions: 9.25" h x .68" w x 6.10" l, .93 pounds
- Binding: Paperback
- 281 pages

Editorial Review

From the Back Cover

Cryptography is a key technology in electronic key systems. It is used to keep data secret, digitally sign documents, access control, etc. Therefore, users should not only know how its techniques work, but they must also be able to estimate their efficiency and security. For this new edition, the author has updated the discussion of the security of encryption and signature schemes and recent advances in factoring and computing discrete logarithms. He has also added descriptions of time-memory trade of attacks and algebraic attacks on block ciphers, the Advanced Encryption Standard, the Secure Hash Algorithm, secret sharing schemes, and undeniable and blind signatures.

Johannes A. Buchmann is a Professor of Computer Science and Mathematics at the Technical University of Darmstadt, and the Associate Editor of the Journal of Cryptology. In 1985, he received the Feodor Lynen Fellowship of the Alexander von Humboldt Foundation. Furthermore, he has received the most prestigious award in science in Germany, the Leibniz Award of the German Science Foundation.

About the first edition:

It is amazing how much Buchmann is able to do in under 300 pages: self-contained explanations of the relevant mathematics (with proofs); a systematic introduction to symmetric cryptosystems, including a detailed description and discussion of DES; a good treatment of primality testing, integer factorization, and algorithms for discrete logarithms; clearly written sections describing most of the major types of cryptosystems....This book is an excellent reference, and I believe it would also be a good textbook for a course for mathematics or computer science majors..."

-Neal Koblitz, The American Mathematical Monthly

Users Review

From reader reviews:

Mary Partee:

Here thing why this particular Introduction to Cryptography (Undergraduate Texts in Mathematics) are different and dependable to be yours. First of all examining a book is good nevertheless it depends in the content from it which is the content is as scrumptious as food or not. Introduction to Cryptography (Undergraduate Texts in Mathematics) giving you information deeper including different ways, you can find any book out there but there is no guide that similar with Introduction to Cryptography (Undergraduate Texts in Mathematics). It gives you thrill studying journey, its open up your personal eyes about the thing this happened in the world which is maybe can be happened around you. You can bring everywhere like in park your car, café, or even in your approach home by train. Should you be having difficulties in bringing the imprinted book maybe the form of Introduction to Cryptography (Undergraduate Texts in Mathematics) in e-book can be your alternate.

Mindy Munson:

The e-book untitled Introduction to Cryptography (Undergraduate Texts in Mathematics) is the book that recommended to you to read. You can see the quality of the book content that will be shown to you. The language that article author use to explained their way of doing something is easily to understand. The article author was did a lot of exploration when write the book, to ensure the information that they share to you is absolutely accurate. You also can get the e-book of Introduction to Cryptography (Undergraduate Texts in Mathematics) from the publisher to make you a lot more enjoy free time.

Lorenza Jones:

This Introduction to Cryptography (Undergraduate Texts in Mathematics) is great e-book for you because the content that is full of information for you who else always deal with world and still have to make decision every minute. This specific book reveal it facts accurately using great coordinate word or we can state no rambling sentences within it. So if you are read it hurriedly you can have whole facts in it. Doesn't mean it only will give you straight forward sentences but hard core information with splendid delivering sentences. Having Introduction to Cryptography (Undergraduate Texts in Mathematics) in your hand like obtaining the world in your arm, facts in it is not ridiculous 1. We can say that no reserve that offer you world inside ten or fifteen moment right but this reserve already do that. So , this can be good reading book. Hi Mr. and Mrs. stressful do you still doubt in which?

Haley Thacker:

Many people spending their time frame by playing outside along with friends, fun activity using family or just watching TV the whole day. You can have new activity to enjoy your whole day by reading through a book. Ugh, you think reading a book can really hard because you have to accept the book everywhere? It fine you can have the e-book, bringing everywhere you want in your Mobile phone. Like Introduction to Cryptography (Undergraduate Texts in Mathematics) which is keeping the e-book version. So , try out this book? Let's view.

Read Introduction to Cryptography (Undergraduate Texts in Mathematics) By Johannes Buchmann for online ebook

Introduction to Cryptography (Undergraduate Texts in Mathematics) By Johannes Buchmann Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read Introduction to Cryptography (Undergraduate Texts in Mathematics) By Johannes Buchmann books to read online.

Online Introduction to Cryptography (Undergraduate Texts in Mathematics) By Johannes Buchmann ebook PDF download

Introduction to Cryptography (Undergraduate Texts in Mathematics) By Johannes Buchmann Doc

Introduction to Cryptography (Undergraduate Texts in Mathematics) By Johannes Buchmann Mobipocket

Introduction to Cryptography (Undergraduate Texts in Mathematics) By Johannes Buchmann EPub