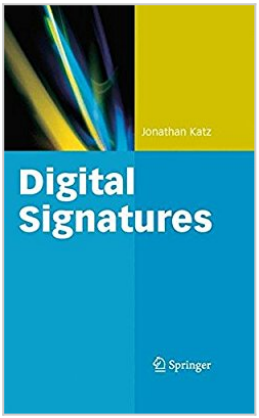

Digital Signatures (Advances in Information Security)

By Jonathan Katz

Digital Signatures (Advances in Information Security) By Jonathan Katz

As a beginning graduate student, I recall being frustrated by a general lack of acces sible sources from which I could learn about (theoretical) cryptography. I remember wondering: why aren’t there more books presenting the basics of cryptography at an introductory level? Jumping ahead almost a decade later, as a faculty member my graduate students now ask me: what is the best resource for learning about (various topics in) cryptography? This monograph is intended to serve as an answer to these 1 questions ? at least with regard to digital signature schemes. Given the above motivation, this book has been written with a beginninggraduate student in mind: a student who is potentially interested in doing research in the ?eld of cryptography, and who has taken an introductory course on the subject, but is not sure where to turn next. Though intended primarily for that audience, I hope that advanced graduate students and researchers will ?nd the book useful as well. In addition to covering various constructions of digital signature schemes in a uni?ed framework, this text also serves as a compendium of various “folklore” results that are, perhaps, not as well known as they should be. This book could also serve as a textbook for a graduate seminar on advanced cryptography; in such a class, I expect the entire book could be covered at a leisurely pace in one semester with perhaps some time left over for excursions into related topics.

Digital Signatures (Advances in Information Security)

By Jonathan Katz

Digital Signatures (Advances in Information Security) By Jonathan Katz

As a beginning graduate student, I recall being frustrated by a general lack of acces sible sources from which I could learn about (theoretical) cryptography. I remember wondering: why aren't there more books presenting the basics of cryptography at an introductory level? Jumping ahead almost a decade later, as a faculty member my graduate students now ask me: what is the best resource for learning about (various topics in) cryptography? This monograph is intended to serve as an answer to these 1 questions ? at least with regard to digital signature schemes. Given the above motivation, this book has been written with a beginninggraduate student in mind: a student who is potentially interested in doing research in the ?eld of cryptography, and who has taken an introductory course on the subject, but is not sure where to turn next. Though intended primarily for that audience, I hope that advanced graduate students and researchers will ?nd the book useful as well. In addition to covering various constructions of digital signature schemes in a uni?ed framework, this text also serves as a compendium of various "folklore" results that are, perhaps, not as well known as they should be. This book could also serve as a textbook for a graduate seminar on advanced cryptography; in such a class, I expect the entire book could be covered at a leisurely pace in one semester with perhaps some time left over for excursions into related topics.

Digital Signatures (Advances in Information Security) By Jonathan Katz Bibliography

- Rank: #5721150 in Books
- Published on: 2010-05-15
- Original language: English
- Number of items: 1
- Dimensions: 9.21" h x .50" w x 6.14" l, 1.03 pounds
- Binding: Hardcover
- 192 pages

Editorial Review

Review

From the book reviews:

“The book talks about the constructions of digital signatures and drives it home. Each chapter is rigorous and complete in its own right, yet there is a level of simplicity and elegance maintained throughout the book that makes it very readable. … The book is essentially a ‘Greatest Hits Collection’ of Digital Signatures, and I would highly recommend it to graduate students and early stage researchers interested in cryptography and Digital Signatures, who have taken a first course in cryptography.” (Subhayan Roy Moulick, SIGACT News, Vol. 46 (1), 2015)

“This book is a basic and fundamental reference for studying and understanding digital signature schemes and all aspects related to their security. This very interesting book has been written mainly for graduate students, but it should also prove useful for researchers and lecturers. … Each chapter ends with a valuable section suggesting further reading on topics dealt with in that chapter.” (Luis Hernández Encinas, Mathematical Reviews, Issue 2011 i)

“This book contains a sound treatment of digital signature schemes. The intended audience is in first place ‘…a beginning graduate student who is potentially interested in doing research in the field of cryptography.’ The book does not only provide a survey of most of the current signature schemes but demonstrate clear statements about the achievable security in the sense of provable security. This makes it valuable also for the advanced researcher.” (Ulrich Tipp, Zentralblatt MATH, Vol. 1202, 2011)

“Katz gives a base-level treatise on the subject of digital signatures by providing readers with a comprehensive understanding of the security guarantees, with descriptions and details of well-known secure signature schemes in the cryptographic literature. … The target audience is graduate students and research scholars of advanced cryptography. … A very useful and noteworthy feature of the book is that, at the end of each chapter, the author gives commentary on the relevant and referred literature survey he did for that chapter.” (C. S. Arora, ACM Computing Reviews, August, 2011)

From the Back Cover

Digital Signatures is the first comprehensive account of the theoretical principles and techniques used in the design of provably secure signature schemes. In addition to providing the reader with a better understanding of the security guarantees provided by digital signatures, the book also contains full descriptions and detailed proofs for essentially all known secure signature schemes in the cryptographic literature. A valuable reference for students, professors, and researchers, Digital Signature Schemes can be used for self-study, as a supplement to a course on theoretical cryptography, or as a textbook in a graduate-level seminar.

About the Author

Jonathan Katz is an associate professor in the Department of Computer Science at the University of Maryland. Active in the cryptography research community, he has held visiting positions at UCLA, '{E}cole Normale Sup'{e}rieure, and IBM. He has given several introductory lectures on cryptography to general audiences in both industry and government, and is an author of the textbook "Introduction to Modern Cryptography".

Users Review

From reader reviews:

Jessica Peacock:

Reading a reserve can be one of a lot of pastime that everyone in the world adores. Do you like reading book so. There are a lot of reasons why people enjoyed. First reading a book will give you a lot of new info. When you read a book you will get new information since book is one of various ways to share the information or even their idea. Second, looking at a book will make an individual more imaginative. When you examining a book especially fictional works book the author will bring you to definitely imagine the story how the character types do it anything. Third, you are able to share your knowledge to some others. When you read this Digital Signatures (Advances in Information Security), you could tells your family, friends and also soon about yours book. Your knowledge can inspire others, make them reading a e-book.

Bryan Jones:

Reading a book tends to be new life style within this era globalization. With looking at you can get a lot of information that can give you benefit in your life. Using book everyone in this world could share their idea. Textbooks can also inspire a lot of people. A lot of author can inspire their particular reader with their story or perhaps their experience. Not only the storyline that share in the textbooks. But also they write about the data about something that you need case in point. How to get the good score toefl, or how to teach your kids, there are many kinds of book that you can get now. The authors nowadays always try to improve their ability in writing, they also doing some research before they write for their book. One of them is this Digital Signatures (Advances in Information Security).

Sandra Lowe:

Your reading sixth sense will not betray anyone, why because this Digital Signatures (Advances in Information Security) guide written by well-known writer who really knows well how to make book that could be understand by anyone who have read the book. Written inside good manner for you, dripping every ideas and publishing skill only for eliminate your personal hunger then you still skepticism Digital Signatures (Advances in Information Security) as good book not just by the cover but also by the content. This is one e-book that can break don't determine book by its cover, so do you still needing an additional sixth sense to pick this!? Oh come on your looking at sixth sense already told you so why you have to listening to an additional sixth sense.

Alexander Pridmore:

Beside this Digital Signatures (Advances in Information Security) in your phone, it can give you a way to get nearer to the new knowledge or facts. The information and the knowledge you can got here is fresh from the oven so don't become worry if you feel like an previous people live in narrow small town. It is good thing to have Digital Signatures (Advances in Information Security) because this book offers for you readable information. Do you occasionally have book but you rarely get what it's facts concerning. Oh come on, that will not happen if you have this within your hand. The Enjoyable blend here cannot be questionable, just like

treasuring beautiful island. So do you still want to miss it? Find this book and read it from right now!

Read Digital Signatures (Advances in Information Security) By Jonathan Katz for online ebook

Digital Signatures (Advances in Information Security) By Jonathan Katz 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 Digital Signatures (Advances in Information Security) By Jonathan Katz books to read online.

Online Digital Signatures (Advances in Information Security) By Jonathan Katz ebook PDF download

Digital Signatures (Advances in Information Security) By Jonathan Katz Doc

Digital Signatures (Advances in Information Security) By Jonathan Katz Mobipocket

Digital Signatures (Advances in Information Security) By Jonathan Katz EPub