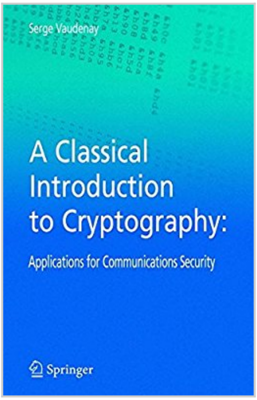

Serge Vaudenay

A Classical Introduction to Cryptography:

Applications for Communications Security

Springer

A Classical Introduction to Cryptography: Applications for Communications Security

By Serge Vaudenay

A Classical Introduction to Cryptography: Applications for Communications Security By Serge Vaudenay

A Classical Introduction to Cryptography: Applications for Communications Security introduces fundamentals of information and communication security by providing appropriate mathematical concepts to prove or break the security of cryptographic schemes.

This advanced-level textbook covers conventional cryptographic primitives and cryptanalysis of these primitives; basic algebra and number theory for cryptologists; public key cryptography and cryptanalysis of these schemes; and other cryptographic protocols, e.g. secret sharing, zero-knowledge proofs and undeniable signature schemes.

A Classical Introduction to Cryptography: Applications for Communications Security is designed for upper-level undergraduate and graduate-level students in computer science. This book is also suitable for researchers and practitioners in industry. A separate exercise/solution booklet is available as well, please go to www.springeronline.com under author: Vaudenay for additional details on how to purchase this booklet.

A Classical Introduction to Cryptography: Applications for Communications Security

By Serge Vaudenay

A Classical Introduction to Cryptography: Applications for Communications Security By Serge Vaudenay

A Classical Introduction to Cryptography: Applications for Communications Security introduces fundamentals of information and communication security by providing appropriate mathematical concepts to prove or break the security of cryptographic schemes.

This advanced-level textbook covers conventional cryptographic primitives and cryptanalysis of these primitives; basic algebra and number theory for cryptologists; public key cryptography and cryptanalysis of these schemes; and other cryptographic protocols, e.g. secret sharing, zero-knowledge proofs and undeniable signature schemes.

A Classical Introduction to Cryptography: Applications for Communications Security is designed for upper-level undergraduate and graduate-level students in computer science. This book is also suitable for researchers and practitioners in industry. A separate exercise/solution booklet is available as well, please go to www.springeronline.com under author: Vaudenay for additional details on how to purchase this booklet.

A Classical Introduction to Cryptography: Applications for Communications Security By Serge Vaudenay Bibliography

- Sales Rank: #985169 in Books
- Published on: 2005-09-16
- Original language: English
- Number of items: 1
- Dimensions: 9.21" h x .81" w x 6.14" l, 1.60 pounds
- Binding: Hardcover
- 336 pages

Editorial Review

Review

From the reviews:

"This impressive hardback introduces fundamentals of information and communications security by providing mathematical concepts to prove or break the security of cryptographic schemes. … The book is designed for upper-level undergraduates and graduate level students in computer science. This comprehensive volume is also suitable for researchers and practitioners in industry." (Cryptologia, Vol. 30, 2006)

"This book presents, using a chronological order, both conventional cryptography and public-key cryptography, as well as the two sides of cryptanalysis: adversary modelling and proof reduction. … This advanced-level textbook is recommended for those interested in cryptography and its applications: students, researchers, computer scientists, mathematicians, engineers, and practitioners in industry." (Michael M. Dediu, Mathematical Reviews, Issue 2007 b)

From the Back Cover

A Classical Introduction to Cryptography: Applications for Communications Security introduces fundamentals of information and communication security by providing appropriate mathematical concepts to prove or break the security of cryptographic schemes.

This advanced-level textbook covers conventional cryptographic primitives and cryptanalysis of these primitives; basic algebra and number theory for cryptologists; public key cryptography and cryptanalysis of these schemes; and other cryptographic protocols, e.g. secret sharing, zero-knowledge proofs and undeniable signature schemes.

A Classical Introduction to Cryptography: Applications for Communications Security is rich with algorithms, including exhaustive search with time/memory tradeoffs; proofs, such as security proofs for DSA-like signature schemes; and classical attacks such as collision attacks on MD4. Hard-to-find standards, e.g. SSH2 and security in Bluetooth, are also included.

A Classical Introduction to Cryptography: Applications for Communications Security is designed for upper-level undergraduate and graduate-level students in computer science. This book is also suitable for researchers and practitioners in industry. A separate exercise/solution booklet is available as well, please go to www.springeronline.com under author: Vaudenay for additional details on how to purchase this booklet.

Users Review

From reader reviews:

Leonard White:

Have you spare time to get a day? What do you do when you have considerably more or little spare time? Yep, you can choose the suitable activity with regard to spend your time. Any person spent their very own spare time to take a walk, shopping, or went to typically the Mall. How about open as well as read a book called A Classical Introduction to Cryptography: Applications for Communications Security? Maybe it is to become best activity for you. You understand beside you can spend your time along with your favorite's book, you can more intelligent than before. Do you agree with it is opinion or you have various other opinion?

Janice Arias:

Do you have something that you enjoy such as book? The e-book lovers usually prefer to opt for book like comic, small story and the biggest some may be novel. Now, why not seeking A Classical Introduction to Cryptography: Applications for Communications Security that give your entertainment preference will be satisfied by means of reading this book. Reading routine all over the world can be said as the opportinity for people to know world far better then how they react towards the world. It can't be mentioned constantly that reading practice only for the geeky individual but for all of you who wants to be success person. So , for every you who want to start examining as your good habit, you are able to pick A Classical Introduction to Cryptography: Applications for Communications Security become your own starter.

Richard Byrnes:

The book untitled A Classical Introduction to Cryptography: Applications for Communications Security contain a lot of information on the idea. The writer explains the girl idea with easy means. The language is very simple to implement all the people, so do certainly not worry, you can easy to read it. The book was compiled by famous author. The author brings you in the new age of literary works. You can actually read this book because you can please read on your smart phone, or device, so you can read the book inside anywhere and anytime. If you want to buy the e-book, you can open their official web-site in addition to order it. Have a nice go through.

Jennifer Williams:

You can get this A Classical Introduction to Cryptography: Applications for Communications Security by look at the bookstore or Mall. Just viewing or reviewing it might to be your solve issue if you get difficulties for ones knowledge. Kinds of this book are various. Not only by simply written or printed and also can you enjoy this book simply by e-book. In the modern era similar to now, you just looking by your mobile phone and searching what your problem. Right now, choose your own ways to get more information about your reserve. It is most important to arrange yourself to make your knowledge are still upgrade. Let's try to choose appropriate ways for you.

Download and Read Online A Classical Introduction to Cryptography: Applications for Communications Security By Serge Vaudenay #FOY26MDJBXE

Read A Classical Introduction to Cryptography: Applications for Communications Security By Serge Vaudenay for online ebook

A Classical Introduction to Cryptography: Applications for Communications Security By Serge Vaudenay 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 A Classical Introduction to Cryptography: Applications for Communications Security By Serge Vaudenay books to read online.

Online A Classical Introduction to Cryptography: Applications for Communications Security By Serge Vaudenay ebook PDF download

A Classical Introduction to Cryptography: Applications for Communications Security By Serge Vaudenay Doc

A Classical Introduction to Cryptography: Applications for Communications Security By Serge Vaudenay Mobipocket

A Classical Introduction to Cryptography: Applications for Communications Security By Serge Vaudenay EPub