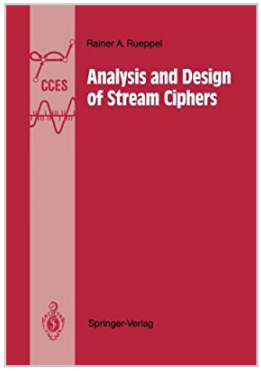

Analysis and Design of Stream Ciphers (Communications and Control Engineering)

By Rainer A. Rueppel

Analysis and Design of Stream Ciphers (Communications and Control Engineering) By Rainer A. Rueppel

It is now a decade since the appearance of W. Diffie and M. E. Hellmann's startling paper, "New Directions in Cryptography". This paper not only established the new field of public-key cryptography but also awakened scientific interest in secret-key cryptography, a field that had been the almost exclusive domain of secret agencies and mathematical hobbyist. A number of ex cellent books on the science of cryptography have appeared since 1976. In the main, these books thoroughly treat both public-key systems and block ciphers (i. e. secret-key ciphers with no memo ry in the enciphering transformation) but give short shrift to stream ciphers (i. e. , secret-key ciphers wi th memory in the enciphering transformation). Yet, stream ciphers, such as those . implemented by rotor machines, have played a dominant role in past cryptographic practice, and, as far as I can determine, re main still the workhorses of commercial, military and diplomatic secrecy systems. My own research interest in stream ciphers found a natural re sonance in one of my doctoral students at the Swiss Federal Institute of Technology in Zurich, Rainer A. Rueppe1. As Rainer was completing his dissertation in late 1984, the question arose as to where he should publish the many new results on stream ciphers that had sprung from his research.

Analysis and Design of Stream Ciphers (Communications and Control Engineering)

By Rainer A. Rueppel

Analysis and Design of Stream Ciphers (Communications and Control Engineering) By Rainer A. Rueppel

It is now a decade since the appearance of W. Diffie and M. E. Hellmann's startling paper, "New Directions in Cryptography". This paper not only established the new field of public-key cryptography but also awakened scientific interest in secret-key cryptography, a field that had been the almost exclusive domain of secret agencies and mathematical hobbyist. A number of ex cellent books on the science of cryptography have appeared since 1976. In the main, these books thoroughly treat both public-key systems and block ciphers (i. e. secret-key ciphers with no memo ry in the enciphering transformation) but give short shrift to stream ciphers (i. e. , secret-key ciphers wi th memory in the enciphering transformation). Yet, stream ciphers, such as those . implemented by rotor machines, have played a dominant role in past cryptographic practice, and, as far as I can determine, re main still the workhorses of commercial, military and diplomatic secrecy systems. My own research interest in stream ciphers found a natural re sonance in one of my doctoral students at the Swiss Federal Institute of Technology in Zurich, Rainer A. Rueppe1. As Rainer was completing his dissertation in late 1984, the question arose as to where he should publish the many new results on stream ciphers that had sprung from his research.

Analysis and Design of Stream Ciphers (Communications and Control Engineering) By Rainer A. Rueppel Bibliography

- Sales Rank: #1620955 in Books
- Published on: 1986-08-01
- Released on: 1986-08-01
- Original language: English
- Number of items: 1
- Dimensions: 9.61" h x .59" w x 6.69" l, .92 pounds
- Binding: Paperback
- 244 pages

Editorial Review

Users Review

From reader reviews:

Samuel Tapp:

What do you about book? It is not important along? Or just adding material when you need something to explain what the ones you have problem? How about your extra time? Or are you busy individual? If you don't have spare time to try and do others business, it is make one feel bored faster. And you have spare time? What did you do? All people has many questions above. They need to answer that question since just their can do which. It said that about book. Book is familiar in each person. Yes, it is suitable. Because start from on pre-school until university need this particular Analysis and Design of Stream Ciphers (Communications and Control Engineering) to read.

John Bullard:

Spent a free the perfect time to be fun activity to do! A lot of people spent their spare time with their family, or their very own friends. Usually they undertaking activity like watching television, going to beach, or picnic in the park. They actually doing same task every week. Do you feel it? Do you need to something different to fill your personal free time/ holiday? Could possibly be reading a book is usually option to fill your cost-free time/ holiday. The first thing that you'll ask may be what kinds of book that you should read. If you want to try out look for book, may be the e-book untitled Analysis and Design of Stream Ciphers (Communications and Control Engineering) can be excellent book to read. May be it might be best activity to you.

Joseph Southard:

It is possible to spend your free time you just read this book this e-book. This Analysis and Design of Stream Ciphers (Communications and Control Engineering) is simple to bring you can read it in the playground, in the beach, train as well as soon. If you did not get much space to bring the printed book, you can buy the particular e-book. It is make you better to read it. You can save often the book in your smart phone. Therefore there are a lot of benefits that you will get when you buy this book.

Cheree Rodriquez:

Is it you who having spare time in that case spend it whole day through watching television programs or just resting on the bed? Do you need something totally new? This Analysis and Design of Stream Ciphers (Communications and Control Engineering) can be the response, oh how comes? A book you know. You are thus out of date, spending your extra time by reading in this fresh era is common not a nerd activity. So what

these guides have than the others?

Read Analysis and Design of Stream Ciphers (Communications and Control Engineering) By Rainer A. Rueppel for online ebook

Analysis and Design of Stream Ciphers (Communications and Control Engineering) By Rainer A. Rueppel 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 Analysis and Design of Stream Ciphers (Communications and Control Engineering) By Rainer A. Rueppel books to read online.

Online Analysis and Design of Stream Ciphers (Communications and Control Engineering) By Rainer A. Rueppel ebook PDF download

Analysis and Design of Stream Ciphers (Communications and Control Engineering) By Rainer A. Rueppel Doc

Analysis and Design of Stream Ciphers (Communications and Control Engineering) By Rainer A. Rueppel Mobipocket

Analysis and Design of Stream Ciphers (Communications and Control Engineering) By Rainer A. Rueppel EPub

0AFDPIEXNYR: Analysis and Design of Stream Ciphers (Communications and Control Engineering) By Rainer A. Rueppel