Cryptography Engineering: Design Principles and Practical Applications

Niels Ferguson, Bruce Schneier, Tadayoshi Kohno

E-Book Rental (120 Days)  ISBN: 978-1-118-08091-7R120  February 2011  $10.00

E-Book Rental (150 Days)  ISBN: 978-1-118-08091-7R150  February 2011  $11.00


DESCRIPTION

The ultimate guide to cryptography, updated from an author team of the world's top cryptography experts.

Cryptography is vital to keeping information safe, in an era when the formula to do so becomes more and more challenging. Written by a team of world-renowned cryptography experts, this essential guide is the definitive introduction to all major areas of cryptography: message security, key negotiation, and key management. You'll learn how to think like a cryptographer. You'll discover techniques for building cryptography into products from the start and you'll examine the many technical changes in the field.

After a basic overview of cryptography and what it means today, this indispensable resource covers such topics as block ciphers, block modes, hash functions, encryption modes, message authentication codes, implementation issues, negotiation protocols, and more. Helpful examples and hands-on exercises enhance your understanding of the multi-faceted field of cryptography.

• An author team of internationally recognized cryptography experts updates you on vital topics in the field of cryptography

• Shows you how to build cryptography into products from the start

• Examines updates and changes to cryptography
• Includes coverage on key servers, message security, authentication codes, new standards, block ciphers, message authentication codes, and more

Cryptography Engineering gets you up to speed in the ever-evolving field of cryptography.

▲ ABOUT THE AUTHOR

Niels Ferguson is a cryptographer for Microsoft who has designed and implemented cryptographic algorithms, protocols, and large-scale security infrastructures.

Bruce Schneier is an internationally renowned security technologist whose advice is sought by business, government, and the media. He is the author of Applied Cryptography, Secrets and Lies, and Schneier on Security.

Tadayoshi Kohno is a professor at the University of Washington. He is known for his research and for developing innovative new approaches to cryptography and computer security education.

For additional product details, please visit https://www.wiley.com/en-us