Java Cryptography Extensions
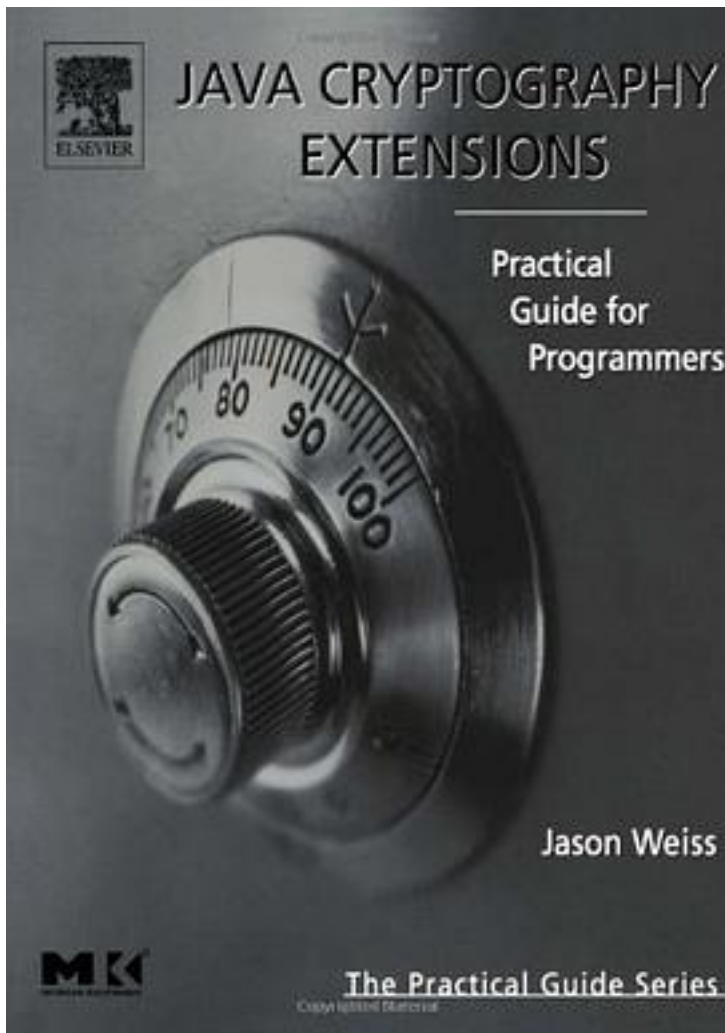
Java Cryptography Extensions_下载链接1_

著者:Weiss, Jason

出版者:

出版时间:2004-3

装帧:

isbn:9780127427515

'For a long time, there has been a need for a practical, down-to-earth developers book

for the Java Cryptography Extension. I am very happy to see there is now a book that can answer many of the technical questions that developers, managers, and researchers have about such a critical topic. I am sure that this book will contribute greatly to the success of securing Java applications and deployments for e-business' - Anthony Nadalin, Java Security Lead Architect, IBM. For many Java developers and software engineers, cryptography is an 'on-demand' programming exercise, where cryptographic concepts are shelved until the next project requires renewed focus. But considerations for cryptography must be made early on in the design process and it's imperative that developers know what kinds of solutions exist. One of Java's solutions to help bridge the gap between academic research and real-world problem solving comes in the form of a well-defined architecture for implementing cryptographic solutions. However, to use the architecture and its extensions, it is important to recognize the pros and cons of different cryptographic algorithms and to know how to implement various devices like key agreements, digital signatures, and message digests, to name a few. In "Java Cryptography Extensions" (JCE), cryptography is discussed at the level that developers need to know to work with the JCE and with their own applications but that doesn't overwhelm by packing in details unimportant to the busy professional. The JCE is explored using numerous code examples and instructional detail, with clearly presented sections on each aspect of the Java library. An online open-source cryptography toolkit and the code for all of the examples further reinforces the concepts covered within the book. No other resource presents so concisely or effectively the exact material needed to begin utilizing the JCE. This book is written by a seasoned veteran of both cryptography and server-side programming. It covers the architecture of the JCE, symmetric ciphers, asymmetric ciphers, message digests, message authentication codes, digital signatures, and managing keys and certificates. It includes a companion web site that contains the code for the examples in the book, open-source cryptographic toolkits, and further resources.

作者介绍:

目录:

Java Cryptography Extensions_下载链接1_

标签

评论

Java Cryptography Extensions_下载链接1_

书评

Java Cryptography Extensions_下载链接1_