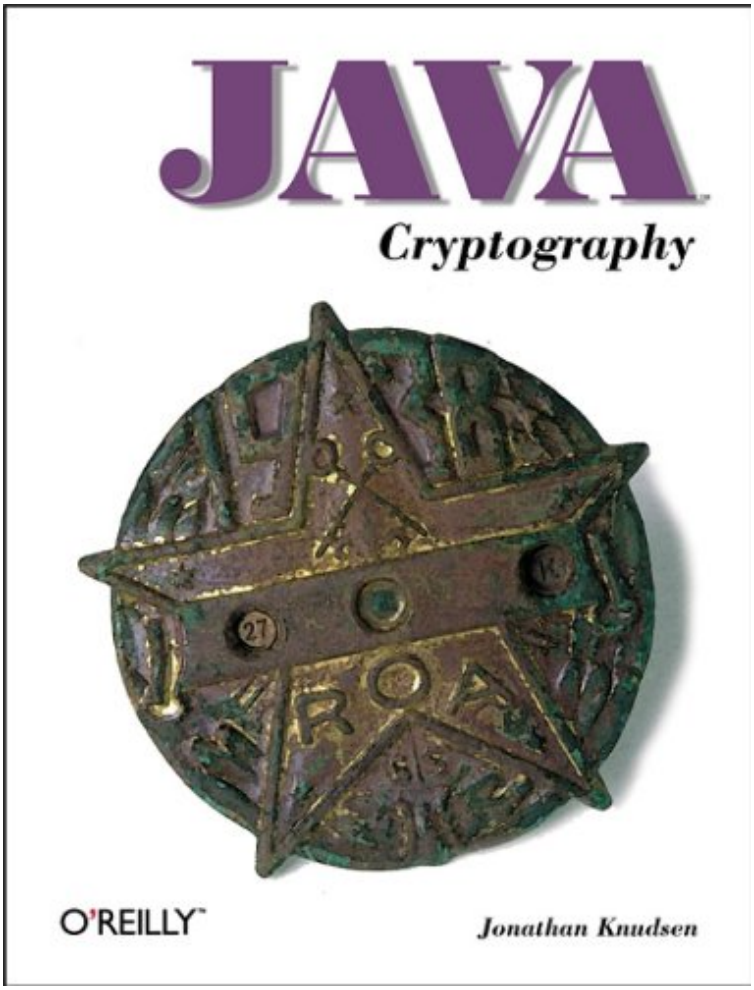
# Java Cryptography (Java Series)

*Von Jonathan Knudsen*
**Download PDF | ePub | DOC | audiobook | ebooks*






Produktinformation -Verkaufsrang: #1679274 in eBooksVerffentlicht am: 1998-05-01Erscheinungsdatum: 2010-05-05File Name: B0043M4ZC0 | File size: 53.Mb

**Von Jonathan Knudsen : Java Cryptography (Java Series)** before purchasing it in order to gage whether or not it would be worth my time, and all praised Java Cryptography (Java Series):

KundenrezensionenHilfreichste Kundenrezensionen4 von 4 Kunden fanden die folgende Rezension hilfreich. Teaches cryptography the wrong wayVon Ein KundeThe goal of this book is to show how to implement a secure application. It does not achieve this. Generally, it is a good idea to rely on algorithms and protocol that are published, well analyzed and preferably standardized. Specially public key cryptography has many pitfalls that are difficult to avoid.However, the author of this book designs his own key exchange protocol and uses ad-hoc padding schemes. This procedure sets a bad example for the reader. The result is what one has to expect from an ad-hoc design: The applications have serious design flaws. For example the ElGamal signature scheme in chapter 9 does not use a hash function besides other omissions. The padding scheme for the ElGamal encryption simply adds 0's and therefore does not prevent

chosen message attacks. The key exchange protocol in chapter 10 constructs a session key from two halves that are sent seperately. Each half can be attacked seperately in a reply attack, etc.To conclude, this book does certainly not show the proper use of cryptography, and hence is hardly worth reading.0 von 0 Kunden fanden die folgende Rezension hilfreich. Written for those without prior crypto experienceVon Ein KundeThis book is intended to teach experienced Java programmers how to add cryptographic elements to their applications. The text is not intended to teach encryption algorithms, basic Java programming, or the overall Java security model: there are other books that fulfill those functions. There is one other limitation: much of the book relies on the Java Cryptography Extensions (JCE) which are only available to those in the United States and Canada (nudge, nudge, wink, wink).Chapter one lists some fundamentals of encryption and the relationship to security. There are also a couple of programs right off the bat that will let you explore message digests, and encrypting and decrypting messages. The basics of confidentiality, authentication, and some major cryptographic algorithms are outlined in chapter two. The explanations are quite terse, but not out of line with the aim of the book. Java Security Architecture (JCA) is explained in chapter three, along with a quick overview of the API (Application Programming Interface) and SPI (Service Provider Interface). Chapter four introduces Java's own pseudo-random number generator, plus programming for key seeds from keyboard timing. Key management, in chapter five, is somewhat weak. The APIs only deal with hierarchical key certification, but this may simply be an example of Knudsen dealing strictly with the language, and leaving the concepts to others. I was, however, bemused at some passages that may have suffered from a lack of copy editing: for example, one section that seemed to confuse production of Message Authentication Codes with working on Macintosh computers. Authentication of various types is covered quite well in chapter six. Chapter seven's guide to encryption covers details not normally dealt with in cryptography texts because it must handle all matters related to getting an encryption algorithm to actually function in an application.Chapter eight gives enough detail about signed applets to prove that they are going to be browser specific for a while. Security provider programming is covered in chapter nine, using the ElGamal algorithm as an example. A sample application is created using an encrypted version of the talk utility in chapter ten. An e-mail application is created in chapter eleven using th provider previously generated in chapter nine. Chapter twelve closes off by looking at security design for the system overall.Appendices review BigInteger arithmetic in Java, the Base64 encoding scheme (an option for converting binary objects to text characters for e-mailing), Java archive files, Javakey, and a quick reference for the Java cryptography classes as covered in the book.Knudsen states that the book is written, as far as possible, without assuming any prior knowledge of cryptography. In this aim he succeeds rather well. The programmer with no background in encryption can still add a reasonable layer of security to his or her application. Those who study further, of course, will be able to ensure a higher level of protection and reliability.0 von 0 Kunden fanden die folgende Rezension hilfreich. The Typical O'Reilly PublicationVon Ein KundeThis book is a fine introduction to cryptography within the "confines" of the Java API from Sun (I don't expect the information in this book to gain widespread acceptance until the next millenium).Not even ten pages into the book, and Knudsen is already discussing the undocumented Java classes for encoding/decoding Base64 arrays .... youch !!I think the author did a commendable job covering the critical issues of this VERY sensitive topic. The author pobably does not expect to get rave reviews after the release of "Applied Java Crytography" -- but then again, THAT book will likey cover the meat and bones that Knudsen's INTRODUCTION didn't touch. He didn't touch it for a reason.But allow me to say right now, THIS book supplies the rudimentary source code (what's legal to distribute, that is) which will be necessary for the cryptographer/cryptanalyst to MASTER before pursuing his/her own classes.This is a new and booming -- albeit delicate -- field .... thanks for writing a book for those of us already experienced in crytography, written in a no-nonsense style, reminding us of the sandbox we're really working in. I had forgotten just how senstive information can be.

KurzbeschreibungCryptography, the science of secret writing, is the biggest, baddest security tool in the application programmer's arsenal. Cryptography provides three services that are crucial in secure programming. These include a cryptographic cipher that protects the secrecy of your data; cryptographic certificates, which prove identity (authentication); and digital signatures, which ensure your data has not been damaged or tampered with.This book covers cryptographic programming in Java. Java 1.1 and Java 1.2 provide extensive support for cryptography with an elegant architecture, the Java Cryptography Architecture (JCA). Another set of classes, the Java Cryptography Extension (JCE), provides additional cryptographic functionality. This book covers the JCA and the JCE from top to bottom, describing the use of the cryptographic classes as well as their innards.The book is designed for moderately experienced Java programmers who want to learn how to build cryptography into their applications. No prior knowledge of cryptography is assumed. The book is peppered with useful examples, ranging from simple demonstrations in the first chapter to full-blown applications in later chapters.Topics include:The Java Cryptography Architecture (JCA)The Java Cryptography Extension (JCE)Cryptographic providersThe Sun key management toolsMessage digests, digital signatures, and certificates (X509v3)Block and stream ciphersImplementations of the

ElGamal signature and cipher algorithmsA network talk application that encrypts all data sent over the networkAn email application that encrypts its messagesCovers JDK 1.2 and JCE 1.2.