Volume 6, Issue 6, August 1999

Telecommunications Electronic Reviews (TER) is a publication of the Library and Information Technology Association.

Contents:

ter issues (/lita/publications/archive/ter)

REVIEW OF: Joshua Marketos. The Java Developer's Toolkit. New York: John Wiley &Sons, 1997.

by Brad Eden

If you are looking for a book that will provide an understandable introduction to Java, as well as basic programming, applications, applets, multithreading, and networking using Java, then this book is for you. If you are looking for a Java book that provides straightforward and practical instructions in that language, as

well as occasional humor and lighthearted chapter titles that guide you through somewhat complicated programming ideas and tips, then this book is definitely for you. If you are looking for the typically dry, complicated, boring computer language programming book, then you need to look elsewhere.

Marketos has written an understandable and entertaining (if such a term can be used with a computer book) introduction and toolkit to the Java programming language. With subchapter titles like "Zen and the art of software maintenance", "The world according to OOP", "Applets and oranges", and "Stupid applet tricks...", Java newbies can experiment and construct all kinds of interesting applications and tools.

A short introduction to the birth of Java, which is described as a "simple, object-oriented, distributed, interpreted, robust, secure, architecture-neutral, portable, high-performance, multithreaded, and dynamic language" by its developers, is followed by explanations on each of these characteristics by the author. A detailed list of what Java can and cannot do is included here, in order to provide upfront to Java newbies its strengths and weaknesses. Chapter 2 looks at the Java Developer's Kit (JDK)--how to use the various tools it provides, and how to install and configure it. Chapter 3 claims to be able to teach object-oriented programming Java in 21 minutes.

Chapter 4 explains simple Java applications and the java.lang package, as well as the two "flavors" of Java development-- applications and applets. Chapter 5 examines Java applets. Chapter 6 provides a detailed explanation and application of the Abstract Window Toolkit (AWT), a generic windowing system that sits on top of native graphical user interfaces (GUIs) to provide a cross-platform GUI capability. Chapter 7 explains Java multithreading, Chapter 8 looks at the Java I/O package, and Chapters 9 and 10 cover Java networking and Java native methods. Chapter 11 deals with designing shopping carts and databases in the Java language for e-commerce. Finally, Chapter 12 provides a glimpse of Java's future potential. A URL links to the source code for all of the applications/applets in the book.

Having little computer experience in programming or in Java, I found this book refreshing and enjoyable to read, given that it is trying to describe how to do programming and system applications in a new computer language. The humor apparent throughout can sometimes be surprising and almost out-of-place in this type of publication, but the information is thorough and well-written. The cost ($29.95) of the book is well within anyone's budget, and I would recommend this book to anyone attempting to experiment with the Java programming language.

Dr. Brad Eden (beden@ccmail.nevada.edu (mailto:beden@ccmail.nevada.edu)) is Head of Cataloging for the University of Nevada at Las Vegas.

table of contents   ter issues (/lita/publications/archive/ter)

REVIEW OF: Jonathan Knudsen. Java Cryptography. O'Reilly and Associates, 1998.

by Ray Olszewski

As the Internet has grown both in absolute size and in the range of activities it supports, users have had an increasing need for methods that provide security in their communications. Fortunately, modern encryption theory has provided mechanisms for secure connections, leading to protocols and services that include SSL (Secure Socket Layer), ssh (secure shell), and PGP (Pretty Good Privacy), as well as other, commercial products.

The programming language Java, designed from the outset to be platform independent and, as of now, almost succeeding in this design goal, had tied its usefulness in many ways to a facility for providing Internet-based services. Not surprisingly, this focus causes Java to include an excellent set of libraries that provide tools for implementing up-to-date encryption methods.

Java Cryptography is a guide to this set of Java capabilities, and it is a good one. It is not for the beginner, at either Java or cryptography--the author assumes from the outset that the reader knows both territories and needs to learn how one of them, encryption methods, works within the other, Java. With this background, he moves quickly and fairly demandingly into the details of implementing the full range of today's encryption requirements in Java.

Individual chapters cover random number generation, using encrypted hashes to authenticate files and messages, implementing and using algorithms for encrypting communication streams, signing applets, encrypting e-mail, and writing a system to generate keys. His examples use the ElGamal encryption method, a variant on Diffie-Hellman that only recently has become generally usable (due to the 1998 expiration of the Diffie-Hellman patent).

The focus is on actual implementation, and in the typical O'Reilly style, this focus means a book rich in working examples. Complete, working applications provided include "CypherMail" for encrypted e-mail, "SafeTalk" to provide network talk services over an encrypted connection, and Java classes that implement ElGamal for message encryption and signatures.

The only weakness I found is in its one departure from standard O'Reilly practice. Due to restrictions imposed by the US government on export of cryptographic software, the author is unable to provide copies of all his source code in downloadable form. This causes a problem in that the code development is spread through the chapters in which each application or library is discussed, and the complete source code for each project is not collected into a single listing. This fragmentation makes actual implementation of the samples something of a challenge. In consequence I did not actually test the applications as part of this review.

With that one caution, though, I recommend this book with enthusiasm. It does a good job of taking the abstract concepts of cryptography and translating them into algorithms that can be implemented using a programming language that is steadily growing in importance. It is a useful book for any applications programmer seeking to improve his or her skills.

Ray Olszewski (ray@comarre.com (mailto:ray@comarre.com) or http://www.comarre.com/ray.html (http://www.comarre.com/ray.html)) is a consulting economist and statistician. His work includes development of custom Web-based software to support on-line research. He spent three years as Network Manager at The Nueva School, a private K-8 school in Hillsborough, California.

document or any part of it for commercial distribution, address requests to the author at ray@comarre.com (mailto:ray@comarre.com).

table of contents ter issues (/lita/publications/archive/ter)

About TER