Preface

The Internet, as a worldwide communication network, has changed our daily life in many ways. A new paradigm of commerce allows individuals to shop online. The World Wide Web (WWW) allows people to share information. The E-mail technology connect people in far-flung corners of the world. This inevitable evolution has also created dependency on the Internet.

The Internet, as an open forum, has created some security problems. Confidentiality, integrity, and authentication are needed. People need to be sure that their Internet communication is kept confidential. When they shop online, they need to be sure that the vendors are authentic. When they send their transactions request to their banks, they want to be certain that the integrity of the message is preserved.

Network security is a set of protocols that allow us to use the Internet comfortably—without worrying about security attacks. The most common tool for providing network security is cryptography, an old technique that has been revived and adapted to network security. This book first introduces the reader to the principles of cryptography and then applies those principles to describe network security protocols.

Features of the Book

Several features of this text are designed to make it particularly easy for readers to understand cryptography and network security.

Structure

This text uses an incremental approach to teaching cryptography and network security. It assumes no particular mathematical knowledge, such as number theory or abstract algebra. However, because cryptography and network security cannot be discussed without some background in these areas of mathematics, these topics are discussed in Chapters 2, 4, and 9. Readers who are familiar with these areas of mathematics can ignore these chapters. Chapters 1 through 15 discuss cryptography. Chapters 16 through 18 discuss network security.

Visual Approach

This text presents highly technical subject matters without complex formulas by using a balance of text and figures. More than 400 figures accompanying the text provide a visual and intuitive opportunity for understanding the materials. Figures are particularly important in explaining difficult cryptographic concepts and complex network security protocols.

Algorithms

Algorithms play an important role in teaching cryptography. To make the presentation independent from any computer language, the algorithms have been given in pseudocode that can be easily programmed in a modern language. At the website for this text, the corresponding programs are available for download.

Highlighted Points

Important concepts are emphasized in highlighted boxes for quick reference and immediate attention.

Examples

Each chapter presents a large number of examples that apply concepts discussed in the chapter. Some examples merely show the immediate use of concepts and formulae; some show the actual input/output relationships of ciphers; others give extra information to better understand some difficult ideas.

Recommended Reading

At the end of each chapter, the reader will find a list of books for further reading.

Key Terms

Key terms appear in bold in the chapter text, and a list of key terms appear at the end of each chapter. All key terms are also defined in the glossary at the end of the book.

Summary

Each chapter ends with a summary of the material covered in that chapter. The summary provides a brief overview of all the important points in the chapter.

Practice Set

At the end of each chapter, the students will find a practice set designed to reinforce and apply salient concepts. The practice set consists of two parts: review questions and exercises. The review questions are intended to test the reader's first-level understanding of the material presented in the chapter. The exercises require deeper understanding of the material.

Appendices

The appendices provide quick reference material or a review of materials needed to understand the concepts discussed in the book. Some discussions of mathematical topics