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 are also presented in the appendices to avoid distracting those readers who are already familiar with these materials.

Proofs

Mathematical facts are mentioned in the chapters without proofs to emphasize the results of applying the facts. For those interested reader the proofs are given in Appendix Q.

Glossary and Acronyms

At the end of the text, the reader will find an extensive glossary and a list of acronyms.

Contents

After the introductory Chapter 1, the book is divided into four parts:

Part One: Symmetric-Key Encipherment

Part One introduces the symmetric-key cryptography, both traditional and modern. The chapters in this part emphasize the use of symmetric-key cryptography in providing secrecy. Part One includes Chapters 2 through 8.

Part Two: Asymmetric-Key Encipherment

Part Two discusses asymmetric-key cryptography. The chapters in this part show how asymmetric-key cryptography can provide security. Part Two includes Chapters 9 and 10.

Part Three: Integrity, Authentication, and Key Management

Part Three shows how cryptographic hashing functions can provide other security services, such as message integrity and authentication. The chapters in this part also show how asymmetric-key and symmetric-key cryptography can complement each other. Part Three includes Chapters 11 through 15.

Part Four: Network Security

Part Four shows how the cryptography discussed in Part One through Three can be used to create network security protocols at three levels of the Internet networking model. Part Four includes Chapters 16 to 18.

How to Use this Book

This book is written for both an academic and a professional audience. Interested professionals can use it for self-guidance study. As a textbook, it can be used for a one-semester or one-quarter course. The following are some guidelines.

- ❑ Parts one to three are strongly recommended.
- ❑ Part four is recommended if the course needs to move beyond cryptography and enter the domain of network security. A course in networking is a prerequisite for Part four.

Online Learning Center

The McGraw-Hill Online Learning Center contains much additional material related to *Cryptography and Network Security*. Readers can access the site at www.mhhe.com/forouzan. Professors and students can access lecture materials, such as Power Point slides. The solutions to odd-numbered problems are provided to students, and professors can use a password to access the complete set of solutions. Additionally, McGraw-Hill makes it easy to create a website for the course with an exclusive McGraw-Hill product called PageOut. It requires no prior knowledge of HTML, no long hours, and no design skills on your part. Instead, PageOut offers a series of templates. Simply fill them with your course information and click on one of 16 designs. The process takes under an hour and leaves you with a professionally designed website. Although PageOut offers "instant" development, the finished website provides powerful features. An interactive course syllabus allows you to post content to coincide with your lectures, so when students visit your PageOut website, your syllabus will direct them to components of Forouzan's Online Learning Center, or specific material of your own.

Acknowledgments

It is obvious that the development of a book of this scope needs the support of many people.

Peer Review

The most important contribution to the development of a book such as this comes from peer reviews. I cannot express my gratitude in words to the many reviewers who spent numerous hours reading the manuscript and providing me with helpful comments and ideas. I would especially like to acknowledge the contributions of the following reviewers:

Kaufman, Robert, *University of Texas, San Antonio*
Kesidis, George, *Penn State*
Stephens, Brooke, *U. of Maryland, Baltimore County*
Koc, Cetin, *Oregon State University*
Uminowicz, Bill, *Westwood College*
Wang, Xunhua, *James Madison University*
Kak, Subhash, *Louisiana State U.*
Dunigan, Tom, *U. of Tennessee, Knoxville*

McGraw-Hill Staff

Special thanks go to the staff of McGraw-Hill. Alan Apt, publisher, proved how a proficient publisher can make the impossible possible. Melinda Bilecki, the developmental editor, gave me help whenever I needed it. Sheila Frank, project manager, guided me through the production process with enormous enthusiasm. I also thank David Hash in design, Kara Kudronowicz in production, and Wendy Nelson, the copy editor.

Behrouz A. Forouzan