大学计算机教育国外著名教材系列（影印版）

PEARSON
Prentice Hall

CLASSICAL AND CONTEMPORARY CRYPTOLOGY

经典密码学与现代密码学

hard J. Spillman 著

清华大学出版社

大学计算机教育国外著名教材系列(影印版)

Classical and Contemporary Cryptology

经典密码学与现代密码学

Richard J. Spillman

Pacific Lutheran University, Tacoma, WA

清 华 大 学 出 版 社

北 京

图书在版编目(CIP)数据

经典密码学与现代密码学 = Classical and Contemporary Cryptology/(美)斯皮尔曼(Spillman, R. J.)著．—影印本．—北京：清华大学出版社，2005.7
(大学计算机教育国外著名教材系列)
ISBN 7-302-11156-1

Ⅰ．经…　Ⅱ．斯…　Ⅲ．密码—理论—高等学校—教材—英文　Ⅳ．TN918.1

中国版本图书馆 CIP 数据核字(2005)第 058945 号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦
http://www.tup.com.cn　　**邮　　编**：100084
社 总 机：010-62770175　　**客户服务**：010-62776969
印 刷 者：北京市清华园胶印厂
装 订 者：三河市新茂装订有限公司
发 行 者：新华书店总店北京发行所
开　　本：148×210　**印张**：9.375
版　　次：2005 年 7 月第 1 版　2005 年 7 月第1 次印刷
书　　号：ISBN 7-302-11156-1/TP・7372
印　　数：1～3000
定　　价：23.00 元

出版说明

进入21世纪，世界各国的经济、科技以及综合国力的竞争将更加激烈。竞争的中心无疑是对人才的竞争。谁拥有大量高素质的人才，谁就能在竞争中取得优势。高等教育，作为培养高素质人才的事业，必然受到高度重视。目前我国高等教育的教材更新较慢，为了加快教材的更新频率，教育部正在大力促进我国高校采用国外原版教材。

清华大学出版社从1996年开始，与国外著名出版公司合作，影印出版了“大学计算机教育丛书(影印版)”等一系列引进图书，受到国内读者的欢迎和支持。跨入21世纪，我们本着为我国高等教育教材建设服务的初衷，在已有的基础上，进一步扩大选题内容，改变图书开本尺寸，一如既往地请有关专家挑选适用于我国高等本科及研究生计算机教育的国外经典教材或著名教材，组成本套“大学计算机教育国外著名教材系列(影印版)”，以飨读者。深切期盼读者及时将使用本系列教材的效果和意见反馈给我们。更希望国内专家、教授积极向我们推荐国外计算机教育的优秀教材，以利我们把“大学计算机教育国外著名教材系列(影印版)”做得更好，更适合高校师生的需要。

清华大学出版社

Preface

The goal of this book is to introduce you to the fascinating world of cryptography. It is a multifaceted world—for some, it is a world of spies and secrets. For others, it is a world of mathematics and computers. Anyway you look at it, cryptography has an air of mystery and adventure. It also transcends traditional academic disciplines. It is not just a computer-science topic—the study of cryptography involves history, political science, engineering, languages, military science, ethics, mathematics, and technology. No single text could cover cryptography from all these perspectives, so the true student of cryptography must be prepared to develop a broad educational background. This book will only serve as the starting point for a long and satisfying search for knowledge and understanding of this very complicated, yet rewarding, topic.

Two overall principles guided the writing of this book. The first is that cryptography did not begin with the invention of the computer. While contemporary ciphers are all computer based, they owe a lot to the early work of the developers of classical ciphers. These developers had to work by hand using paper and pencil to discover weaknesses in the classical ciphers. Without the aid of a computer or even a calculator, they had to train their minds to recognize patterns and to organize data. Hence, to learn how to "think" like a cryptographer, you need to understand and appreciate the cleverness and patience that underlie the classical systems.

The second guiding principle is that a course in cryptography is not (and should not be) a programming course. While it may be helpful for students to write one or two programs that implement a cipher or an analysis tool, the time it would take learning how to write and debug code for all the important ciphers and tools would significantly reduce the time available to learn the real substance of cryptology. The task of writing cipher programs should be part of an algorithms or programming course. Hence, this book comes with a software package, Cryptographic Analysis Program (CAP), that provides access to both classical and contemporary ciphers. It also contains a set of tools for the analysis of those ciphers. The combination of the text and the software will give you real hands-on experience.

Beginning students, hobbyists, and advanced students should find something worthwhile in this text and its accompanying software program, CAP. Part One covers classical issues in cryptography and is a good place for those new to the field to begin their study. More advanced students may want to quickly scan this part for information on running CAP and perhaps spend more time on those classical ciphers or analysis techniques that are unfamiliar. Part Two covers contemporary ciphers including stream, block, and public key systems. This is the section that the more advanced students will find most useful. Part Three considers the future of cryptography and provides a short introduction to quantum systems. The world of quantum computing is so strange that it challenges our view of how the universe operates. This section is really for those who can abandon all common sense, be they beginning or advanced students.

There is a Web page for this book, which can be found at http://www.plu.edu/~spillmrj. (Follow the CAP pointers.) It contains a set of PowerPoint® files which are designed for lectures. Instructors also have access to answers to the problems in the book as well as additional problems and test questions.

The single most unique feature of this text is the accompanying software package, CAP. Together, CAP and the text are designed to create a complete learning environment. As you read about a particular cipher system, CAP allows you to explore the operation of that system. As you study an analysis technique, CAP allows you to experiment with it. CAP implements 30 different ciphers following a standardized interface so that once you become familiar with the implementation of one cipher you can easily run all the ciphers. CAP also provides a wide range of analysis tools that allow you to test the resistance of most CAP ciphers to cryptanalysis and to discover weaknesses that may be exploited in those ciphers. The usefulness of CAP is reflected in the problems at the end of each chapter. The problem sets are unique and, at times, challenging because they rely on your access to CAP. Above all, CAP is fun. It comes with a game feature so you can continue to test your cryptographic skills after you complete the text material. The CAP website (previously referenced) will contain additional challenges and post readers' high scores (if you will send in your game scores).

I hope you find the study of cryptography as interesting and rewarding as I found the writing of this book.

RICHARD J. SPILLMAN
Pacific Lutheran University,
Tacoma, WA

大学计算机教育国外著名教材系列（影印版） 最新出版图书

- Computer Networks, Fourth Edition
  计算机网络(第 4 版)
  作者：Andrew S. Tanenbaum
  ISBN 7-302-07815-7
  定价：69.00 元

- Java Structures: Data Structures in Java for the Principled Programmer, Second Edition
  数据结构 Java 语言描述(第 2 版)
  作者：Duane A. Bailey
  ISBN 7-302-07415-1
  定价：46.00 元

- Discrete Mathematics, Fifth Edition
  离散数学(第 5 版)
  作者：K.A.Ross
  ISBN 7-302-07463-1
  定价：56.00 元

- Modern Systems Analysis & Design, Third Edition
  现代系统分析与设计（第 3 版）
  作者：Hoffer, George, Valacich
  ISBN 7-302-07794-0
  定价：69.00 元

- Data Structures and Algorithms
  数据结构与算法
  作者：Aho, Hopcroft, Ullman
  ISBN 7-302-07564-6
  定价：40.00 元

- Data Mining: A Tutorial Based Primer
  数据挖掘基础教程
  作者：Roiger, Geatz
  ISBN 7-302-07667-7
  定价：43.00 元

- Computer Science: An Overview, 7th Edition
  计算机科学导论（第 7 版）
  作者：Brookshear
  ISBN 7-302-07792-4
  定价：54.00 元

- Digital Image Processing
  数字图像处理
  作者：K.R. Castleman
  ISBN 7-302-07464-X
  定价：59.00 元

- Network Security Essentials: Applications and Standards, Second Edition
  网络安全基础教程：应用与标准（第 2 版）
  作者：William Stallings
  ISBN 7-302-07793-2
  定价：39.00 元

- Wireless Communications and Networks
  无线通信与网络
  作者：William Stallings
  ISBN 7-302-07413-5
  定价：52.00 元

- TCP/IP Protocol Suite, Second Edition
  TCP/IP 协议簇（第 2 版）
  作者：Behrouz A. Forouzan,
  Sophia Chung Fegan
  ISBN：7-302-07835-1
  定价：75.00

- Computer Vision: A Modern Approach
  计算机视觉：一种现代的方法
  作者：Forsyth, Ponce
  ISBN 7-302-07795-9
  定价：65.00 元

- Operating Systems Principles
  操作系统原理
  作者：Bic, Shaw
  ISBN 7-302-07724-x
  定价：50.00 元

- Discrete Mathematics with Combinatorics
  离散数学暨组合数学
  作者：James A. Anderson
  ISBN 7-302-07789-4
  定价：79.00 元

- The 80X86 IBM PC and Compatible Computers: Assembly Language, Design, and Interfacing Volumes I & II, Fourth Edition
  80X80 IBM PC 及兼容计算机：汇编语言、设计与接口技术，卷 I 和 II（第 4 版）
  作者：Muhammad Ali Mazidi
  Janice Gillispie Mazidi
  ISBN：7-302-07885-8
  定价：89.00 元

- Computer Graphics: C version, Second Edition
  计算机图形学（C 语言版）（第 2 版）
  作者：Donald Hearn, M. Pauline Baker
  ISBN：7-302-8084-4
  定价：69.00 元

- Software Engineering: A Practitioner's Approach, Fifth Edition
  软件工程：实践者之路（第 5 版）
  作者：Roger S. Pressman
  ISBN：7-302-04139-3
  定价：79.00 元

- Java: An Introduction to Computer Science and Programming, Third Edition
  Java 语言：计算机科学与程序设计（第 3 版）
  作者：Walter Savitch
  ISBN：7-302-08303-7
  定价：86.00 元（含光盘）

- Itanium Architecture for Programmers: Understanding 64-Bit Processors and EPIC Principles
  安腾体系结构：理解 64 位处理器和 EPIC 原理
  作者：James S. Evans, Gregory L. Trimper
  ISBN：7-302-8486-6
  定价：49.00 元

- Practical Object-Oriented Design with UML, 2e
  面向对象设计 UML 实践（第 2 版）
  作者：Mark Priestley
  ISBN：7-302-08784-9
  定价：39.00 元

- Metrics and Models in Software Quality Engineering, Second Edition
  软件质量工程的度量与模型（第 2 版）
  作者：Stephen H. Kan
  ISBN：7-302-08839-X
  定价：49.00 元

- Computational Complexity
  计算复杂性
  作者：Christos H. Papadimitriou
  ISBN：7-302-08955-8
  定价：59.00 元

- Process Quality Assurance for UML-Based Projects
  UML 项目管理的过程质量保证
  作者：Bhuvan Unhelkar
  ISBN：7-302-09215-X
  定价：49.00 元（含光盘）

- Java Network Programming and Distributed Computing
  Java 网络程序设计与分布式计算
  作者：David Reilly, Michael Reilly
  ISBN：7-302-09767-4
  定价：44.80 元

- Data Structures and Problem Solving Using C++ (2nd Edition)
  数据结构与问题求解（C++版）
  作者：Mark Allen Weiss
  ISBN：7-302-09765-8
  定价：84.00 元

- Introduction to Programming Using Java: An Object-Oriented Approach Second Edition
  Java 面向对象程序设计（第 2 版）
  作者：David Arnow, Scott Dexter,
  Gerald Weiss
  ISBN：7-302-09766-6
  定价：68.00 元

- Cryptography and Network Security
  密码学与网络安全
  作者：Atul Kahate
  ISBN 7-302-09967-7
  定价：48.00 元

- Object Models: Strategies, Patterns, and Applications, Second Edition
  对象模型：策略、模式与应用（第 2 版）
  作者： Peter Coad
  ISBN 7-302-09965-0
  定价：62.00 元

- Semiotics in Information Systems Engineering
  信息系统工程中的符号学
  作者：Kecheng Liu
  ISBN 7-302-09962-6
  定价：23.00 元

- Grid Computing
  网格计算
  作者：Joshy Joseph, Craig Fellenstein
  ISBN 7-302-10025-X
  定价：39.00 元

- Introduction to Logic Design
  逻辑设计基础
  作者：Alan B. Marcovitz
  ISBN 7-302-05717-6
  定价：50.00 元

- Embedded Systems: Architecture, Programming and Design
  嵌入式系统体系结构、编程与设计
  作者：Raj Kamal
  ISBN 7-302-10297-X
  定价：59.00 元

- C++: The Complete Reference, Fourth Edition
  C++完全参考手册（第 4 版）
  作者：Herbert Schildt
  ISBN 7-302-10157-4
  定价：96.00 元

- The Art of Assembly Language
  汇编语言艺术
  作者：Randall Hyde
  ISBN 7-302-10435-2
  定价：88.00 元

- Parallel Programming: in C with MPI and OpenMP
  并行程序设计: C、MPI 与 OpenMP
  作者：Michael J. Qiunn
  ISBN 7-302-11157-X

- Software Project Management in Practice
  软件项目管理实践
  作者：Pankaj Jalote
  ISBN 7-302-10682-7
  定价：35.00 元

- Fundamentals of Algorithmics
  算法基础
  作者：Gilles Brassard, Paul Bratley
  ISBN 7-302-11155-3
  定价：35.00 元

- Classic Data Structures in Java
  经典数据结构（Java 语言版）
  作者：Timothy Budd
  ISBN 7-302-11154-5
  定价：43.00 元

- Business Data Communications, 5E
  数据通信——原理、技术与应用（第 5 版）
  作者：William Stallings
  ISBN 7-302-11152-9
  定价：38.00 元

- Classic and Contemporary Cryptology
  经典密码学与现代密码学
  作者：Richard J. Spillman
  ISBN 7-302-11156-1
  定价：23.00 元

■ Object-Oriented Programming in C++, 2E C++面向对象程序设计（第 2 版） 作者：Richard Johnsonbaugh, Martin Kalin	■ Assembly Language for Intel-Based Computers, 4E Intel 汇编语言程序设计（第 4 版） 作者：Kip R. Irvine
■ Introduction to wireless Technology 无线技术导论 作者：Gary S. Rogers, John S. Edwards	■ The C++ Standard Library : A Tutorial and Reference C++标准库教程 作者：Nicolai M. Josuttis
■ Neural Networks: A Classroom Approach 神经网络教程 作者：Satish Kumar	■

其他影印版图书

■ C++ Network Programming, Volume 1: Mastering Complexity with ACE and Patterns C++网络编程，卷 1：运用 ACE 和模式消除复杂性 ISBN 7-302-07644-8 作者：Douglas C. Schmidt Stephen D. Huston 定价：29.00 元	■ C++ Network Programming, Volume 2: Systematic Reuse with ACE and Frameworks C++网络编程,卷 2：基于 ACE 和框架的系统化复用 ISBN 7-302-07964-1 作者：Douglas C. Schmidt Stephen D. Huston 定价：34.00 元
■ Computing Concepts 新概念计算机英语 ISBN 7-302-07357-0 作者：Stephen Haag Maeve Cummings Alan I Rea, Jr 定价：52.00 元	■

Contents

Chapter 1 Introduction to Cryptology 1

1.0 Introduction 1
1.1 Cryptography 2
1.2 Important Terms 3
1.3 Cipher Evaluation 4
1.4 Cryptanalysis 5
1.5 A Brief History of Codes and Ciphers 6
1.6 Classical and Contemporary Ciphers 8
1.7 Introduction to CAP 9
1.8 Summary 11
1.9 Important Terms 12
Resources 12
Problems 12

Part 1 Classical Cryptology 15

Chapter 2 Classical Monoalphabetic Ciphers 16

2.0 Introduction 16
2.1 Keyword Cipher 16
2.1.1 Cryptanalysis of Keyword Ciphers *18*
2.1.2 Frequency Information *19*
2.1.3 Using CAP to Break a Keyword Cipher *22*
2.1.3.1 Frequency Analysis in CAP 22
2.1.3.2 Letter Identification in CAP 22
2.1.3.3 Word Identification in CAP 23
2.1.3.4 Keyword Worksheet 24
2.2 Affine Cipher 24
2.2.1 Cryptanalysis of the Affine Cipher *27*
2.3 Multiliteral Cipher 29
2.3.1 Cryptanalysis of a Multiliteral Cipher *29*
2.4 Monoalphabetic Ciphers—A Short Historical View 30
2.5 Summary 32

2.6 Important Terms 33
Resources 33
Problems 33

Chapter 3 Classical Polyalphabetic Ciphers 36

3.0 Introduction 36
3.1 Vigenere Cipher 37
3.1.1 Cryptanalysis of the Vigenere Cipher 39
3.1.2 Cryptanalysis of the Vigenere Cipher with CAP 43
3.2 Autokey Cipher 46
3.2.1 Cryptanalysis of the Autokey Cipher 47
3.4 Nihilist Cipher 50
3.5 Cylinder Cipher 51
3.5.1 Cryptanalysis of the Bazeries Cylinder 53
3.6 Rotor ciphers 56
3.6.1 Breaking Enigma 59
3.6.2 Using CAP to Break a Rotor Cipher 60
3.7 The Rise of the Machines—A Brief History 60
3.8 Summary 63
3.9 Important Terms 64
Resources 65
Problems 65

Chapter 4 Classical Polygraphic Ciphers 67

4.0 Introduction 67
4.1 Playfair Cipher 68
4.1.1 Cryptanalysis of Playfair 70
4.1.2 Cryptanalysis of Playfair with CAP 74
4.2 The Hill Cipher 75
4.2.1 Hill Cipher in CAP 77
4.2.2 Cryptanalysis of the Hill Cipher 78
4.3 Beale Ciphers—A Brief Historical Interlude 80
4.4 Summary 82
4.5 Important terms 83
Resources 83
Problems 83

Chapter 5 Classical Transposition Ciphers 85

5.0 Introduction 85
5.2 Permutation Cipher 87
5.2.1 Cryptanalysis of a Permutation Cipher 87

5.3 Column Permutation Cipher 89

5.3.1 Cryptanalysis of Column Transpositions 90

5.3.1.1 Possible Column Sizes 91

5.3.1.2 Determining the Correct Rectangle 91

5.3.1.3 Restoring the Column Order 92

5.3.2 Using CAP to Break a Column Transposition 94

5.4 Double-Transposition Cipher 96

5.4.1 Cryptanalysis of the Double-Transposition Cipher 96

5.4.2 Using CAP to Break a Double Transposition 97

5.5 A Brief History of Transpositions 98

5.6 Summary 101

5.7 Important Terms 101

Resources 102

Problems 102

Part 2 Contemporary Ciphers 103

Chapter 6 Stream Ciphers 104

6.0 Introduction 104

6.0.1 Computer Characteristics 105

6.0.2 XOR Function 106

6.1 Stream Cipher 107

6.1.1 Linear Feedback Shift Registers 107

6.1.2 LFSR Period Analysis 109

6.1.3 Random-Bit Tests 110

6.1.4 Implementing a Stream Cipher in CAP 112

6.2 Breaking a Stream Cipher 113

6.2.1 Insertion Attack on a Stream Cipher 113

6.2.2 Probable-Word Attack One: Matching Bit Strings 114

6.2.3 Probable-Word Attack Two: Word Match 116

6.2.4 Using CAP to Break a Stream Cipher 117

6.3 Other Stream-Cipher Implementations 117

6.3.1 RC4 119

6.3.2 Evaluation of RC4 121

6.3.3 A5 121

6.3.4 Cellular Automata 122

6.3.5 Other Ways to Generate Random Numbers 126

6.4 An Unbreakable Cipher 127

6.5 A Practical Application 127

6.6 An Historical Perspective on Stream Ciphers 128

6.7 Summary 129

6.8 Important Terms 130

Resources 130

Problems 131

Chapter 7 Block Ciphers 132

7.0 Introduction 132
7.1 Block-Cipher Modes 133
7.1.1 Contemporary Block-Cipher Modes 134
7.1.2 Padding 136
7.2 Product Ciphers 137
7.2.1 Evaluation of a Block Cipher 137
7.3 Data Encryption Standard 138
7.3.1 DES Key 138
7.3.2 DES Stages 139
7.3.3 Alternative Implementations of DES 145
7.3.4 DES in CAP 145
7.3.5 Cryptanalysis of DES 147
7.3.5.1 Differential Cryptanalysis 148
7.3.5.2 Linear Cryptanalysis 152
7.3.5.3 Meet-in-the-Middle Attack 155
7.3.5.4 Side-Channel Analysis 157
7.3.5.5 Bob, Alice, and Eve 157
7.4 IDEA 158
7.5 Advanced Encryption Standard 159
7.5.1 Rijndael Structure 160
7.5.2 Key Schedule 165
7.5.3 AES Operation 166
7.5.4 AES Security 167
7.5.5 Hardware Implementation 168
7.5.6 Other Finalists 170
7.5.6.1 RC6 171
7.5.6.2 Twofish 172
7.5.6.3 Evaluation and Performance 172
7.6 Using Block Ciphers 175
7.6.1 A Quick Overview of Network Connections 175
7.6.2 IPSec Connections 177
7.7 Block Ciphers' Short History 177
7.8 Summary 179
7.9 Important Terms 180
Resources 180
Problems 181

Chapter 8 Public Key Ciphers 183

8.0 Introduction 183
8.1 The Public Key Process 184
8.2 RSA 186
8.3 Number Theory—a very short introduction 188
8.3.1 Modular Inverses 189

8.3.2 Prime Numbers *190*
8.3.3 Fast Exponentiation *195*
8.4 RSA in CAP **196**
8.5 Analysis of RSA **197**
8.5.1 Large Integer Factoring *197*
8.5.2 Other RSA Attacks *200*
8.5.2.1 Side-Channel Attacks **201**
8.5.2.2 Improper Use of RSA Attacks **202**
8.6 ElGamal Public Key System **203**
8.6.1 Generator Numbers *205*
8.6.2 Using CAP to Implement ElGamal *205*
8.6.3 Observations *207*
8.7 Knapsack Cipher **207**
8.7.1 Breaking the Knapsack Cipher *209*
8.7.2 The Knapsack Cipher in CAP *211*
8.8 Elliptic Curve Ciphers (ECC) **212**
8.8.1 Observations *215*
8.9 Public Key Applications **216**
8.10 Historical Developments in Public Key Ciphers **216**
8.11 Summary **217**
8.12 Important Terms **218**
Resources **218**
Problems **218**

Chapter 9 Key Management, Digital Signatures, Hash Functions, and Certificates **221**

9.0 Introduction **221**
9.1 Key Exchange **222**
9.1.1 Internet Key Exchange Process *225*
9.1.2 Group Keys *226*
9.1.2 Broadcast Encryption *230*
9.2 Authenticity **232**
9.3 Digital Signatures **234**
9.3.1 Hash Functions *235*
9.3.1.1 MD5 **237**
9.3.1.2 Secure Hash Algorithm (SHA) **239**
9.3.1.3 Comparison of MD5 and SHA-1 **241**
9.3.1.4 Block-Cipher-Based Hash Functions **241**
9.3.1.5 Attacks on Hash Functions **242**
9.3.1.1 Hash Functions in CAP **244**
9.3.2 Blind Signatures *246*
9.3.3 Digital Signature Standard (DSS) *249*
9.4 Public Key Infrastructure and Certificates **252**
9.4.1 Establishing a Certificate *253*
9.4.2 Certificate Contents *254*

9.4.3 Using a Certificate 254
9.4.4 Revocation of a Certificate 255
9.5 Applications 256
9.5.1 Smart Cards 256
9.5.2 Secure Socket Layer 257
9.6 Historical Perspective 260
9.7 Summary 261
9.8 Important Terms 261
Resources 262
Problems 262

Part 3 The Future of Cryptology 267

Chapter 10 Quantum Cryptography 268

10.0 Introduction 268
10.1 Quantum Systems—A Brief Introduction 268
10.1.1 Qubits 269
10.1.2 The Weird World of Quantum Physics 269
10.2 Quantum Factoring 272
10.3 Quantum Key Management 274
10.3.1 Eavesdropping 275
10.3.2 Privacy Amplification 278
10.3.3 Experimental Verification 280
10.4 Summary 280
10.5 Important Terms 281
Resources 281
Problems 281

Index 283

Chapter 1

Introduction to Cryptology

1.0 INTRODUCTION

We live in an exciting, fast-paced world and nothing is changing faster than the way we deal with information. Using the Internet, we can access and use information in ways that we never even dreamed of just a few years ago. Rather than going to the bank and standing in line waiting for a teller, we can pay bills, write checks, and shift money between accounts from home, 24 hours a day, 7 days a week. We can apply for and receive approval for loans without ever leaving home. We can buy books, food, gifts, and just about anything else over the Internet. Instead of running a garage sale in our front yard on a weekend, we can sell anything at anytime over the Net. We can buy and sell stock. We can post information for others to read and find information on just about any subject. With the advent of wireless technology, we can do all this and more from almost any location on earth using a cellular phone.

Sure, these are exciting times, but they also have a down side. The same technology that makes life so much easier has the potential to destroy our lives when used by criminals. For example, identity theft is one of the fastest growing crimes in the United States today. It thrives because the legal penalties have not caught up with the effects of the crime, besides the fact that it is easy to do. This is because most of the information "out there" about individuals is not protected. To enjoy the benefits while avoiding the pitfalls of new technology, we must have some method of protecting our identity and our personal information. How this can be done is precisely the subject matter of this book. It is about "secret writing," which has been around for centuries, but has now become a vital force for protecting and nurturing the growth of information technology. The field is called cryptography.

Cryptography is the study of codes and ciphers. David Kahn, in what has to be called the "bible of cryptography," defines it as follows: "Cryptology is protection. It is to that extension of modern man—communications—what the carapace is to the turtle, ink to the squid, camouflage to the chameleon." It is centuries old yet it remains fresh, new, and exciting. It is a field that is constantly changing and discovering new challenges. As a result, this is more than