Modern Cryptography

Chuck Easttom

Modern Cryptography

Applied Mathematics for Encryption and Information Security

Second Edition

Springer

Chuck Easttom
Georgetown University and
Vanderbilt University
Plano, USA

ISBN 978-3-031-12303-0 ISBN 978-3-031-12304-7 (eBook)
https://doi.org/10.1007/978-3-031-12304-7

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

I dedicate this book to my wife Teresa who is always long suffering with my work and research, and who has always been amazingly supportive. I could not have done any of this without her support. A quote from one of my favorite movies describes how I feel about her and her support "What truly is logic? Who decides reason? My quest has taken me to the physical, the metaphysical, the delusional, and back. I have made the most important discovery of my career—the most important discovery of my life. It is only in the mysterious equations of love that any logic or reasons can be found. I am only here tonight because of you. You are the only reason I am. You are all my reasons.

Introduction

The book *Modern Cryptography: Applied Mathematics for Encryption and Information Security* was first published with McGraw Hill, then later revised and published with Springer. This is the second edition with Springer. What has changed you might wonder? Some chapters have had only very minor changes, for example, Chap. 12 has had only a few updates. Other chapters have had not only revisions but also new algorithms added. Chapter 10 now provides details on the YAK cipher. The mathematics of Chap. 5 has been expanded. Chapters 20 and 21 are entirely new and cover quantum-resistant cryptography algorithms. Along with that addition, Chap. 19 that provides a general overview of quantum computing has also been expanded. Chapter 13 now covers additional digital certificate types. Chapter 8 has also been substantially expanded. Most importantly, all chapters have been reviewed to make concepts clearer for the reader.

As with the previous editions, this book is not meant for the mathematician or cryptographer to deep dive into the topic. It is meant for the programmer, cyber security professional, network administrator, or others who need to have a deeper understanding of cryptography. For that reason, mathematical proofs are not included in this book. Sufficient mathematics to generally understand the concepts is provided, but no more than is absolutely needed.

Beginning with the first version of this book in 2015, the intent has been the same: to fill a gap in cryptography literature. There are some excellent books written for the mathematically sophisticated. These books provide so much rich detail on the algorithms and the "why" behind the math. However, these are largely inaccessible to those with less rigorous mathematical backgrounds. Then there are cybersecurity books which provide very little detail on cryptography, books that prepare one for cybersecurity certifications such as CompTIA Security+ and ISC2 CISSP. However, those books provide only the most cursory review of cryptography. This book is meant to be a bridge between those two worlds. When you finish this book, you will know far more than you do now, even assuming you hold several cybersecurity certifications. However, there is much more to learn. There are a few specific books I recommend after you have completed this one. Any of the following will take you deeper into the math behind the cryptography:

Understanding Cryptography: A Textbook for Students and Practitioners by Christof Paar and Jan Pelzl.

An Introduction to Mathematical Cryptography (Undergraduate Texts in Mathematics) Second Edition, 2014, by Hoffstien, Pipher, and Silverman.

Introduction to Modern Cryptography (Chapman & Hall/CRC Cryptography and Network Security Series) Second Edition by Katz and Lindell.

Now those books will skip over things like s-box design, quantum-resistant cryptography, and a few other issues. But they will dive much deeper into current symmetric and asymmetric algorithms as well as cryptographic hashes. So, if you complete this current book, and wish to dive deeper, I recommend one or more of these.

Contents

About the Author

Chuck Easttom is author of 36 books, including several on computer security, forensics, and cryptography. His books are used at over 60 universities. He has also authored scientific papers (more than 70 so far) on digital forensics, cyber warfare, cryptography, and applied mathematics. He is an inventor with 25 computer science patents. He holds a Doctor of Science in Cyber Security (dissertation topic: a study of lattice-based cryptographic algorithms for post quantum computing) and three master's degrees (one in applied computer science, one in education, and one in systems engineering). Chuck also has a PhD in technology, focusing on nanotechnology (dissertation title: "The Effects of Complexity on Carbon Nanotube Failures") and a PhD in computer science (dissertation title: "A Systematic Framework for Network Forensics Using Graph Theory"). Chuck is a senior member of the IEEE and a senior member of the ACM as well as a member of IACR (International Association of Cryptological Research) and INCOSE (International Council on Systems Engineering). He is also a distinguished speaker of the ACM (Association of Computing Machinery) and a distinguished visitor of the IEEE Computer Society. Chuck currently is an adjunct lecturer at Georgetown University and Vanderbilt University.

Abbreviations

AES	Advanced Encryption Standard
CA	Certificate Authority
CBC	Cipher Block Chaining
CCM	Counter with CBC-MAC
CFB	Cipher Feedback
CMAC	Cipher-based Message Authentication Code
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
DE	Full Disk Encryption
DES	Data Encryption Standard
DRBG	Deterministic Random Bit Generator.
DSA	Digital Signature Algorithm
EAP	Extensible Authentication Protocol
ECB	Electronic Code Book
FIPS	Federal Information Processing Standard
GCM	Galois/Counter Mode
GGH	Glodreich, Goldwasser, and Halevi
GHASH	Galois HASH
HMAC	keyed-Hash Message Authentication Code
IDEA	International Data Encryption Algorithm
IV	Initialization Vector
LLL	Lenstra–Lenstra–Lovász
LSB	Least Significant Bit
MAC	Message Authentication Code
MD	Message Digest
MD5	Message Digest 5
NIST	National Institute of Standards and Technology
NTRU	N-th degree Truncated polynomial Ring Units
OAEP	Optimal asymmetric encryption padding
OFB	Output Feedback
OTP	One-Time Pad

PGP	Pretty Good Privacy
PKC	Public Key Cryptography
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PRG	Pseudo-Random Generator
PRNG	Pseudo-Random Number Generator.
RC4	Rivest Cipher 4
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
SRTP	Secure Real-time Transport Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access II
WPA3	Wi-Fi Protected Access III
XOR	Exclusive OR