# CRYPTOGRAPHY: A NEW DIMENSION IN COMPUTER DATA SECURITY

# CRYPTOGRAPHY: A NEW DIMENSION IN COMPUTER DATA SECURITY

## A Guide for the Design and Implementation of Secure Systems

**CARL H. MEYER**
**STEPHEN M. MATYAS**

*Cryptography Competency Center*
*IBM Corporation, Kingston, New York*


A Wiley-Interscience Publication

JOHN WILEY & SONS

New York • Chichester • Brisbane • Toronto • Singapore

*TO*

*MARLIES V. AND SANDRA L.*



***Library of Congress Cataloging in Publication Data:***

Meyer, Carl, Ph.D.
Cryptography: A New Dimension in Computer Data Security—A Guide for the Design and Implementation of Secure Systems

Bibliography: p.
Includes index.
1. Cryptography–Handbooks, manuals, etc.
I. Matyas, Stephen. II. Title.

Z103.M55 001.54'36 82-2831
ISBN 0-471-04892-5 AACR2

Printed in the United States of America

10 9 8

# Preface

This book deals with today's cryptography. Unlike past classical schemes used for the concealment of diplomatic and military secrets of monarchs and government officials at all levels, today's cryptography must provide cost-effective, secure approaches for protecting the vast amounts of digital data gathered and communicated with electronic data processing (EDP) systems. Consequently, the material in this book is intended for the increasing number of both technical and nontechnical people concerned with computer data security and privacy.

Advances in cryptography appeared with unprecedented frequency in the 1970s as strong encryption-based protocols and new cryptographic applications emerged. On January 15, 1977, the National Bureau of Standards adopted an encryption algorithm as a Federal standard—The Data Encryption Standard (DES)—marking a milestone in cryptographic research and development. Subsequently, in December 1980, the American National Standards Institute adopted the same algorithm for commercial use in the United States. Another milestone was set by the proposal of a new concept called Public Key Cryptography, an approach still being developed and no standard algorithm yet agreed upon.

Many readers may find themselves unacquainted with cryptography, but confronted with problems of cryptographic design or the implementation of cryptographic protection at some level within a communications network or EDP system. To meet the approaching challenges to the technical world, full coverage of these aspects of cryptography is provided.

It is noteworthy that cryptography is the only known practical means for protecting information transmitted through a large communications network, be it telephone line, microwave, or satellite. A detailed discussion of how cryptography can be used to achieve communications security (COMSEC) is provided. Moreover, various attack scenarios are discussed so that the engineer and systems designer can understand and appreciate the problems and difficulties involved in providing a cryptographically secure COMSEC solution.

Cryptography can be used to achieve file security. A protocol is developed for the encryption of data stored on removable media. Enhanced authentication protocols, including personal verification, message authentication, and digital signatures, can also be achieved through cryptographic techniques. These subjects are of particular interest to those concerned with electronic funds transfer and credit card applications within the banking and finance industry, or any other area where the originator, timeliness, contents, and intended receiver of a message must be verified.

The banking and finance industry has been the leader in promoting the use of cryptography for protecting assets transferred via messages sent

through large networks of computers and terminals. To address this subject properly, we have reprinted a significant portion of the *PIN Manual,* prepared by the staff of MasterCard International, Inc., and previously available only through MasterCard's Security Department. This material is augmented by our detailed analysis of EFT systems security. A set of EFT security requirements is presented. It should be evaluated by those designing or planning EFT applications. Various implementations are discussed, including design trade-offs and techniques for achieving superior security in future systems.

Any key-controlled cryptographic algorithm, such as the DES, requires a protocol for the management of its cryptographic keys. The details of a key management scheme providing support for the protection of communications between individual end users (end-to-end) and for the protection of data stored or transported on removable media are given. Procedures for the safe and secure generation, distribution, and installation of cryptographic keys are also discussed.

Shannon's treatment of cryptography (in his landmark paper on Secrecy Systems) has been used as a starting point for the coverage of the subjects of unicity distance and work factor. Both statistical and information theory approaches are given, providing the reader with a more thorough understanding of the approaches for achieving cryptographic strength.

This book is intended for those people interested in understanding the role of cryptography in achieving high levels of computer data security. Perhaps of even greater importance is the fact that cryptography is identified as a complete solution to some data security problems. For others, it provides only a partial solution, but this is equally important to an understanding of what problems can and cannot be solved using cryptography. Engineers, designers, planners, managers, academicians, and students can benefit from one or more of the practical and theoretical subjects treated in the text.

The state-of-the-art material for this book was derived from our involvement in research and development efforts in the field of cryptography, and more generally from our work in the field of data security.

The views expressed in this book are those of the authors and not necessarily those of the IBM Corporation.

Starting with the third printing, the function for generating redundant information for a message integrity check has been changed from modulo two addition, which was found to have certain undesirable properties, to modulo $2^{64}$ addition. The change affects pages 69, 79, 82-83, 101-105, 257-259, 361, 385, 399, 400-401, 411-415.

Carl H. Meyer
Stephen M. Matyas

*Kingston, New York*
*July, 1982*

# Acknowledgments

We are indebted to David B. Mayer, whose early review of Chapters 1 through 3 was instrumental in setting the presentation format to enable this work to appeal to a broader audience.

David Kahn reviewed Chapter 1 and provided many valuable criticisms that redirected the chapter's content and approach.

Stephen M. Lipton supplied the section Technical Implications of Privacy Legislation in Chapter 1. He also assisted and shared his technical expertise in the preparation of portions of Chapter 9 dealing with the legal significance of digital signatures.

Miles Smid reviewed the material dealing with message authentication and digital signatures. Several weaknesses and one subtle attack against one of the authentication procedures uncovered by Smid are documented in Chapter 9. Both Miles Smid and Carl Campbell reviewed and criticized early versions of Chapter 11, which led to a more precise discussion of alternative cryptographic methods in electronic funds transfer systems.

Jonathan Oseas reviewed the entire manuscript and provided valuable comments, especially for Chapter 11. As our manager, he also made resources available that accelerated the book's completion.

Donald W. Davies and Dr. Wyn L. Price critically reviewed major portions of the manuscript and were responsible for pointing out the existence of semiweak keys.

We are indebted to Stanley A. Kurzban, who reviewed the entire manuscript. His many excellent comments and suggestions improved the manuscript both from a technical and editorial standpoint.

We are indebted also to Ronald K. Freeman for his careful editing skills and his continued support and assistance in the preparation of this manuscript.

We especially wish to thank Richard E. Lennon for his collaboration and suggestions with the material in Chapters 4 and 11. His tireless efforts with the composition and editing of the manuscript are deeply appreciated. Without his help, this book would have been delayed at least one year.

Many of our colleagues generously provided detailed criticism of different portions of the manuscript: Dr. Willis H. Ware reviewed a large part of the work; Robert H. Courtney reviewed Chapter 1; Professors Ronald L. Rivest and Martin E. Hellman reviewed the section on public-key algorithms; Dr. Don Coppersmith collaborated with us in developing a computer procedure to solve simple substitution ciphers and reviewed Chapter 12 and associated appendices; Charles C. Wood reviewed Chapters 1 and 4 and provided many excellent comments; Dr. Glen G. Langdon, Jr. reviewed Chapter 12; Frank S. Piedad, James B. Warner, Marvin Sendrow, and Jerry Svigals reviewed Chapter 11 and associated appendices.

Salim Akl, Stanley Benton, Professor G. R. Blakley, Frank Davis, Whitfield Diffie, William H. Ehrsam, Robert C. Elander, Ronald C. Gault, Horst Feistel, John B. Gillett, Robert R. Jueneman, Dr. Stephen T. Kent, Edwin Lester, Michael J. Martino, Dr. Christian Mueller-Schloer, Louise D. Nielsen, Paul N. Prentice, Mok-Kong Shen, Robert E. Shuck, Albert A. Smith, Jr., Dolfis G. Smith, and Howard Zeidler all offered constructive criticism and ideas that significantly improved this book.

Gracious assistance in the preparation of the manuscript was provided by many of our colleagues. O. Tom Thomas supplied the material from which Appendices C and E were derived. Laura A. Wheatherly assisted by obtaining permission from MasterCard International Inc. to reprint sections 1 through 4 of the PIN Manual. Thomas E. Deuser and John T. Minick helped in the composition of the book. Fern Franke, Frank Marquette, Sherry Collins, Jim Economos, and Susan Swiderski of AGS Typography prepared the manuscript's many excellent figures and tables.

We also owe a debt to Horst Feistel, who started the cryptographic effort at IBM with his LUCIFER algorithm and thus laid the foundation for the DES.

Finally, we wish to thank Dr. Walter L. Tuchman, under whose direction the DES algorithm was developed, and the IBM Corporation for making it possible for us to write this book.

C. M.
S. M.

# Contents

# Abbreviations

**Cipher Modes and Associated Parameters:**

| | |
|---|---|
| CBC | cipher block chaining |
| CE | compressed encoding |
| CFB | cipher feedback |
| ECB | electronic codebook (see block cipher) |
| ICV | initial chaining value |
| OCV | output chaining value |
| OFB | output feedback (see key auto-key cipher |
| X | plaintext |
| Y | ciphertext |
| Z | initializing vector (synonymous with ICV) |
| DEA | Data Encryption Algorithm (ANSI; synonymous with DES) |
| DES | Data Encryption Standard (NBS) |
| PKC | Public Key Cryptosystem |
| RSA | Rivest, Shamir, Adelman (public key) algorithm |

**Cryptographic Keys:**

| | |
|---|---|
| K | primary data-encrypting key |
| KA | authentication key |
| KC | primary communications key (synonymous with session key) |
| KF | primary file key |
| KI | interchange key |
| KMT | terminal master key |
| KN | secondary key |
| KNC | secondary (node) communication key |
| KNF | secondary node file key |
| KP | personal key |
| KPG | personal key-generating key used to generate KP from ID |
| KPN | PIN generating key used to generate PIN from ID |
| KS | session key |
| KSTR | transaction session key |
| KT | resident terminal key |
| KTR | transaction key |

| | |
|---|---|
| PK | public key in a public-key cryptosystem |
| PKb | public bank key in a PKC |
| PKc | public customer key in a PKC |
| PKu | public universal key in a PKC |
| SK | secret key in a PKC |
| SKb | secret bank key in a PKC |
| SKc | secret customer key in a PKC |
| SKu | secret universal key in a PKC |

**Cryptographic Operations:**

| | | |
|---|---|---|
| AF | authenticate forward | (host) |
| AR | authenticate reverse | (host) |
| ECPH | encipher data | (host) |
| EMK | encipher under master key | (host) |
| ENC | encipher | (terminal) |
| ENCO | encipher only | (host) |
| DCPH | decipher data | (host) |
| DEC | decipher | (terminal) |
| DECK | decipher key | (terminal) |
| DECO | decipher only | (host) |
| GKEY | generate key | (host) |
| GSK1 | generate session key 1 | (host) |
| GSK2 | generate session key 2 | (host) |
| LKD | load key direct | (terminal) |
| MGK | merge key | (host) |
| RFMK | reencipher from master key | (host) |
| RTMK | reencipher to master key | (host) |
| SMK | set master key | (host) |
| WMK | write master key | (terminal) |

**Cryptographic Macros:**

CIPHER
GENKEY
RETKEY

**System Terminology:**

| | |
|---|---|
| ATM | automated teller machine |
| BSC | binary synchronous communication |
| CC | communications controller |
| HPC | host processing center |
| KDC | key distribution center |

| | |
|---|---|
| LU | logical unit |
| PLU | primary logical unit |
| PU | physical unit |
| RH | request/response header |
| RU | request/response unit |
| SDLC | synchronous data link control |
| SLU | secondary logical unit |
| SNA | system network architecture |
| SSCP | systems services control point |

**Organizations:**

| | |
|---|---|
| ANSI | American National Standards Institute |
| CCITT | Consultative Committee on International Telephone and Telegraph |
| ISO | International Standards Organization |
| NBS | National Bureau of Standards |
| NSA | National Security Administration |

**Parameters Associated with Verification and Authentication**

| | |
|---|---|
| AP | authentication parameter |
| BID | bank identifier |
| CRV | cryptographic verification |
| DGS | digital signature |
| ID | user identifier |
| MAC | message authentication code |
| PAC | personal authentication code |
| PAN | primary account number |
| PIN | personal identification number |
| RN | random number |
| Tcard | time-variant information generated by bank card |
| TID | terminal identifier |
| TOD | time-of-day |
| TR | transaction request |
| Tterm | time-variant information generated by terminal |
| Rf | reference |
| Z | initializing vector |