

**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.

Copyright © 1982 by John Wiley & Sons, Inc.

All rights reserved. Published simultaneously in Canada.

Reproduction or translation of any part of this work beyond that permitted by Section 107 or 108 of the 1976 United States Copyright Act without the permission of the copyright owner is unlawful. Requests for permission or further information should be addressed to the Permissions Department, John Wiley & Sons, Inc.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional service. If legal advice or other expert assistance is required, the services of a competent professional person should be sought. *From a Declaration of Principles jointly adopted by a Committee of the American Bar Association and a Committee of Publishers.*

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, XIX

1. THE ROLE OF CRYPTOGRAPHY IN ELECTRONIC DATA PROCESSING 1

- Cryptography, Privacy, and Data Security, 1
 - Attack Scenarios, 1*
 - Technical Implications of Privacy Legislation, 4*
- The Data Encryption Standard, 6
- Demonstrating Effective Cryptographic Security, 8
- The Outlook for Cryptography, 10
- References, 11

2. BLOCK CIPHERS AND STREAM CIPHERS 13

- Cryptographic Algorithms, 14
 - Enciphering and Deciphering, 14*
 - Work Factor, 18*
 - Types of Attacks, 20*
 - Designing an Algorithm, 20*
- Block Ciphers, 23
 - Conventional Algorithms, 26*
 - Public-Key Algorithms, 32*
 - RSA Algorithm, 33*
 - Trapdoor Knapsack Algorithm, 48*
- Stream Ciphers, 53
- Block Ciphers with Chaining, 62
 - Patterns Within Data, 62*
 - Block Chaining Using a Variable Key, 67*
 - Block Chaining Using Plaintext and Ciphertext Feedback, 69*
 - A Self-Synchronizing Scheme Using Ciphertext Feedback, 71*
 - Examples of Block Chaining, 73*
 - Short Block Encryption, 73*
- Stream Ciphers with Chaining, 85
 - A Chaining Method with the Property of Error Propagation, 86*
 - A Chaining Method with the Property of Self-Synchronization, 88*
 - Cipher Feedback Stream Cipher, 91*
- Effects of Padding and Initializing Vectors, 98

Cryptographic Message Authentication Using Chaining Techniques, 100	
Comparison of Block Ciphers and Stream Ciphers, 105	
References, 111	

3. THE DATA ENCRYPTION STANDARD

113

Classes of Ciphers, 113	
Design Criteria, 118	
<i>Breaking a System with Two Key-Tapes, 118</i>	
<i>Breaking a Key Auto-Key Cipher Using Linear Shift Registers, 121</i>	
<i>Breaking a Plaintext Auto-Key Cipher Using Linear Shift Registers, 129</i>	
<i>Designing a Cipher, 137</i>	
Description of the Data Encryption Standard, 141	
<i>Generation of Key Vectors Used for Each Round of DES, 143</i>	
<i>Weak and Semiweak Keys, 147</i>	
<i>Details of the DES Algorithm, 153</i>	
<i>Summary of the DES Procedure, 159</i>	
<i>Numerical Example, 160</i>	
<i>Some Remarks About the DES Design, 162</i>	
<i>Implementation Considerations for the S-Box Design, 163</i>	
Analysis of Intersymbol Dependencies for the Data Encryption Standard, 165	
<i>Interdependence Between Ciphertext and Plaintext, 168</i>	
<i>Interdependence Between Ciphertext and Key, 178</i>	
<i>Summary and Conclusions, 189</i>	
References, 189	

4. COMMUNICATION SECURITY AND FILE SECURITY USING CRYPTOGRAPHY

192

Networks, 192	
Network Encryption Modes, 195	
Fundamentals of Link Encryption, 201	
<i>Asynchronous, 203</i>	
<i>Byte-Synchronous, 204</i>	
<i>Bit-Synchronous, 206</i>	
An Overview of End-To-End Encryption, 206	
Cipher Key Allocation, 208	
<i>Specification of Cipher Keys, 209</i>	
<i>An Example of the Encryption of Transmitted Data, 219</i>	
<i>An Example of the Encryption of a Data File, 222</i>	
The Cryptographic Facility, 222	

Cipher Key Protection, 226	
<i>Protection of Terminal Keys, 226</i>	
<i>Protection of Host Keys, 228</i>	
<i>Hierarchy of Cipher Keys, 232</i>	
The Host Cryptographic System, 234	
Basic Cryptographic Operations, 237	
<i>Cryptographic Operations at a Terminal, 239</i>	
<i>Cryptographic Operations at a Host, 243</i>	
<i>Key Parity, 249</i>	
<i>Partitioning of Cipher Keys, 250</i>	
Cipher Macro Instruction, 253	
Key Management Macro Instructions, 260	
<i>GENKEY and RETKEY Macros, 260</i>	
<i>Using GENKEY and RETKEY, 265</i>	
The Cryptographic Key Data Set, 267	
Summary, 269	
References, 269	

5. THE HOST SYSTEM CRYPTOGRAPHIC OPERATIONS

271

Single-Domain Communication Security Using Pregenerated Primary Keys, 271	
Single-Domain Communication Security Using Dynamically Generated Primary Keys, 274	
<i>Two Master Keys, 275</i>	
<i>Requirements, 278</i>	
Single-Domain Communication Security and File Security Using Dynamically Generated Primary Keys, 278	
<i>Problems Associated with Storing Enciphered Data, 278</i>	
<i>Three Master Keys, 280</i>	
<i>An Example of File Encryption, 283</i>	
<i>Requirements, 284</i>	
Multiple-Domain Encryption, 284	
<i>A Protocol for Communication Security, 285</i>	
<i>A Protocol for File Security, 288</i>	
<i>Transporting a New File, 288</i>	
<i>Transporting an Existing File, 289</i>	
Additional Considerations, 291	
Extended Cryptographic Operations, 292	
<i>Cryptographic Key Distribution Using Composite Keys, 293</i>	
<i>A Composite Key Protocol, 294</i>	
Summary, 299	
References, 299	

6. GENERATION, DISTRIBUTION, AND INSTALLATION OF CRYPTOGRAPHIC KEYS 300

Generation of the Host Master Key, 301

Tossing Coins, 301

Throwing Dice, 302

Random Number Table, 303

Generation of Key-Encrypting Keys, 303

A Weak Key-Generating Procedure, 304

A Strong Key-Generating Procedure, 304

An Alternate Approach for Generating Key-Encrypting Keys, 307

Encipherment of Keys under the Master Key's Variants, 308

Transforming Cryptographic Keys, 311

Generation of Data-Encrypting Keys, 314

An Approach for Generating Keys with the Cryptographic Facility, 315

An Alternate Approach for Generating Data-Encrypting Keys, 316

Entering a Master Key at the Host Processor, 317

Hard-Wired Entry, 318

Indirect Entry, 321

Attack Via External Manipulations, 322

Master Key Entry at a Terminal, 323

On-Line Checking, 323

Off-Line Checking, 323

Distribution of Cryptographic Keys, 326

Lost Cryptographic Keys, 327

Recovery Techniques, 328

Summary, 329

References, 330

7. INCORPORATION OF CRYPTOGRAPHY INTO A COMMUNICATIONS ARCHITECTURE 331

Session-Level Cryptography in a Single-Domain Network, 333

Transparent Mode of Operation, 333

Nontransparent Mode of Operation, 339

Private Cryptography in a Single-Domain Network, 339

Session-Level Cryptography in a Multidomain Network, 343

Application Program-to-Application Program Cryptography, 347

Padding Considerations, 349

References, 349

8. AUTHENTICATION TECHNIQUES USING CRYPTOGRAPHY 350

Fundamental Concepts, 350

Handshaking, 351

Message Authentication, 354

Authentication of a Message's Origin, 354

Authentication of a Message's Timeliness, 358

Authentication of a Message's Contents, 359

Authentication of a Message's Receiver, 364

A Procedure for Message Authentication, 364

Authentication of Time-Invariant Data, 367

Authentication of Passwords, 368

Authentication Using Test Patterns Generated from the Host Master Key, 371

A Procedure for Authentication of Cryptographic Keys, 381

Another Authentication Method Using Test Patterns Generated from the Host Master Key, 382

References, 385

9. DIGITAL SIGNATURES 386

Significance of Signatures, 386

Law of Acknowledgements, 387

Law of Agency, 388

Uniform Commercial Code, 388

Contributory Negligence, 389

Obtaining Digital Signatures, 390

Universal Signatures, 391

An Approach Using Public-Key Algorithms, 392

An Approach Using Conventional Algorithms, 396

Arbitrated Signatures, 409

An Approach Using the DES Algorithm, 410

An Example of Arbitrating a Signature, 412

A Weak Approach, 414

Additional Weaknesses, 416

Using DES to Obtain Public-Key Properties, 417

A Key Notarization System for Computer Networks, 417

A Method Using Variants of the Host Master Key, 421

Legalizing Digital Signatures, 423

Initial Written Agreement, 424

Choice of Law, 425

Judicial Notice Recognized, 426

References, 427

10. APPLYING CRYPTOGRAPHY TO PIN-BASED ELECTRONIC FUNDS TRANSFER SYSTEMS 429

Introduction, 429

Section One—Basic PIN Concepts, 430

Why PINs?, 430

PIN Secrecy, 431

PIN Length, 432

Allowable PIN Entry Attempts, 433

PIN Issuance, 434

PIN Validation for Local Transactions, 440

PIN Validation for Interchange Transactions, 441

Conclusions, 443

Section Two—EFT Fraud Threats, 444

EFT Fraud Categories, 445

Passive Fraud Threats, 446

Relative Risks, 448

Active Fraud Threats, 449

Fraud and Liability, 451

Conclusions, 453

Section Three—Principles of Fraud Prevention, 454

Cryptography, The Tool for Fraud Prevention, 454

Preventing Passive Fraud Threats, 455

Preventing Active Fraud Threats, 457

Fraud Prevention in Interchange, 461

Conclusions, 463

Section Four—Implementation of Fraud Prevention Techniques, 464

Suggested Characteristics of Hardware Security Module

Implementation, 464

Suggested Capabilities, 465

PIN Validation, 467

Key Management, 468

MAC Generation, 469

Utilization, 469

Conclusions, 473

References, 473

11. APPLYING CRYPTOGRAPHY TO ELECTRONIC FUNDS TRANSFER SYSTEMS—PERSONAL IDENTIFICATION NUMBERS AND PERSONAL KEYS 474

Background, 474

Security Exposures in EFT Systems, 478

<i>Communication Link Security</i>	478
<i>Computer Security</i>	478
<i>Terminal Security</i>	479
<i>Bank Card Security</i>	481
Identification and Authentication of System Users	482
<i>Transferable User Characteristics</i>	482
<i>Nontransferable User Characteristics</i>	482
Requirements for Personal Verification and Message Authentication	483
<i>Authentication Parameter</i>	484
<i>Personal Authentication Code</i>	486
<i>Personal Verification Using AP Only</i>	487
<i>Personal Verification Using AP and PAC</i>	488
<i>Message Authentication Using a MAC</i>	489
<i>EFT Security Requirements</i>	490
<i>Comments on the EFT Security Requirements</i>	499
Personal Verification in the On-Line Mode	499
<i>Personal Verification with Dependent PINs and Dependent Personal Keys</i>	500
<i>Personal Verification with Independent PINs and Independent Personal Keys</i>	502
<i>Minimizing Card Storage Requirements</i>	507
Personal Verification in the Off-Line and Off-Host Modes	511
<i>Personal Verification with System-Selected PINs Employing a PIN Generating Key</i>	512
<i>Personal Verification with User-Selected PINs Employing Offsets</i>	514
<i>Personal Verification with User-Selected PINs Employing PACs</i>	514
Guidelines for Cryptographic Designs	517
<i>Threats to PIN Secrecy</i>	520
<i>Key Management Requirements</i>	523
<i>Threats to the Secrecy of a Key Stored on a Magnetic Stripe Card</i>	526
The PIN/System Key Approach	530
<i>Key Management Considerations for PIN/System Key Approach</i>	535
<i>Defending Against the Misrouting Attack</i>	536
<i>A PIN/System Key Approach for Noninterchange</i>	541
<i>A PIN/System Key Approach for Interchange</i>	541
<i>Disadvantages of the PIN/System Key Approach</i>	544
<i>Advantages of the PIN/System Key Approach</i>	545
The PIN/Personal Key Approach	546
<i>Description of a PIN/Personal Key Approach Using a Magnetic Stripe Card</i>	546
<i>Key Management Considerations for PIN/Personal Key Approach</i>	548
<i>Advantages of the PIN/Personal Key Approach</i>	548
<i>Objections to the PIN/Personal Key Approach Using a Magnetic Stripe Card</i>	549
<i>Personal Key Approach with an Intelligent Secure Card</i>	551

The PIN/Personal Key/System Key (Hybrid Key Management) Approach
Using an Intelligent Secure Card, 557

Description of a Hybrid Key Management Approach, 558

Key Management Considerations for the Hybrid Approach, 561

Hybrid Key Management Approach for Noninterchange, 562

Hybrid Key Management Approach for Interchange, 566

Cryptographic Considerations for an Intelligent Secure Card, 569

Security Enhancements with Digital Signatures, 569

Advantages, 576

Key Management Considerations—Symmetric Versus Asymmetric
Algorithms, 577

Authentication With and Without Secrecy, 578

Secrecy Without Authentication, 583

A Cryptographic System Using an Intelligent Secure Card and a
Public-Key Algorithm, 588

Description of a Public Key Management Approach, 589

Key Management Considerations for Asymmetric Algorithms, 593

Off-Line Use, 594

On-Line Use in Interchange and Noninterchange, 596

Concluding Remarks, 604

Glossary, 604

References, 605

12. MEASURES OF SECRECY FOR CRYPTOGRAPHIC SYSTEMS

607

Elements of Mathematical Cryptography, 608

Information Flow in a Conventional Cryptographic System, 608

A Cipher with Message and Key Probabilities, 609

The Random Cipher, 614

Number of Meaningful Messages in a Redundant Language, 615

Probabilistic Measures of Secrecy Using a Random Cipher, 618

*Probability of Obtaining the Key When Only Ciphertext Is Available
for Analysis, 618*

An Example of Simple Substitution on English (Ciphertext Only), 621

*Probability of Obtaining the Key When Plaintext and Corresponding
Ciphertext Are Available for Analysis, 624*

Probability of Obtaining the Plaintext, 625

An Expansion of Shannon's Approach Using Information Theory, 627

Information Measures, 628

*Unicity Distance for a Cipher When Only Ciphertext is Available
for Analysis, 629*

*Unicity Distance for a Cipher When Plaintext and Corresponding
Ciphertext Are Available for Analysis, 631*

Relationships Among $H(X|Y)$, $H(K|Y)$, and $H(K|X, Y)$, 632
Unicity Distance for the Data Encryption Standard, 635

Work Factor as a Measure of Secrecy, 636

The Cost and Time to Break a Cipher, 636

Simple Substitution on English—Some Preliminaries, 637

*Empirical Results for Simple Substitution on English Using a
Digram Frequency Analysis, 640*

*Empirical Results for Simple Substitution on English Using
Single-Letter Frequency Analysis, 642*

Comparison of Results, 642

References, 647

APPENDIX A. FIPS PUBLICATION 46 649

APPENDIX B. FURTHER COMPUTATIONS OF INTEREST 671

Time-Memory Trade-Off, 671

Birthday Paradox, 672

References, 673

APPENDIX C. PLASTIC CARD ENCODING PRACTICES AND STANDARDS 675

General Physical Characteristics, 675

Track 1, 675

Track 2, 676

Track 3, 677

References, 678

APPENDIX D. SOME CRYPTOGRAPHIC CONCEPTS AND METHODS OF ATTACK 679

Further Discussion of Authentication Parameters, 679

One-Way Functions, 679

Attack Using Repeated Trials, 681

Further Discussion of Authentication Parameters and
Personal Authentication Codes, 687

Implementation Examples, 687

Attack Against a 16-Digit PIN, 688

Attack Against a 12-Digit PIN, 688

Proposals for Authentication Parameters and Personal

	<i>Authentication Codes</i> , 689 <i>The Advantage of an AP that Depends on ID</i> , 694 Increasing Exhaustive Attack Work Factor by Implementation Methods, 696 <i>Multiple Encryption and Block Chaining</i> , 696 <i>Reduction of Exhaustion Work Factor for Selected Plaintext Attack</i> , 697 <i>The Meet-in-the-Middle Attack Against Double Encryption</i> , 705 <i>Attack Against Triple Encryption with Three Independent Keys</i> , 708 <i>Attack Against Triple Encryption with Two Independent Keys</i> , 711 References, 712	
APPENDIX E.	CRYPTOGRAPHIC PIN SECURITY—PROPOSED ANSI METHOD	713
	Storage of PINs, 713 Transmission of PINs, 713 <i>Reversible PIN Encryption</i> , 714 <i>Cleartext PIN Block Format</i> , 714 <i>Ciphertext PIN Format</i> , 715 <i>Received Ciphertext PIN</i> , 716 References, 716	
APPENDIX F.	ANALYSIS OF THE NUMBER OF MEANINGFUL MESSAGES IN A REDUNDANT LANGUAGE	717
	References, 727	
APPENDIX G.	UNICITY DISTANCE COMPUTATIONS	728
	Transposition, 728 Simple Substitution, 731 Homophonic Substitution, 733 References, 740	
APPENDIX H.	DERIVATION OF $p(u)$ AND $p(SM)$	741
	References, 746	
INDEX		747

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