

89069572584



b89069572584a

MEYER  
CRYPTOGRAPHY

Z  
103  
M55  
1982

# **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



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 guide for the design and implementation of cryptographic 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 7 6 5 4 3 2 1

# 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                                                                                      |

|                                                                                |                |
|--------------------------------------------------------------------------------|----------------|
| <b>6. GENERATION, DISTRIBUTION, AND INSTALLATION OF CRYPTOGRAPHIC KEYS</b>     | <b>300</b>     |
| Generation of the Host Master Key, 301                                         |                |
| <i>Tossing Coins, 301</i>                                                      |                |
| <i>Throwing Dice, 302</i>                                                      |                |
| <i>Random Number Table, 303</i>                                                |                |
| Generation of Key-Encrypting Keys, 303                                         |                |
| <i>A Weak Key-Generating Procedure, 304</i>                                    |                |
| <i>A Strong Key-Generating Procedure, 304</i>                                  |                |
| <i>An Alternate Approach for Generating Key-Encrypting Keys, 307</i>           |                |
| <i>Encipherment of Keys under the Master Key's Variants, 308</i>               |                |
| <i>Transforming Cryptographic Keys, 311</i>                                    |                |
| Generation of Data-Encrypting Keys, 314                                        |                |
| <i>An Approach for Generating Keys with the Cryptographic Facility, 315</i>    |                |
| <i>An Alternate Approach for Generating Data-Encrypting Keys, 316</i>          |                |
| Entering a Master Key at the Host Processor, 317                               |                |
| <i>Hard-Wired Entry, 318</i>                                                   |                |
| <i>Indirect Entry, 321</i>                                                     |                |
| Attack Via External Manipulations, 322                                         |                |
| Master Key Entry at a Terminal, 323                                            |                |
| <i>On-Line Checking, 323</i>                                                   |                |
| <i>Off-Line Checking, 323</i>                                                  |                |
| Distribution of Cryptographic Keys, 326                                        |                |
| Lost Cryptographic Keys, 327                                                   |                |
| Recovery Techniques, 328                                                       |                |
| Summary, 329                                                                   |                |
| References, 330                                                                |                |
| <br><b>7. INCORPORATION OF CRYPTOGRAPHY INTO A COMMUNICATIONS ARCHITECTURE</b> | <br><b>331</b> |
| Session-Level Cryptography in a Single-Domain Network, 333                     |                |
| <i>Transparent Mode of Operation, 333</i>                                      |                |
| <i>Nontransparent Mode of Operation, 339</i>                                   |                |
| 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 |  |
| <i>Description of a Hybrid Key Management Approach, 558</i>                                            |  |
| <i>Key Management Considerations for the Hybrid Approach, 561</i>                                      |  |
| <i>Hybrid Key Management Approach for Noninterchange, 562</i>                                          |  |
| <i>Hybrid Key Management Approach for Interchange, 566</i>                                             |  |
| <i>Cryptographic Considerations for an Intelligent Secure Card, 569</i>                                |  |
| <i>Security Enhancements with Digital Signatures, 569</i>                                              |  |
| <i>Advantages, 576</i>                                                                                 |  |
| Key Management Considerations—Symmetric Versus Asymmetric Algorithms, 577                              |  |
| <i>Authentication With and Without Secrecy, 578</i>                                                    |  |
| <i>Secrecy Without Authentication, 583</i>                                                             |  |
| A Cryptographic System Using an Intelligent Secure Card and a Public-Key Algorithm, 588                |  |
| <i>Description of a Public Key Management Approach, 589</i>                                            |  |
| <i>Key Management Considerations for Asymmetric Algorithms, 593</i>                                    |  |
| <i>Off-Line Use, 594</i>                                                                               |  |
| <i>On-Line Use in Interchange and Noninterchange, 596</i>                                              |  |
| Concluding Remarks, 604                                                                                |  |
| Glossary, 604                                                                                          |  |
| References, 605                                                                                        |  |

## 12. MEASURES OF SECRECY FOR CRYPTOGRAPHIC SYSTEMS

607

|                                                                                                                     |  |
|---------------------------------------------------------------------------------------------------------------------|--|
| Elements of Mathematical Cryptography, 608                                                                          |  |
| <i>Information Flow in a Conventional Cryptographic System, 608</i>                                                 |  |
| <i>A Cipher with Message and Key Probabilities, 609</i>                                                             |  |
| <i>The Random Cipher, 614</i>                                                                                       |  |
| <i>Number of Meaningful Messages in a Redundant Language, 615</i>                                                   |  |
| Probabilistic Measures of Secrecy Using a Random Cipher, 618                                                        |  |
| <i>Probability of Obtaining the Key When Only Ciphertext Is Available for Analysis, 618</i>                         |  |
| <i>An Example of Simple Substitution on English (Ciphertext Only), 621</i>                                          |  |
| <i>Probability of Obtaining the Key When Plaintext and Corresponding Ciphertext Are Available for Analysis, 624</i> |  |
| <i>Probability of Obtaining the Plaintext, 625</i>                                                                  |  |
| An Expansion of Shannon's Approach Using Information Theory, 627                                                    |  |
| <i>Information Measures, 628</i>                                                                                    |  |
| <i>Unicity Distance for a Cipher When Only Ciphertext is Available for Analysis, 629</i>                            |  |
| <i>Unicity Distance for a Cipher When Plaintext and Corresponding Ciphertext Are Available for Analysis, 631</i>    |  |

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

of large numbers of such cards could be truly disastrous. The use of lost and stolen cards is a potential problem but the use of any sort of PIN system could control this fraud threat. The remaining threat is the modification or insertion of data in real time. Though a serious threat, it would not have nearly as devastating an effect as the massive use of counterfeit cards.

The two main types of fraud threats are passive, the determination of PINs and corresponding account identities to enable the use of lost, stolen, or counterfeit cards, and active, the fraudulent modification or insertion of data in real time. Of these two, the passive is of greater concern in an interchange environment, not only because the passive threats could lead to mass fraud in the form of counterfeit cards, but also because it would be virtually impossible to ascertain the negligent party and thus establish liability for such fraud. Active threats, though potentially serious, are not judged to be catastrophic, and quite often can be traced back to the offending institution.

As a result, it is concluded that an EFT system should protect against passive threats in all aspects of interchange. If very high security is desired, it appears that an issuer's clear PINs should not be allowed, even momentarily, in any general purpose EDP equipment of an acquirer or switch but rather than such clear PINs should be restricted to physically secure cryptographic hardware where they, and the cryptographic keys used to encrypt them, can be physically protected. By imposing stringent security requirements upon all acquirers and switches, it seems more reasonable to then place liability for any use of lost, stolen, or counterfeit cards on the issuer, any compromise of his cardholders' PINs being assumed to result from negligence on the part of the issuer or its cardholders.

A further conclusion is that protection against active fraud threats can be left up to an acquirer's discretion, provided he is willing to assume responsibility for any such fraud against which he does not provide protection. However, it does appear desirable to protect transactions in interchange between institutions against these active threats.

Perhaps the most important conclusion of all is that fraud in a nationwide interchange environment could eventually become a serious problem, if not a major catastrophe. Thus, in planning for interchange, and during the evolution toward it, careful provisions must be made to ensure that adequate security is indeed realized. Security must be an inherent characteristic of EFT from the start. It cannot be added on after the fact.

### SECTION THREE: PRINCIPLES OF FRAUD PREVENTION

#### Cryptography, The Tool for Fraud Prevention

Most of the techniques used to prevent fraud in an EFT system are based upon the use of cryptography. Cryptography involves encryption and decryption. Encryption is the transformation of clear (comprehensible) data by means of an algorithm (i.e., a defined procedure) and a secret number called a key into a form called cipher, which bears no resemblance to the original, clear data. Only someone else possessing the identical secret key is able to decrypt the transformed data and recreate its original clear form.

The Interbank recommended encryption algorithm for use in EFT is the Data Encryption Standard (DES), which is the cryptographic algorithm sponsored by the National Bureau of Standards for data security. It is the only publicly available algorithm which has been certified as highly secure by the United States Government. DES is a block encryption technique. That is, given an input data block of 64 binary bits, a 56 bit secret binary key, and the encrypt command, the algorithm produces 64 cipher bits. These bits bear no obvious relation to the input. In fact, a minor (i.e., one bit) change in the input produces a drastic change in the output. Given these 64 cipher bits, the same 56 bit key, and the decrypt command, the algorithm produces the original clear data.

Though inherently a binary, block encryption technique, DES can be applied in various ways to implement virtually any desired type of encryption.

### Preventing Passive Fraud Threats

As described in the preceding section, passive fraud threats are those which enable the PIN for known accounts to be ascertained. As a result, the use of lost, stolen, or counterfeit cards is possible. Given today's technology, the fraud threat can be virtually prevented by:

1. Insuring that the PIN is encrypted at all times except when within a physically secure environment.
2. Insuring that the keys used to encrypt PINs are never available in "clear" form except within physically secure environments.
3. Insuring that physically secure environments, in which clear PINs and clear PIN encrypting keys are found, are in fact secure against physical compromise.

### PIN Encryption

To be protected against compromise the PIN should be encrypted using DES and a secret key. Furthermore, the PIN should be encrypted as a function of some quantity which varies from transaction to transaction, or at least from account to account. Were this not done, identical clear PINs encrypted under the same key would produce identical ciphers. This fact could be exploited by a criminal, who would, for example, open ten accounts under fictitious names. He would then know ten PINs and institute transactions from a specific EFT terminal against each of his ten accounts. He would also have tapped the line from his terminal, and would record the encrypted PIN from each of his ten transactions. Next he would use the tap to record transactions from other cardholders. Whenever the encrypted PIN from one of these transactions exactly matched the encrypted PIN from one of his accounts, he would know that the clear PINs were identical. In an environment in which most or all PINs are four digits, he would be able to ascertain the PIN for approximately one account in a thousand which used this particular terminal. For each of these cases, from other information in the recorded transaction, he could determine the contents of the associated card's magnetic stripe, and

thus make a counterfeit copy of this card and use it to draw against the cardholder's funds.

One method of encrypting the PIN as a function of a varying quantity (and thus preclude the above indicated fraud threat) is to concatenate the clear PIN with a value six decimal digits or longer, which is:

1. A random or pseudorandom number,
2. A counter, which increments on each transaction, or
3. The least significant digits of the account number.

The result, which must be no more than 64 binary bits in length, is block encrypted using DES and a secret key. The entire 64 bit resulting cipher thus serves as the encrypted PIN for this transaction.

Other equally secure PIN encryption methods exist in which the encrypted PIN is a decimal value of the same number of digits as the clear PIN.

#### Protection of Cryptographic Keys

PINs should always be encrypted under secret 56 bit DES keys. Maintaining the secrecy of these keys is of the utmost importance, because if any such key becomes compromised the PINs encrypted under it can be similarly compromised. There are two problems associated with key secrecy. The first is the generation and distribution of keys in such a way as to preclude compromise. This is called key management, and will be discussed subsequently. The other, protection of the key while it is within the cryptographic device, will be considered now.

#### Physical Protection of PINs and Cryptographic Keys

PINs and keys must be physically protected whenever they are in clear (unencrypted) form within cryptographic devices. (For high security, clear PINs and keys should exist nowhere else.) The most effective solution to this problem appears to be the interlocking of the device's enclosure. All of the cryptographic logic is placed within a physically secure enclosure and tamper detection circuitry, built into the enclosure, detects any attempt to gain access to the internal circuitry of the device. The secret keys are interlocked by means of these tamper circuits so that any act of tampering causes the keys to be erased.

The immediate erasure of the keys obviously protects them from compromise. Tapping of the device to ascertain future PINs is prevented also, because opening the device to install the tap erases the secret keys and this renders the device inoperative (i.e., unable to decrypt incoming PINs). As a result, the tap will not successfully capture PINs.

In order to protect the PIN at its point of entry into the system, the PIN keyboard must be a part of this protected enclosure. If it is, and if the enclosure is properly protected via the above suggested interlocks, the terminal tapping threat discussed in the preceding section is precluded.

### Preventing Active Fraud Threats

Though passive fraud threats may be countered by simply protecting the PIN from disclosure, countering active threats is more difficult, with different countermeasures needed for different threats.

#### Data Modification

Many active fraud threats involve the modification of data in real time. These threats can be countered by either of two techniques, message encryption or message authentication. Message encryption, as the name implies, is simply the encryption of all, or at least most, of the message which conveys the transaction. This technique has the advantage of providing privacy as well as security. The disadvantage, however, is that the encrypted message cannot be comprehended or processed by the EDP systems (acquirer's, switch's, issuer's) through which the transaction passes. Thus, the message must be decrypted prior to being processed, but once decrypted, it loses its cryptographic protection, and therefore is susceptible to fraudulent modification within the EDP system.

Message authentication is a technique which produces cryptographic check digits which are appended to the message. These digits are analogous to a parity check or cyclic redundancy check, except that in this case the check digits are cryptographically generated, using DES and a secret key. These digits, called the message authentication code or MAC, are generated by the originator, appended to the transmitted message, and then checked by the recipient, who also holds the same secret key used in the generation process. Should anyone attempt to modify the message between the time the MAC is generated and the time it is checked, he would be detected. Not knowing the secret key, he would be unable to generate the correct MAC for his modified message. Similarly, no one can successfully introduce a spurious message because he could not generate the proper MAC for this message.

The suggested technique for MAC generation is as follows: The first 64 bits of that portion of the transaction to be protected are block encrypted using DES and the secret key. Then the next 64 transaction bits to be thus protected are Exclusive-ORed (modulo 2 added) with the just produced cipher. The result is then block encrypted using the same key, producing a new 64 bits of cipher. This procedure is continued until all critical transaction fields have been included. (The final data block will likely be less than 64 bits, so it is padded with zeros to make a full 64 bits prior to being Exclusive-ORed with the just produced cipher.) Some subset of the final cipher, at least six decimal digits or five hexadecimal digits, serves as the MAC.

As a minimum, the following fields should be included in the MAC generation for a transaction request message:

1. Transaction type (debit, credit, etc.).
2. Cardholder's account number.
3. Amount.

4. Transaction identification information (that information which uniquely identifies a specific transaction from a particular terminal).

In the case of a transaction response message, the equivalent fields plus the response code (approved, disapproved) should be protected. Alternatively, the MAC can be generated only if the transaction is approved, because no known fraud threat could exploit an unprotected disapproved response message.

Though the MAC approach does not provide privacy, its advantage over message encryption is that the protected message is also intelligible, and thus can be processed by EDP systems. With message encryption, the protection is lost when the message is decrypted, so the message is protected against fraudulent modifications only over communications lines but not within EDP systems. Thus message authentication, by protecting the transaction against fraudulent modifications both over communications lines and within EDP systems, is the recommended approach.

As indicated in the preceding section, message authentication can be optional within an acquirer's own network, provided the acquirer is willing to assume any fraud loss which might result from the failure to protect against any "active" fraud threats. However, it is recommended that all transactions in interchange be protected against active fraud by means of message authentication. If subsequent privacy legislation requires encryption, this can be accomplished, for the interchange network, by using link encryption devices, or by encrypting the six or so least significant digits of the account number to conceal the cardholder's identity.

#### Replay of Debit Authorization

Perhaps the most likely active fraud threat is the isolation of a terminal (especially an ATM) from its host, giving it an "approved" response to every transaction request. Message authentication alone cannot necessarily solve this problem, because it might be possible to record the "approved" response to a valid transaction prior to isolating the unit, then institute identical fraudulent transactions, and replay the previously recorded "approved" response. This fraud threat can be countered only if there is something unique about each transaction (even two transactions for the same amount against the same account), and the transaction-approved response includes this uniqueness, which is checked by the terminal. Furthermore, this unique characteristic must not be something which the criminal can duplicate. For example, the terminal itself can insert a sequence number into the transaction request message. This same number is included in the transaction authorization message back to the terminal protected under the MAC. The terminal checks for agreement between the two values and authorizes the completion of the transaction (e.g., the dispensing of cash) only if the sent and received sequence numbers are identical. Thus, it is impossible to replay the "approved" response to a previous transaction because the sequence number is invalid for any other transaction. Furthermore, the replay version cannot be modified to include the current sequence number, because the MAC would not check.

For this approach to provide the required degree of protection, the sequence number should not repeat within the life of the cryptographic key used in the MAC generation. Alternately, it could be a random, rather than a sequential value, provided it is truly unpredictable, and is at least six decimal digits in length.

Other approaches can provide the same effect. For example, if the terminal key is changed after every transaction, a MAC on the transaction authorization message is unique to a given transaction.

### Fraudulent Credits

The four fraud threats associated with credit transactions are:

1. Modified credits (amount field increased, or debit made into a credit).
2. Misdirected credits (account number modified).
3. Spurious credits (totally fictitious credit transaction).
4. Fraudulent replay of previously valid credit transaction.

The first three fraud threats may be countered by the use of message authentication. The use of MAC prevents undetected modifications in any critical transaction field, and also prevents the origination of totally spurious transactions. The fourth fraud threat, however, is somewhat more difficult to counter. Though message sequence numbers are commonly used to detect duplicated messages, these numbers are not considered a part of the security system and thus cannot be relied upon for fraud prevention purposes. That is, they can only be checked in the presumably non-secure main frame, and cannot be checked in special security equipment.

It appears that the responsibility for detecting replayed credits must rest with the issuer. Under this approach, the issuer would be expected to check the previous real time EFT credit transaction for the account in question and verify that it had occurred earlier than the current credit transaction. (This assumes that real time EFT credit transactions are stored in chronological order and that the date/time field in every such credit transaction is protected by the transaction's MAC.) The issuer could then immediately detect a replayed transaction.

It should be noted that real time credits in a retail EFT system should be relatively infrequent. Normal bank deposits are not real time because they are subject to verification and to check clearances. The only expected real time credits would result from the return of merchandise, a relatively uncommon occurrence, so placing the responsibility for detecting the replay of such credits upon the issuer should not be an undue burden.

### Encrypted PIN Substitution

Unless appropriately precluded, it would be possible for a criminal to record an encrypted PIN as it leaves a terminal in a valid transaction, then, by active wiretapping at a later time, replay this recorded encrypted PIN as part of a fraudulent transaction. This fraud threat is prevented by techniques which

insure that the same PIN when encrypted by the same terminal on two or more different occasions always produces a unique cipher each time. This can be achieved by encrypting the PIN as a function of a variable quantity, such as a terminal generated transaction sequence number (in addition to the secret key). To be fully effective, this terminal should utilize message authentication for the transaction authorization message. This message should include the same variable quantity (e.g., the transaction sequence number) which is used in the encryption of the PIN in the transaction request message. Only if the variable quantity in the authorization message matches the one the terminal used for PIN encryption in the request message, and only if the authorization message is successfully authenticated by the terminal, does the terminal complete the transaction. At the host end, PIN validation and authentication of the authorization message should be performed as a single operation in a physically secure environment, the message authentication code for the authorization message being generated only if the cardholder entered PIN is successfully validated.

If the above indicated procedures are followed, the criminal is prevented from fraudulently replaying a previously recorded encrypted PIN. This PIN would have been encrypted as a function of a previously used variable quantity which could not be successfully reused.

Another technique which can be used to prevent the substitution of the encrypted cardholder entered PIN is key transformation. With this technique, the terminal's key is changed after every transaction. This is accomplished by generating the new key from the old key via a cryptographic procedure. Since the key used to encrypt the PIN changes on each transaction, the criminal is unable to successfully replay the encrypted PIN from a previous transaction. To insure this completely, however, the authorization message to the terminal must be authenticated using the current key.

Other fraud threats are possible if the criminal is able to substitute the encrypted version of a PIN, which the criminal himself knows, for the cardholder's encrypted PIN of reference. Two techniques are required to preclude this threat. First, the cardholder's PIN must be encrypted as a function of his account number. This prevents the criminal from substituting his encrypted PIN of reference for that of the targeted cardholder. Second, the PINs of reference must be encrypted under a cryptographic key never used to encrypt cardholder entered PINs. This prevents the criminal from using an invented PIN with a counterfeit card for the targeted account, then replacing the PIN of reference for this account with the encrypted version of the invented PIN.

It should be noted that the prevention of this fraud threat requires that the PIN of reference and the entered PIN both be decrypted (or that the latter be decrypted, then reencrypted like the former) before a comparison is made since both are encrypted under different keys. This does not permit a commonly used PIN validation technique in which the encrypted cardholder entered PIN is compared in a non-secure environment against a similarly encrypted PIN of reference.

### Fraud Prevention in Interchange

The fraud threats associated with interchange are basically no different than those already considered, namely, passive threats to ascertain PINs (for use with lost, stolen or counterfeit cards), and active threats to modify or insert data in real time. Thus, the fraud prevention techniques considered above apply to interchange just as much as to local operations. However, interchange poses a practical problem concerning the implementation of these fraud prevention techniques, the necessity to translate from one cryptographic key to another.

A typical interchange transaction begins when the cardholder enters his PIN at some EFT terminal which also reads his card. At this point the PIN must be encrypted in a key unique to this particular terminal.

Similarly, if message authentication is used, it must be based on a key, the same or different, but still unique to this particular terminal. In an EFT system with thousands or tens of thousands of encrypting EFT terminals, it is not feasible, or even desirable, for every key of every acquirer's terminal to be known at every issuer's facility. Thus, each acquirer must have the capability to translate from the terminal's key to an interchange key known either by the issuer, or by the switch which serves the acquirer (in which case the switch will make a second translation into a key known to the issuer). Furthermore, in the case of the PIN, this translation must take place under conditions of very high security, desirably using special, physically protected, cryptographic hardware. As indicated previously, it may eventually be considered unacceptable for one institution's clear PINs, or the clear keys used to encrypt such PINs, to reside even momentarily in the general purpose EDP equipment of any other institution. Thus, for high security, the acquirer should not perform this translation function of the PIN using CPU software, but rather should use the above indicated physically secure hardware.

In the case of message authentication, however, this does not necessarily apply. Since message authentication is optional on the acquirer's part, he may use CPU software for MAC translation. However, in this case a completely different key must be used for MAC generation than is used for PIN encryption or the clear PIN key would exist in the acquirer's CPU. Since the acquirer may utilize special cryptographic hardware for PIN translation, it is suggested that this same hardware be used for MAC translation as well.

Should an acquirer or a switch find an invalid incoming MAC while performing MAC translation, it is considered acceptable for this institution simply to generate an invalid outgoing MAC. In this way, only the issuer, who performs the final MAC check, need implement the error paths which handle the invalid MAC situation.

Another acceptable technique is to superimpose the MAC on the encrypted PIN and avoid an additional field to the message. This may be accomplished by Exclusive-ORing the MAC and the encrypted PIN. Should the MAC not check, the issuer finds a garbled PIN, and the PIN check fails. While this technique cannot distinguish between an invalid PIN and a modified message,

this is of little consequence since the net result in either case is to disallow the transaction.

It is assumed that the EFT system as a whole provides an adequate degree of error control, so that the MAC is relied upon for fraud detection rather than error detection. Since fraud attempts are expected to be virtually nonexistent because of the use of message authentication, there is virtually no inefficiency in relaying a message with an invalid MAC all the way to the issuer.

Returning again to a typical interchange transaction, the encrypted PIN is transmitted from the EFT terminal, encrypted in this terminal's secret key. Optionally a MAC, to protect the critical message fields, is also included. The transaction message, including the encrypted PIN, and optionally the MAC, reaches the acquirer's facility. Here the above indicated cryptographic transaction takes place. The PIN is decrypted using the terminal key, and reencrypted using an interchange key. If there is an incoming MAC, this too is translated into the interchange key. If there is no incoming MAC, one is generated.

The interchange key indicated above is either a bilateral key shared by the issuer and the acquirer, or a key shared by the acquirer and his EFT switch. In this latter case, the transaction goes to the switch where a second cryptographic translation occurs, translating the PIN and MAC from the key used between switch and acquirer to that used between switch and issuer. The message with this new encrypted PIN and MAC is then transmitted from switch to issuer, where the MAC is checked and the PIN decrypted and validated. If the transaction is approved by the issuer, a transaction authorization message is sent from issuer to switch. This message is protected by means of a MAC using the key shared by switch and issuer. The switch, upon receiving the transaction authorization message, translates it into the key used between switch and acquirer. The MAC in this key reaches the acquirer. If the MAC is valid, the appropriate authorization response is transmitted to the terminal where the transaction originated. If this terminal expects a MAC with the authorization message, such a MAC is generated, in the terminal key.

### Countering the Fake Equipment Threat

Perhaps the most difficult fraud threat to counter is the fake equipment threat, in which a dishonest merchant induces unsuspecting cardholders to use EFT terminals with PIN pads which are fake. Either the entire terminal is fake, or a fake PIN pad is added to a non-PIN-using terminal. In either case the PIN pad output goes to a recorder, as does the output of the magnetic stripe reader. From the information thus collected, the criminal is able to produce usable counterfeit cards. Fortunately, this fraud threat is considered too blatant to be especially probable, but must be considered nevertheless.

This threat can be countered only with the help of the cardholders themselves, some of whom can be induced into cooperating by the offer of substantial rewards (but only after the fraud threat has actually materialized). To enable the cardholders to detect that something is suspicious, a code printed on the EFT receipt must indicate whether or not a PIN was used

with the transaction in question. For example, a Transaction Proof Code with a non-zero leading digit printed on the receipt, can indicate that a PIN was used. If the leading digit is zero, a PIN was not used. Thus, an observant cardholder who uses such a terminal with a PIN pad and finds the leading digit of his Transaction Proof Code is zero, would know that he could receive a reward for informing the financial institution of this fact without alerting the merchant.

In a similar manner, an account-related sequence number, maintained by the issuing institution and printed on the EFT receipt, would allow the alert cardholder to immediately detect a totally fake terminal (which did not communicate with his institution) because the sequence number printed on the receipt would not be the number he was expecting.

It is possible that the dishonest merchant could have a non-PIN terminal (with a fake PIN pad) modified so as to change, in real time, the leading Transaction Proof Code digit from zero to some other value. However, the Transaction Proof Code as recorded by the financial institution also prints on the cardholder's monthly statement. Thus, the alert cardholder would also know that he could receive a reward for reporting discrepancies between his EFT receipts and his statement (provided these discrepancies could be confirmed by the institution). The totally fake terminal (which resulted in no statement entry) and the terminal which actively modified the Transaction Proof Code, would be discovered through such cardholder reports. In an interchange environment with on-line EFT, it would be virtually impossible for the dishonest merchant to predict just how soon after using his fake equipment an alert cardholder would receive a statement and report his suspicions. The dishonest merchant would be exposed to an unacceptably high level of detection and therefore would not likely attempt this type of fraud in the first place.

While many cardholders would either not understand, or ignore the above suggested reward offers, a small number of intelligent and alert cardholders should respond. Even these few should be sufficient to pinpoint such dishonest merchants relatively quickly.

Since this fraud threat is considered rather improbable by Interbank, little attention need be paid at this time. Nevertheless, the possibility of the threat, and the techniques for countering it, should be kept in mind.<sup>3</sup>

### Conclusions

The two basic techniques used to provide security in an EFT environment are PIN encryption and message authentication. PIN encryption prevents passive fraud threats from ascertaining PINs, and thus precludes the use of lost, stolen, and counterfeit cards. For PIN encryption to be effective, the PIN must be physically protected everywhere that it is not encrypted. Similarly, the cryptographic keys used to encrypt PINs must be protected. Inter-

<sup>3</sup> A fake equipment attack, which cannot be defended against using the above mentioned technique is described in Chapter 11 in the section entitled Threats to the Secrecy of a Key Stored on a Magnetic Stripe Card.

locking these keys with the cryptographic device's enclosure is one obvious technique for providing the required physical protection.

Message authentication insures message integrity, and prevents most active fraud threats. A few active fraud threats, however, require specialized countermeasures, as does the fake equipment.

Interchange does not pose any unique fraud threats, but it does require a special cryptographic capability—translation from one cryptographic key to another under conditions of very high security.

The above discussion has presented only the basic principles of fraud prevention. The following section considers, in some detail, how these principles can be effectively implemented, both in EDP facilities and in EFT terminals. In addition, techniques for secure PIN management and key management will be considered.

#### SECTION FOUR: IMPLEMENTATION OF FRAUD PREVENTION TECHNIQUES

Section Three considered the general principles which are recommended for preventing fraud in EFT networks. This section will describe in further detail how these principles can be applied, through the use of a "security module." In its preferred implementation, such a module is a physically secure hardware device which serves as a peripheral to an EDP system. Potentially less secure implementations are also possible, in which security module functions are implemented in mainframe software. The implementation used by an issuer for its own PINs is clearly its decision. The implementation used by an acquirer in Interbank interchange may be dictated by future standards, though it is presently premature to indicate what such standards will be.<sup>4</sup>

##### Suggested Characteristics of Hardware Security Module Implementation

When very high security is desired, hardware implementation of the security module is recommended. The previously mentioned Interbank security study considered in detail how such a hardware device could best be implemented. The hardware implementation as suggested by this study is now considered.

The suggested security module is a self-contained, physically secure, microprocessor controlled cryptographic device programmed to perform the cryptographic functions which the EDP center of a financial institution requires for its EFT operations. A security module interfaces with the institution's EDP system as a peripheral device. Information which requires cryptographic processing is sent from the computer to the module, which almost immediately sends back the results.

Each security module can be programmed to perform virtually any required cryptographic function. These programs are written to insure that the secret ingredients in EFT operations, customer PINs and cryptographic keys, never exist in a clear form outside the physically secure internal circuitry of a security module or of an EFT terminal's cryptographic hardware. In effect,

<sup>4</sup> See Cryptographic PIN Security—Proposed ANSI Method, Appendix E.