

BIBLIOTHEQUE DU CERIST

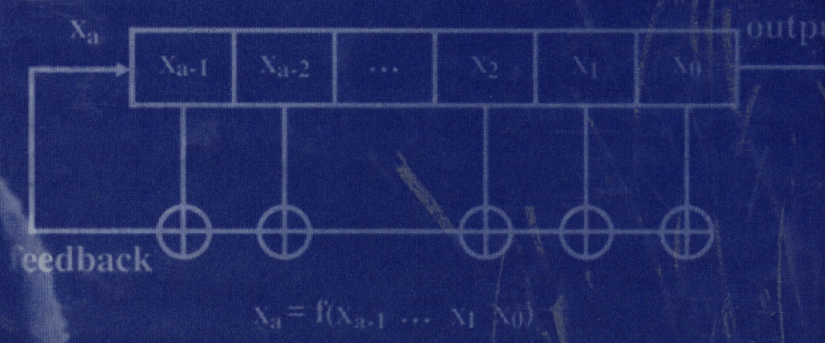
$$= B \log(1 + S/N)$$

 WILEY

CRYPTOGRAPHY, INFORMATION THEORY, AND ERROR-CORRECTION

A Handbook for the 21st Century

AIDEN A. BRUEN
MARIO A. FORCINITO



WWW.
LINK AVAILABLE

*Cryptography,
Information Theory,
and Error-Correction*

BIBLIOTHEQUE DU CERIST

**WILEY-INTERSCIENCE
SERIES IN DISCRETE MATHEMATICS AND OPTIMIZATION**

ADVISORY EDITORS

RONALD L. GRAHAM

University of California at San Diego, U.S.A.

JAN KAREL LENSTRA

*Department of Mathematics and Computer Science,
Eindhoven University of Technology, Eindhoven, The Netherlands*

JOEL H. SPENCER

Courant Institute, New York, New York, U.S.A.

A complete list of titles in this series appears at the end of this volume.

IST 2903

Cryptography, Information Theory, and Error-Correction

A Handbook for the 21st Century

Aiden A. Bruen

Mario A. Forcinito

 **WILEY-
INTERSCIENCE**

A JOHN WILEY & SONS, INC., PUBLICATION

BIBLIOTHEQUE DU CERIST



Cover: Marshfield Clinic granted permission for the use of the DNA helix.

Copyright © 2005 by John Wiley & Sons, Inc. All rights reserved.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

Published simultaneously in Canada.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600, or on the web at www.copyright.com. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representation or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services please contact our Customer Care Department within the U.S. at 877-762-2974, outside the U.S. at 317-572-3993 or fax 317-572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print, however, may not be available in electronic format.

Library of Congress Cataloging-in-Publication Data:

Bruen, Aiden A., 1941

Cryptography, information theory, and error-correction : a handbook for the 21st century
/ Aiden A. Bruen, Mario A. Forcinito
p. cm.

Includes bibliographical references and index.

ISBN 0-471-65317-9 (cloth)

1. Computer security. 2. Telecommunications systems Security measures. 3.
Cryptography. I. Forcinito, Mario, 1962- II. Title.

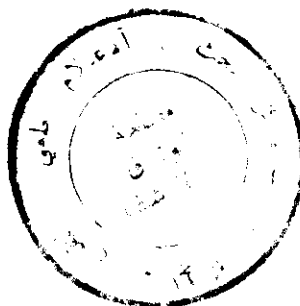
QA76.9.A25B79 2005
005.8 dc22

2004058044

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

Contents



Preface

xiii

I	Cryptography	1
1	History and Claude E. Shannon	3
1.1	Historical Background	3
1.2	Brief Biography of Claude E. Shannon	8
1.3	Career	9
1.4	Personal—Professional	10
1.5	Scientific Legacy	11
1.6	Modern Developments	14
2	Classical Ciphers and Their Cryptanalysis	17
2.1	Introduction	17
2.2	The Caesar Cipher	18
2.3	The Scytale Cipher	20
2.4	The Vigenère Cipher	21
2.5	The Enigma Machine and Its Mathematics	22
2.6	Frequency Analysis	26
2.7	Breaking the Vigenère Cipher, Babbage–Kasiski	26
2.8	Modern Enciphering Systems	31
2.9	Problems	32
2.10	Solutions	33
3	RSA, Key Searches, SSL, and Encrypting Email	39
3.1	Background	41
3.2	The Basic Idea of Cryptography	41
3.3	Public Key Cryptography and RSA on a Calculator	45
3.4	The General RSA Algorithm	48
3.5	Public Key Versus Symmetric Key	51

3.6	Attacks, Security of DES, Key-spaces	54
3.7	Summary of Encryption	56
3.8	SSL (Secure Socket Layer)	57
3.9	PGP and GPG	59
3.10	RSA Challenge	60
3.11	Problems	61
3.12	Solutions	64
4	The Fundamentals of Modern Cryptography	69
4.1	Encryption Revisited	69
4.2	Block Ciphers, Shannon's Confusion and Diffusion	71
4.3	Perfect Secrecy, Stream Ciphers, One-Time Pad	73
4.4	Hash Functions	76
4.5	Message Integrity Using Symmetric Cryptography	79
4.6	General Public Key Cryptosystems	80
4.7	Electronic Signatures	82
4.8	The Diffie-Hellman Key Exchange	84
4.9	Quantum Encryption	87
4.10	Key Management and Kerberos	89
4.11	DES	91
4.12	Problems	92
4.13	Solutions	92
5	DES, AES and Operating Modes	95
5.1	The Data Encryption Standard Code	95
5.2	Triple DES	101
5.3	DES and Unix	102
5.4	The Advanced Encryption Standard Code	102
5.5	Problems	109
5.6	Solutions	110
6	Elliptic Curve Cryptography (ECC)	113
6.1	Abelian Integrals, Fields, Groups	113
6.2	Curves, Cryptography	115
6.3	Nonsingularity	117
6.4	The Hasse Theorem, and an Example	117
6.5	More Examples	118
6.6	The Group Law on Elliptic Curves	119
6.7	Key Exchange with Elliptic Curves	122

6.8	Elliptic Curves mod n	122
6.9	Encoding Plain Text	122
6.10	Security of ECC	123
6.11	More Geometry of Cubic Curves	123
6.12	Cubic Curves and Arcs	124
6.13	Homogeneous Coordinates	124
6.14	Fermat's Last Theorem, Elliptic Curves, Gerhard Frey	125
6.15	Problems	126
6.16	Solutions	126
7	Attacks in Cryptography	131
7.1	Cryptanalysis	131
7.2	Soft Attacks	132
7.3	Brute Force Attacks	133
7.4	Man-In-The-Middle Attacks	134
7.5	Known Plain Text Attacks	135
7.6	Known Cipher Text Attacks	135
7.7	Chosen Plain Text Attacks	136
7.8	Chosen Cipher Text Attacks, Digital Signatures	136
7.9	Replay Attacks	137
7.10	Birthday Attacks	137
7.11	Birthday Attack on Digital Signatures	138
7.12	Birthday Attack on the Discrete Log Problem	139
7.13	Attacks on RSA	139
7.14	Attacks on RSA using Low-Exponents	140
7.15	Timing Attack	141
7.16	Differential Cryptanalysis	142
7.17	Implementation Errors and Unforeseen States	143
8	Practical Issues	145
8.1	Introduction	145
8.2	Hot Issues	146
8.3	Authentication	147
8.4	E-Commerce	151
8.5	E-Government	152
8.6	Key Lengths	153
8.7	Digital Rights	154
8.8	Wireless Networks	154
8.9	Communication Protocols	156

II	Information Theory	159
9	Information Theory and Its Applications	161
9.1	Axioms, Physics, Computation	161
9.2	Entropy	162
9.3	Information Gained, Cryptography	164
9.4	Practical Applications of Information Theory	166
9.5	Information Theory and Physics	167
9.6	Axiomatics of Information Theory	168
9.7	Number Bases, Erdős, and the Hand of God	169
9.8	Weighing Problems and Your MBA	171
9.9	Shannon Bits, the Big Picture	173
10	Random Variables and Entropy	175
10.1	Random Variables	175
10.2	Mathematics of Entropy	178
10.3	Calculating Entropy	179
10.4	Conditional Probability	180
10.5	Bernoulli Trials	184
10.6	Typical Sequences	185
10.7	Law of Large Numbers	186
10.8	Joint and Conditional Entropy	187
10.9	Applications of Entropy	192
10.10	Calculation of Mutual Information	193
10.11	Mutual Information and Channels	194
10.12	The Entropy of $X + Y$	195
10.13	Subadditivity of the Function $-x \log x$	196
10.14	Entropy and Cryptography	196
10.15	Problems	196
10.16	Solutions	198
11	Source Coding, Data Compression, Redundancy	203
11.1	Introduction, Source Extensions	204
11.2	Encodings, Kraft, McMillan	205
11.3	Block Coding, The Oracle, Yes-No Questions	211
11.4	Optimal Codes	212
11.5	Huffman Coding	213
11.6	Optimality of Huffman Coding	218
11.7	Data Compression, Lempel-Ziv Coding, Redundancy	219

11.8 Problems	222
11.9 Solutions	223
12 Channels, Capacity, the Fundamental Theorem	225
12.1 Abstract Channels	226
12.2 More Specific Channels	227
12.3 New Channels from Old, Cascades	228
12.4 Input Probability, Channel Capacity	231
12.5 Capacity for General Binary Channels, Entropy	234
12.6 Hamming Distance	236
12.7 Improving Reliability of a Binary Symmetric Channel	237
12.8 Error Correction, Error Reduction, Good Redundancy	238
12.9 The Fundamental Theorem of Information Theory	241
12.10 Summary, the Big Picture	248
12.11 Problems	248
12.12 Solutions	249
13 Signals, Sampling, SNR, Coding Gain	253
13.1 Continuous Signals, Shannon's Sampling Theorem	253
13.2 The Band-Limited Capacity Theorem, an Example	256
13.3 The Coding Gain	259
14 Ergodic and Markov Sources, Language Entropy	261
14.1 General and Stationary Sources	261
14.2 Ergodic Sources	264
14.3 Markov Chains and Markov Sources	265
14.4 Irreducible Markov Sources, Adjoint Source	269
14.5 Cascades and the Data Processing Theorem	270
14.6 The Redundancy of Languages	271
14.7 Problems	274
14.8 Solutions	275
15 Perfect Secrecy: the New Paradigm	277
15.1 Symmetric Key Cryptosystems	277
15.2 Perfect Secrecy and Equiprobable Keys	279
15.3 Perfect Secrecy and Latin Squares	280
15.4 The Abstract Approach to Perfect Secrecy	282
15.5 Cryptography, Information Theory, Shannon	283
15.6 Unique Message from Ciphertext, Unicity	283

15.7 Problems	284
15.8 Solutions	286
16 Shift Registers (LFSR) and Stream Ciphers	289
16.1 Vernam Cipher, Psuedo-Random Key	290
16.2 Construction of Feedback Shift Registers	290
16.3 Periodicity	293
16.4 Maximal Periods, Pseudo-Random Sequences	296
16.5 Determining the Output from $2m$ Bits	297
16.6 The Tap Polynomial and the Period	300
16.7 Berlekamp–Massey Algorithm	301
16.8 Problems	304
16.9 Solutions	305
17 The Genetic Code	307
17.1 Biology and Information Theory	308
17.2 History of Genetics	308
17.3 Structure of DNA	309
17.4 DNA as an Information Channel	309
17.5 The Double Helix, Replication	310
17.6 Protein Synthesis and the Genetic code	310
17.7 Viruses	312
17.8 Entropy and Compression in Genetics	313
17.9 Channel Capacity of the Genetic Code	314
III Error-Correction	317
18 Error-Correction, Haddamard, Block Designs	319
18.1 General Ideas of Error Correction	319
18.2 Error Detection, Error Correction	320
18.3 A Formula for Correction and Detection	321
18.4 Hadamard Matrices	322
18.5 Mariner, Hadamard and Reed–Muller	325
18.6 Reed–Muller Codes	325
18.7 Block Designs	326
18.8 A Problem of Landar, the Bruen–Ott Theorem	328
18.9 The Main Coding Theory Problem, Bounds	328
18.10 Problems	333
18.11 Solutions	333

19 Finite Fields, Linear Algebra, and Number Theory	335
19.1 Modular Arithmetic	335
19.2 A Little Linear Algebra	339
19.3 Applications to RSA	341
19.4 Primitive Roots for Primes and Diffie-Hellman	342
19.5 The Extended Euclidean Algorithm	345
19.6 Proof that the RSA Algorithm Works	346
19.7 Constructing Finite Fields	346
19.8 Pollard's $p - 1$ Factoring Algorithm	350
19.9 Turing Machines, Complexity, P and NP	351
19.10 Problems	354
19.11 Solutions	355
20 Introduction to Linear Codes	359
20.1 Repetition Codes and Parity Checks	359
20.2 Details of Linear Codes	361
20.3 Parity Checks, the Syndrome, Weights	364
20.4 Hamming Codes, an Inequality	366
20.5 Perfect Codes, Errors and the BSC	367
20.6 Generalizations of Binary Hamming Codes	368
20.7 The Football Pools Problem, Extended Hamming Codes	369
20.8 Golay Codes	370
20.9 McEliece Cryptosystem	371
20.10 Historical Remarks	372
20.11 Problems	373
20.12 Solutions	375
21 Linear Cyclic Codes, Shift Registers and CRC	379
21.1 Cyclic Linear Codes	379
21.2 Generators for Cyclic Codes	381
21.3 The Dual Code and The Two Methods	383
21.4 Linear Feedback Shift Registers and Codes	384
21.5 Finding the Period of an LFSR	386
21.6 Cyclic Redundancy Check (CRC)	387
21.7 Problems	388
21.8 Solutions	390
22 Reed Solomon, MDS Codes, Bruen-Thas-Blokhuis	393
22.1 Cyclic Linear Codes and Vandermonde	394

22.2 The Singleton Bound	396
22.3 Reed–Solomon Codes	397
22.4 Reed–Solomon Codes and the Fourier Transform Approach	398
22.5 Correcting Burst Errors, Interleaving	399
22.6 Decoding Reed–Solomon Codes	400
22.7 An Algorithm for Decoding and an Example	403
22.8 MDS Codes and a Solution of a Fifty Year-Old Problem	405
22.9 Problems	408
22.10 Solutions	408
23 MDS Codes, Secret Sharing, Invariant Theory	411
23.1 General MDS Codes	411
23.2 The Case $k = 2$, Bruck Nets	412
23.3 Upper Bounds on MDS Codes, Bruck-Ryser	414
23.4 MDS Codes and Secret Sharing Schemes	416
23.5 MacWilliams Identities, Invariant Theory	417
23.6 Codes, Planes, Blocking Sets	418
23.7 Binary Linear Codes of Minimum Distance 4	422
24 Key Reconciliation, New Algorithms	423
24.1 Symmetric and Public Key Cryptography	423
24.2 General Background	424
24.3 The Secret Key and the Reconciliation Algorithm	426
24.4 Equality of Remnant Keys: the Halting Criterion	429
24.5 Linear Codes: the Checking Hash Function	431
24.6 Convergence and Length of Keys	433
24.7 Main Results	438
24.8 Some Details on the Random Permutation	439
24.9 The Case Where Eve Has Non-zero Initial Information	441
24.10 Hash Functions Using Block Designs	442
24.11 Concluding Remarks	443
ASCII	445
Shannon’s Entropy Table	447
Glossary	449
Bibliography	454

CONTENTS

xiii

Index

462