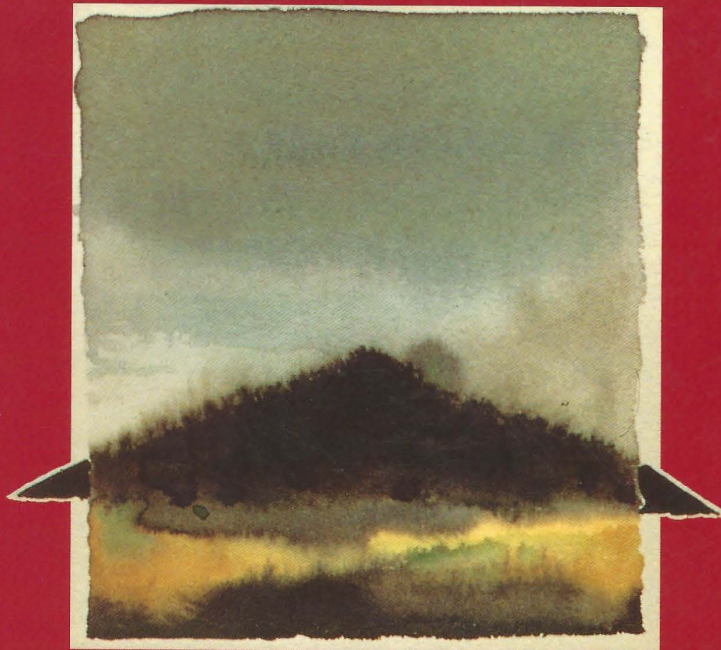


*“... the best introduction
to cryptography I’ve
ever seen.... The book
the National Security
Agency wanted never
to be published...”*

—Wired Magazine

**SECOND
EDITION**

APPLIED CRYPTOGRAPHY



**Protocols, Algorithms,
and Source Code in C**

BRUCE SCHNEIER

**APPLIED CRYPTOGRAPHY,
SECOND EDITION**

PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C

BRUCE SCHNEIER



John Wiley & Sons, Inc.

New York • Chichester • Brisbane • Toronto • Singapore

Publisher: Katherine Schowalter
Editor: Phil Sutherland
Assistant Editor: Allison Roarty
Managing Editor: Robert Aronds
Text Design & Composition: North Market Street Graphics

Designations used by companies to distinguish their products are often claimed as trademarks. In all instances where John Wiley & Sons, Inc. is aware of a claim, the product names appear in initial capital or all capital letters. Readers, however, should contact the appropriate companies for more complete information regarding trademarks and registration.

This text is printed on acid-free paper.

Copyright © 1996 by Bruce Schneier
Published by John Wiley & Sons, Inc.

All rights reserved. Published simultaneously in Canada.

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.

In no event will the publisher or author be liable for any consequential, incidental, or indirect damages (including damages for loss of business profits, business interruption, loss of business information, and the like) arising from the use or inability to use the protocols and algorithms in this book, even if the publisher or author has been advised of the possibility of such damages.

Some of the protocols and algorithms in this book are protected by patents and copyrights. It is the responsibility of the reader to obtain all necessary patent and copyright licenses before implementing in software any protocol or algorithm in this book. This book does not contain an exhaustive list of all applicable patents and copyrights.

Some of the protocols and algorithms in this book are regulated under the United States Department of State International Traffic in Arms Regulations. It is the responsibility of the reader to obtain all necessary export licenses before implementing in software for export any protocol or algorithm in this book.

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.

Library of Congress Cataloging-in-Publication Data:

Schneier, Bruce

Applied Cryptography Second Edition : protocols, algorithms, and source code in C
/ Bruce Schneier.

p. cm.

Includes bibliographical references (p. 675).

ISBN 0-471-12845-7 (cloth : acid-free paper). — ISBN
0-471-11709-9 (paper : acid-free paper)

1. Computer security. 2. Telecommunication—Security measures.

3. Cryptography. I. Title.

QA76.9.A25S35 1996

005.8'2—dc20

95-12398
CIP

Printed in the United States of America
10 9 8 7 6

- 10.6 COMPRESSION, ENCODING, AND ENCRYPTION 226
- 10.7 DETECTING ENCRYPTION 226
- 10.8 HIDING CIPHERTEXT IN CIPHERTEXT 227
- 10.9 DESTROYING INFORMATION 228

PART III CRYPTOGRAPHIC ALGORITHMS

11 MATHEMATICAL BACKGROUND 233

- 11.1 INFORMATION THEORY 233
- 11.2 COMPLEXITY THEORY 237
- 11.3 NUMBER THEORY 242
- 11.4 FACTORING 255
- 11.5 PRIME NUMBER GENERATION 258
- 11.6 DISCRETE LOGARITHMS IN A FINITE FIELD 261

12 DATA ENCRYPTION STANDARD (DES) 265

- 12.1 BACKGROUND 265
- 12.2 DESCRIPTION OF DES 270
- 12.3 SECURITY OF DES 278
- 12.4 DIFFERENTIAL AND LINEAR CRYPTANALYSIS 285
- 12.5 THE REAL DESIGN CRITERIA 293
- 12.6 DES VARIANTS 294
- 12.7 HOW SECURE IS DES TODAY? 300

13 OTHER BLOCK CIPHERS 303

- 13.1 LUCIFER 303
- 13.2 MADRYGA 304
- 13.3 NEWDES 306
- 13.4 FEAL 308
- 13.5 REDOC 311
- 13.6 LOKI 314
- 13.7 KHUFU AND KHAFRE 316
- 13.8 RC2 318
- 13.9 IDEA 319
- 13.10 MMB 325
- 13.11 CA-1.1 327
- 13.12 SKIPJACK 328

14 STILL OTHER BLOCK CIPHERS 331

- 14.1 GOST 331
- 14.2 CAST 334
- 14.3 BLOWFISH 336
- 14.4 SAFER 339
- 14.5 3-WAY 341

14.6	CRAB	342
14.7	SXAL8/MBAL	344
14.8	RC5	344
14.9	OTHER BLOCK ALGORITHMS	346
14.10	THEORY OF BLOCK CIPHER DESIGN	346
14.11	USING ONE-WAY HASH FUNCTIONS	351
14.12	CHOOSING A BLOCK ALGORITHM	354
15 COMBINING BLOCK CIPHERS 357		
15.1	DOUBLE ENCRYPTION	357
15.2	TRIPLE ENCRYPTION	358
15.3	DOUBLING THE BLOCK LENGTH	363
15.4	OTHER MULTIPLE ENCRYPTION SCHEMES	363
15.5	CDMP KEY SHORTENING	366
15.6	WHITENING	366
15.7	CASCADING MULTIPLE BLOCK ALGORITHMS	367
15.8	COMBINING MULTIPLE BLOCK ALGORITHMS	368
16 PSEUDO-RANDOM-SEQUENCE GENERATORS AND STREAM CIPHERS 369		
16.1	LINEAR CONGRUENTIAL GENERATORS	369
16.2	LINEAR FEEDBACK SHIFT REGISTERS	372
16.3	DESIGN AND ANALYSIS OF STREAM CIPHERS	379
16.4	STREAM CIPHERS USING LFSRS	381
16.5	A5	389
16.6	HUGHES XPD/KPD	389
16.7	NANOTEQ	390
16.8	RAMBUTAN	390
16.9	ADDITIVE GENERATORS	390
16.10	GIFFORD	392
16.11	ALGORITHM M	393
16.12	PKZIP	394
17 OTHER STREAM CIPHERS AND REAL RANDOM-SEQUENCE GENERATORS 397		
17.1	RC4	397
17.2	SEAL	398
17.3	WAKE	400
17.4	FEEDBACK WITH CARRY SHIFT REGISTERS	402
17.5	STREAM CIPHERS USING FCSRS	405
17.6	NONLINEAR-FEEDBACK SHIFT REGISTERS	412
17.7	OTHER STREAM CIPHERS	413
17.8	SYSTEM-THEORETIC APPROACH TO STREAM-CIPHER DESIGN	415
17.9	COMPLEXITY-THEMATIC APPROACH TO STREAM-CIPHER DESIGN	416
17.10	OTHER APPROACHES TO STREAM-CIPHER DESIGN	418

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.