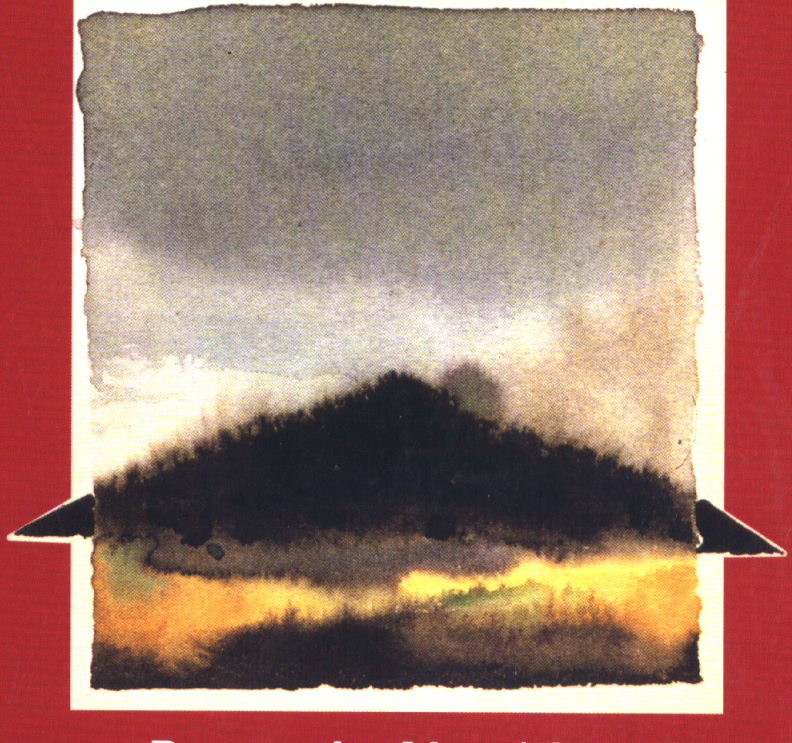
"... the best introduction to cryptography I've ever seen.... The book the National Security Agency wanted never to be published...."
—*Wired* magazine

MORE THAN 100,000 COPIES SOLD

SECOND EDITION

APPLIED CRYPTOGRAPHY



Protocols, Algorithms, and Source Code in C

BRUCE SCHNEIER

from reviews of the first edition of

APPLIED CRYPTOGRAPHY

Protocols, Algorithms, and Source Code in C

". . . the definitive text on the subject. . . ."
—*Software Development Magazine*

". . . good reading for anyone interested in cryptography."
—*BYTE*

"This book should be on the shelf of any computer professional involved in the use or implementation of cryptography."
—*IEEE Software*

". . . dazzling . . . fascinating. . . . This book *absolutely must* be on your bookshelf . . ."
—*PC Techniques*

". . . comprehensive . . . an encyclopedic work . . ."
—*The Cryptogram*

". . . a fantastic book on cryptography today. It belongs in the library of anyone interested in cryptography or anyone who deals with information security and cryptographic systems."
—*Computers & Security*

"An encyclopedic survey . . . could well have been subtitled 'The Joy of Encrypting' . . . a useful addition to the library of any active or would-be security practitioner."
—*Cryptologia*

". . . encyclopedic . . . readable . . . well-informed . . . picks up where Dorothy Denning's classic *Cryptography and Data Security* left off a dozen years ago. . . . This book would be a bargain at twice the price."
—*;login:*

"This is a marvelous resource—the best book on cryptography and its application available today."
—Dorothy Denning
Georgetown University

". . . Schneier's book is an indispensable reference and resource. . . . I recommend it highly."
—Martin Hellman
Stanford University

Errata

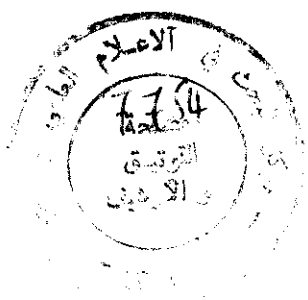
A list of the errors found in this book along with corresponding corrections is updated periodically. For the most recent electronic version, send email to:

schneier@counterpane.com

For the most recent printed version, send a stamped, self-addressed envelope to:

AC Corrections
Counterpane Systems
101 E. Minnekaka Parkway
Minneapolis, MN 55419

Readers are encouraged to distribute electronic or printed versions of this list to other readers of this book.



APPL[illegible]PHY, SECON[illegible]EDITION

PROTOCOLS, ALGO[illegible]SOURCE CODE IN C

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

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
20 19 18 17 16 15 14 13 12

Contents in Brief

Contents

PART II CRYPTOGRAPHIC TECHNIQUES