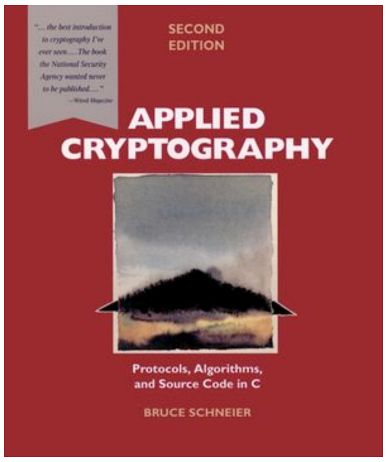

# Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition

Bruce Schneier

| | | | |
|---|---|---|---|
| Paperback | 978-0-471-11709-4 | January 1996 | **CAD $71.99** |

## DESCRIPTION

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

". . .monumental . . . fascinating . . . comprehensive . . . the definitive work on cryptography for computer programmers . . ." -Dr. Dobb's Journal

". . .easily ranks as one of the most authoritative in its field." -PC Magazine

". . .the bible of code hackers." -The Millennium Whole Earth Catalog

This new edition of the cryptography classic provides you with a comprehensive survey of modern cryptography. The book details how programmers and electronic communications professionals can use cryptography-the technique of enciphering and deciphering messages-to maintain the privacy of computer data. It describes dozens of cryptography algorithms, gives practical advice on how to implement them into cryptographic software, and shows how they can be used to solve security problems. Covering the latest developments in practical cryptographic techniques, this new edition shows programmers who design computer applications, networks, and storage systems how they can build security into their software and systems.

What's new in the Second Edition?

* New information on the Clipper Chip, including ways to defeat the key escrow mechanism

* New encryption algorithms, including algorithms from the former Soviet Union and South Africa, and the RC4 stream cipher

* The latest protocols for digital signatures, authentication, secure elections, digital cash, and more

* More detailed information on key management and cryptographic implementations

## ✍ ABOUT THE AUTHOR

**BRUCE SCHNEIER** is President of Counter-pane Systems, a consulting firm specializing in cryptography and computer security. He is a contributing editor to Dr. Dobb's Journal, serves on the board of directors of the International Association of Cryptologic Research, and is a member of the Advisory Board for the Electronic Privacy Information Center. He is the author of E-Mail Security (Wiley) and is a frequent lecturer on cryptography, computer security, and privacy.

To purchase this product, please visit https://www.wiley.com/en-ca/9780471117094