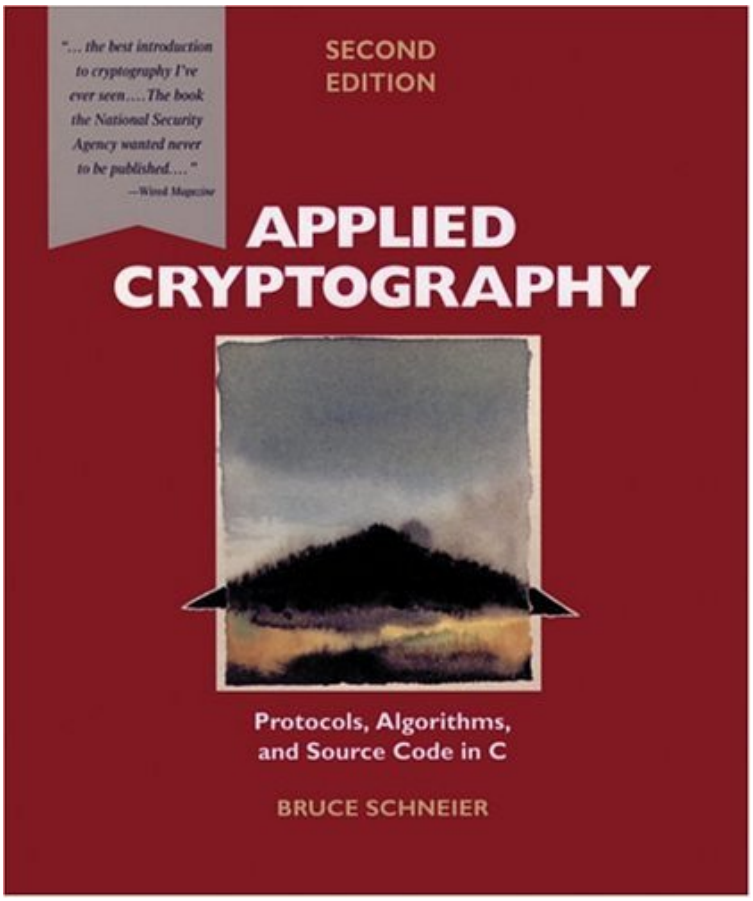
# Applied Cryptography: Protocols, Algorithms, and Source Code in C

*Von Bruce Schneier*
*ebooks | Download PDF | *ePub | DOC | audiobook*






Produktinformation -Verkaufsrang: #429926 in eBooksVerffentlicht am: 2008-04-18Erscheinungsdatum: 2008-04-18File Name: B000SEHPK6 | File size: 24.Mb

**Von Bruce Schneier : Applied Cryptography: Protocols, Algorithms, and Source Code in C** before purchasing it in order to gage whether or not it would be worth my time, and all praised Applied Cryptography: Protocols, Algorithms, and Source Code in C:

KundenrezensionenHilfreichste Kundenrezensionen1 von 1 Kunden fanden die folgende Rezension hilfreich. The most comprehensive text on computer-era cryptology.Von Ein KundeHabitues of sci.crypt will be familiar with Bruce Schneier's*Applied Cryptography*; if any of them have but one text on cryptofor reference, it will almost certainly be *Applied Cryptography*. It is the de facto standard reference on modern cryptography as well as serving as an excellent introduction to the subject. The art is very old - Julius Caesar was the first recorded user of cryptography for military purposes - and reached a watershed when computers were put to work in order to break German and Japanese ciphers. Indeed, that was the first *real* application of electronic computers. A natural development was the use of computers for the development of cryptographic systems. That is where Bruce Schneier's remarkable book begins. It is

notable for two reasons: the breadth and depth of coverage, and the high standard of technical communication. As a reference its scope is encyclopaedic, providing descriptions and assessments of just about every non-military crypto system developed since computers were first applied to the purpose. There are also military-cum-government algorithms amongst the collection, some from the old Soviet Union and others from South Africa. It is not just an A-Z procession of algorithms; the author progresses in a logical manner through the many technical aspects of cryptography. It is common to find that masters of mysterious technical arts are poor communicators. Bruce Schneier demonstrates exceptional skill as a technical communicator. Here is a book about an esoteric subject - one built on a foundation of theoretical mathematics - that ordinary folk can read. Sure, one needs to be motivated by an interest in the subject, and the technical level sometimes requires a more than ordinary background in number theory and the like - but a degree in theoretical mathematics is not necessary to derive pleasure and profit from reading *Applied Cryptography*. A thirty-page chapter provides a brief, but lucid account of the necessary mathematical background, spanning information theory, complexity theory, number theory, factoring, prime number generation, and modular arithmetic. Even if one needs no other information than a useful description of modular arithmetic the book is worth looking at; I can't think of any better source outside full-blown mathematical texts, and the author does it without being obscure. The book is divided into parts, beginning with protocols (the introductory chapter is an excellent overview of crypto as it is presently applied) from the basic kind through to the esoteric that find application in digital cash transactions. Public key encryption, the second - and most significant - watershed in cryptography, is introduced with an explanation of how it is used in hybrid systems. Part II deals with cryptographic techniques and discusses the important issues of key length, key management, and algorithm types. The strength of a crypto system relies very heavily on the length of the key, the way in which it is generated, and key management. A chapter is devoted to the practical aspects of using algorithms (which one, public-key as against symmetric crypto, hardware versus software) for various purposes (such as communications and data storage). Part III is about particular algorithms, providing for each one a background of its development, a description, its security, and how it is likely to stand up to attack. The algorithms are divided into classes: block (some twenty-one are described); pseudo-random-sequence generators and stream ciphers (PKZIP is a stream cipher); real random-sequence generators; one-way hash functions; public-key; public-key digital signature; identification schemes; key-exchange algorithms; and other special algorithms. Many specific algorithms are described with information about covering patents. Part IV is entitled, The Real World; in the words of the author, "It's one thing to design protocols and algorithms, but another thing to field them in operational systems. In theory, theory and practice are the same; in practice they are different". A chapter discusses a number of implementations, including IBM Secret-Key Management Protocol, Mitrenet (an early public-key system), ISDN Packet Data Security Overlay, STU-III, Kerberos, KryptoKnight, Sesame, PEM, PGP, MSP, smart cards, universal electronic payment system, and Clipper. Another chapter discusses politics and puts the problems of US export restrictions into context and deals with patents. It also has information about bodies with an interest in public access to cryptography and standards, and legal issues. An afterword by Matt Blaze should be required reading by everyone who thinks a good cryptosystem is all that one needs for security; the human factor can undo the strongest system. A final part contains C source code for DES, LOKI91, IDEA, GOST, Blowfish, 3-Way, RC5, A5, and SEAL. North American readers can obtain a 3-disk set containing code for some forty-one algorithms, four complete systems, source code for some other utilities, text files, errata, and notes on new protocols and algorithms. Who, apart from crypto professionals and aficionados, is likely to find *Applied Cryptography* of interest? Anyone with an intelligent interest in the art, and who wants something more substantial than a quasi adventure account of modern crypto; anyone with a responsibility for protecting data and/or communications; network administrators; builders of firewalls; students and teachers of computer science; programmers; and anyone with a serious interest in theoretical mathematics - I'm sure the list could be expanded considerably.Apart from a book to be read, it is the most complete and up-to-date resource and reference presently available. The list of references (1653 of them) is a resource in its own right. An essential acquisition for libraries. The book, of necessity, contains highly technical material, but it can be read. The publishers, Wiley's, are to be congratulated. Reviewed by Major Keary majkeary@netspace.net.au DISCLAIMER: The opinions expressed are my own. I have no interest, financial or otherwise, in the success or failure of this book, and - apart from a review copy - I have received no compensation from anyone who has.3 von 3 Kunden fanden die folgende Rezension hilfreich. Pflicht-Kauf in Punkto KryptographieVon www.scip.chBruce Schneier ist neben der von ihm entwickelten Krypto-Algorithmen ebenso fr sein relativ populistisches Fachbuch bekannt. Darin beschreibt er sehr detailliert und bergreifend die Funktionsweise der verschiedenen Protokolle und Methoden. Ein Pflicht-Kauf fr all jene, die sich ernsthaft mit Kryptographie beschftigen mchten. Laut einem Mail-Wechsel mit Schneier (Oktober 2002) wird es keine dritte Auflage dieses Werks geben, da das Thema explodiert ist und nicht mehr in einem einzelnen Band abgehandelt werden knne.1 von 1 Kunden fanden die folgende Rezension hilfreich. The best introduction to cryptography I have readVon owen.cunningham@fmr.comIf you are already a cryppie or other security professional, this book will not add much to your knowledge. But if you are a programmer or other systems person with a desire to familiarize yourself with the field, I can't recommend this book highly enough. A reasonably solid mathematical background is required to fully understand the algorithms, but the book is structured in such a way

that you can skip most of the heavily technical stuff and still get a lot out of the read.Because this is essentially an introductory text, generality is the name of the game. Pretty much everything is covered, but to a low, or medium at best, degree of depth. (Only DES is covered thoroughly.) However, the reference list in the back is huge, and you can use it to easily track down any more detailed information that you're after.

Kurzbeschreibung". . .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.deCryptographic techniques have applications far beyond the obvious uses of encoding and decoding information. For Internet developers who need to know about capabilities, such as digital signatures, that depend on cryptographic techniques, there's no better overview than Applied Cryptography, the definitive book on the subject. Bruce Schneier covers general classes of cryptographic protocols and then specific techniques, detailing the inner workings of real-world cryptographic algorithms including the Data Encryption Standard and RSA public-key cryptosystems. The book includes source-code listings and extensive advice on the practical aspects of cryptography implementation, such as the importance of generating truly random numbers and of keeping keys secure.Pressestimmen"the definitive publicly available text on the theory and practice of cryptography" (Computer Shopper, January 2002)