Dr. Dobb's Essential Books On CRYPTOGRAPHY AND SECURITY

- **Foreword - Bruce Schneier**
- **Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition**
- **Cryptography: A New Dimension in Computer Data Security**
- **Contemporary Cryptology: The Science of Information**
- **Cryptography and Data Security**
- **Applied Cryptography, Cryptographic Protocols, and Computer Security**
- **Cryptography: Theory and Practice**
- **Handbook of Applied Cryptography**
- **Military Cryptanalysis, Volume I-IV**
- **RSA Laboratories FAQ on Cryptography, RSA Laboratories Technical Reports, RSA Laboratories Security Bulletins, and CryptoBytes Newsletter**

Dr. Dobb's CD-ROM LIBRARY

- **COPYRIGHT INFORMATION**

Dr. Dobb's Essential Books On CRYPTOGRAPHY AND SECURITY

- RSA Laboratories
  - Answers to Frequently Asked Questions About Today's Cryptography
  - Laboratories Security Bulletins & Newsletter
  - 512 Bit
  - Introduction to Cryptanalyst

Dr. Dobb's CD-ROM LIBRARY

- COPYRIGHT INFORMATION -

Foreword

by Bruce Schneier,
Contributing Editor
Dr. Dobb's Journal

Historically, cryptography has been used for one thing--to keep secrets. (Written language itself has been used as a form of cryptography. In ancient China, for instance, only the select few were allowed to learn to read and write.) The first documented use of cryptography was in about 1900 BC. In Egypt, a scribe used nonstandard hieroglyphs in an inscription. There are other examples from ancient history: A Mesopotamian tablet from 1500 BC contains an enciphered formula for making pottery glaze. Then there was the Hebrew ATBASH cipher from 500-600 BC, the Greek skytale from 486 BC, and Julius Caesar's simple substitution cipher from 50- 60 BC. The Kama Sutra of Vatsayana lists even lists cryptography as the 44th and 45th of 64 arts men and women should know and practice.

Today it's a completely different world. Public-key cryptography was invented in 1976, and with it came a huge taxonomy of cryptographic primitives--not just algorithms to encrypt data, but public-key encryption, digital signatures and key exchange, one-way hash functions, message authentication codes, weird mathematical systems for things like currency and voting. Today, cryptography is primarily used for authentication--electronic commerce, contracts, obligations, metering. It's found in satellite-TV

decoders, burglar alarms, pre-paid electricity meters, ATMs, and just about every new Internet protocol. It's there to prevent lying and cheating. For good or bad, privacy is almost an afterthought.

The books and papers on this CD-ROM trace this transition of cryptography from simply a means of keeping secrets to a fundamental building block of electronic commerce and online interactions. There are military cryptanalysis manuals from the pre-public-key era of cryptography, including Military Cryptanalysis, Volumes I- IV, by William Friedman (considered by many the father of modern cryptography). There are books written in the early 1980s, when the new world of cryptography was very new, and people had no experience in actually fielding such systems-- Dorothy Denning's Cryptography and Data Security, Stephen Matyas and Carl Meyer's Cryptography: A New Dimension in Computer Data Security, and Richard Demillo's Applied Cryptology, Cryptographic Protocols, and Computer Security Models. There are books tracing the academic development of cryptography, notably Gustavus Simmons's Contemporary Cryptology: The Science of Information Integrity and Doug Stinson's Cryptography: Theory and Practice. There are books that concentrate on the practical implementations of cryptography--Handbook of Applied Cryptography, by Paul Van Oorschot, Scott Vanston, and Alfred Menezes. And there's Applied Cryptography: Protocols, Algorithms, and Source Code in C, which I wrote.

This is the first time that all of these works, along with technical notes and security bulletins leading research labs, have been brought together to be skimmed, read, searched on a single source. There is a lot of knowledge on this unique CD-ROM. I invite you to take advantage of it.

The information included on this CD-ROM is protected by Copyright.

- **Applied Cryptography, Cryptographic Protocols, and Computer Security Models by Richard Demillo. Copyright 1983, American Mathematical Society. All rights reserved.**

- **Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition, by Bruce Schneier. Copyright 1995, John Wiley & Sons, Inc. All rights reserved.**

- **Contemporary Cryptology: The Science of Information Integrity, edited by Gustavus J. Simmons, Copyright 1992, IEEE. All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage and retrieval system, without permission in writing from the IEEE.**

- **Cryptography and Data Security by Dorothy Denning. Copyright 1982, Addison-Wesley Publishing Co., Inc. All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without permission in writing from Addison-Wesley Longman, Inc. Use of this licensed CD-ROM version is subject to the terms of the individual, noncommercial license granted the purchaser of this CD-ROM version.**

- **Cryptography: A New Dimension in Computer Data Security, by Carl Meyer. Copyright 1982, John Wiley &Sons. All rights reserved.**

- **Cryptography: Theory and Practice, by Douglas Stinson., Copyright 1995, CRC Press. All rights reserved.**
- **Handbook of Applied Cryptography, by Paul C. Van Oorschot, Scott A. Vanstone, and Alfred Menezes. Copyright 1996, CRC Press. All rights reserved.**
- **Military Cryptanalysis, Volume I, by William Friedman, Aegean Park Press. All rights reserved**
- **Military Cryptanalysis, Volumes II, by William Friedman, Aegean Park Press. All rights reserved.**
- **Military Cryptanalysis, Volumes III, by William Friedman, Aegean Park Press. All rights reserved.**
- **Military Cryptanalysis, Volumes IV, by William Friedman, Aegean Park Press. All rights reserved.**
- **"RSA Laboratories FAQ on Cryptography," "RSA Laboratories Technical Reports," "RSA Laboratories Security Bulletins," and "CrytoBytes Newsletter" Copyright 1997 RSA Data Security, Inc. All rights reserved.**