# BIBLIOGRAPHY


Allen, Norman, and Thomas B. Polmar, *The Encyclopedia of Espionage*, Gramercy Books, 1997, ISBN 0-517-20269-7. An alphabetical treatment of espionage.

Deavours, Cipher A., David Kahn, Louis Kruh, Greg Mellen, Brian J. Winkel, and Editors, *Selections from Cryptologia: History, People, and Technology*, Artec House, 1998, ISBN 0-89006-862-3. Cryptologic illuminations from the past.

Denning, Dorothy E., *Information Warfare and Security*, Addison-Wesley, 1999, ISBN 0-201-43303-6. Introduction to cyber information warfare.

Diffie, Whitfield, and Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption*, MIT Press, 1998, ISBN 0-262-04167-7. Nontechnical treatment of privacy issues.

Doraswamy, Naganand, and Dan Harkins, *IPSec*, Prentice Hall, 1999, ISBN 0-13-011898-2. Extensive treatment of IPsec.

Feghhi, Jalal, Jalil Feghhi, and Peter Williams, *Digital Certificates: Applied Internet Security*, Addison-Wesley, 1999, ISBN 0-201-30980-7. Extensive treatment of digital certificates.

Kahn, David, *The Codebreakers: The Story of Secret Writing*, Scribner, 1967, ISBN 0-684-83130-9. A comprehensive history of cryptography.

Kaufman, Charlie, Radia Perlman, and Mike Speciner, *Network Security: Private Communication in a Public World*, Prentice Hall, 1995, ISBN 0-13-061466-1. Introduction to cryptography without the extensive mathematics background assumed by other books.

Menezes, A. J., P. C. van Ooschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997, ISBN 0-8493-8523-7. Thorough mathematical cryptographic reference for professional cryptographers.

Nicholos, Randy, *ICSA Guide to Cryptography*, McGraw-Hill, 1999, ISBN 0-07-913759-8. Comprehensive discussion of historical to modern-day cryptography.

Schneier, Bruce, *Applied Cryptography*, *Second Edition*, Wiley, 1996, ISBN 0-471-12845-7. Essential reference for cryptographic engineers by the foremost pundit in the field.

Singh, Simon, *The Code Book*, Doubleday, 1999, ISBN 0-385-49531-5. A historical account of cryptography and a look at the future.

Smith, Richard E., *Internet Cryptography*, Addison-Wesley, 1997, ISBN 0-201-92480-3. In-depth discussion of IPsec and link encryption.

Stallings, William, *Cryptography and Network Security Principles and Practice*, 2d edition, Prentice Hall, 1999, ISBN 0-13-869017-0. Practical discussion of cryptographic principles by a prolific author of networking texts.

Stinson, Douglas R., *Cryptography Theory and Practice*, CRC Press, 1995, ISBN 0-9493-8521-0. In-depth mathematical treatment.

Welsh, Dominic, *Codes and Cryptography*, Oxford University Press, 1988, ISBN 0-19-853287-3. Based on author's mathematics course on information theory.

Wrixon, Fred B., *Codes and Ciphers: An A to Z of Covert Communication from the Clay Tablet to the Mierdot*, Prentice Hall General Reference, 1992, 1st edition (out of print). A summary of cryptographic history in encyclopedia format.

Wrixon, Fred B., *Codes, Ciphers & Other Cryptic & Clandestine Communication: Making and Breaking Secret Messages from Hieroglyphs to the Internet*, Black Dog & Leventhal Publishers, 1998, ISBN 1-57912-040-7. All types of clandestine communication techniques from antiquity to the present, organized by subject matter.

For a more extensive review of most of these and other cryptography books, we recommend www.youdzone.com/cryptobooks.html.

## Articles

Bellovin, Steven M., "Problem Areas for the IP Security Protocols," July 1996, USENIX UNIX Security Symposium, www.usenix.org/publications/library/proceedings/sec96/full_papers/bellovin/bellovin.txt. The cut-and-paste attack.

Bleichenbacker, D. "Chosen Ciphertext Attacks against Protocols Based on RSA PKCS#1," Advances in Cryptology, CRYPTO 98

Marlowe, Lara, "French Banks Panic Over Electronic Cards," March 15, 2000, The Irish Times on the Web, www.ireland.com:80/newspaper/finance/2000/0315/fin18.htm.

Sullivan, Bob, "Can Hackers Kill Credit Cards?" March 15, 2000, MSNBC, www.msnbc.com/news/382141.asp.

Smart Card Integrators, Inc., "Smart Card Information," www.sci-s.com/sub/history.html.

# Internet Resources

Although most sites are listed only once, many of them could be listed in more than one category. All sites are also listed at www.HxMel.com.

## Sites with Many Good Links

| | |
|---|---|
| theory.lcs.mit.edu/~rivest/crypto-security.html#Other | R. Rivest, creator of RSA |
| www.Counterpane.com | B. Schneier, author of *Applied Cryptography* |
| www.cryptography.com/ | SSL 3.0 designer P. Kocher |
| www.infowar.com | Long-time security activist W. Schwartau |
| www.io.com/~ritter/ | Introduction by professional cryptologist T. Ritter |
| www.pbs.org/wgbh/nova/decoding/textindex.html | Public Broadcasting System |

## Standards

| | |
|---|---|
| csrc.ncsl.nist.gov/fips/fips1401.htm | U.S. government standards |
| www.Ietf.org | IETF standards for e-everything |
| www.imc.org | Internet Mail Consortium |
| www.rsasecurity.com/rsalabs/pkcs/ | Public key cryptographic standards |

## U.S. Government

| | |
|---|---|
| csrc.nist.gov/encryption/ | First stopping point |
| gits-sec.treas.gov/krdptut.htm | Government Information Technology Services |
| www.gsa.gov/aces/about.htm | Public key information |
| www.nsa.gov | Information Systems Security Organization |

## Tutorials and Teaching

| | |
|---|---|
| web.mit.edu/network/pgp.html | MIT's PGP distribution site |
| world.std.com/~franl/crypto/ | Has good links as well |
| www.certicom.com | Elliptic curve tutorial |
| www.conceptLabs.co.uk | Introduction to cryptography |
| www.cosc.georgetown.edu/~denning/crypto/ | Cryptographic policy and good links as well |
| www.counterpane.com/insiderisks5.html | Some public key precautions |
| www.cs.adfa.oz.au/teaching/studinfo/csc/lectures/ | Australian military |
| www.hifn.com | Introduction to cryptography and compression |
| www.iks-jena.de/mitarb/lutz/certification/mc/cert.htm | More public key precautions |
| www.math.washington.edu/~koblitz/crlogia.html | Teaching aids by an ECC inventor, N. Koblitz |
| www.microsoft.com/technet/security/kerberos/default.asp | Microsoft Kerberos |
| www.nsa.gov/museum/ | NSA Cryptography Museum |
| www.timestep.com/ | SSL and IPsec articles |
| www.und.nodak.edu/org/crypto/crypto/ | University of North Dakota/American Cryptogram Association |
| www.youdzone.com/rapelcgvba.html | Interactive RSA tutorial and more |

## Applications and Selected Vendors

| | |
|---|---|
| www.baltimore.com | Example of a PKI retailer |
| www.celocom.com/web/celo/d.asp | Example of a digital signature retailer |
| www.checkpoint.com | Example of VPN and firewall builder and seller |
| www.cisco.com/warp/public/759/ | Routers and cryptography |
| www.pgp.com | Two commercial distributors of PGP |
| www.pgpi.com | International PGP site |
| www.smartcardforum.org | Smart cards |
| www.vpnc.org | Virtual private networks |
| www.zks.net | Remaining anonymous with Zero Knowledge |

## Privacy

| | |
|---|---|
| www.computerprivacy.org | Americans for Computer Privacy |
| www.eff.org | Electronic Frontier Foundation |
| www.epic.org | Electronic Privacy Information Center |

## News

| | |
|---|---|
| www.faqs.org/faqs/by-newsgroup/sci/sci.crypt.html | Newsgroup FAQ |
| www.icsa.net | International Computer Security Association |
| www.infosecuritymag.com/ | *Information Security* magazine |
| www.mercurycenter.com/svtech/reports/gmsv/ | Silicon Valley's local newspaper |
| www.nytimes.com | *New York Times* |
| www.pwcglobal.com/cce | PricewaterhouseCoopers |
| www.zdnet.com/zdnn/ecrime/ | ZDNet dedicated site |

## Bankers and Lawyers

| | |
|---|---|
| www.abaecom.com/ | American Bankers Association |
| www.bakerinfo.com/ecommerce | Example of law firm specializing in digital signatures |
| www.bsa.org/policy/encryption/ | Business Software Alliance policy |
| www.digsigtrust.com/ | American Bar Association |
| www.ilpf.org/ | Internet Law & Policy Forum |
| www.mbc.com | Example of law firm specializing in cryptography |

## Computer Code

| | |
|---|---|
| www.attrition.org/~wrlwnd/crypto /crypto_tutorial/ | Tutorials, too |
| www.cryptix.org | Java source code |
| www.cryptography.org | North American Cryptography archives |
| www.ussrback.com | Underground Security Systems Research |

## Miscellaneous

| | |
|---|---|
| www.ams.org | American Mathematical Society |
| www.attlabs.att.co.uk/andyc/enigma/ enigma_j.html | Enigma implemented in Java |
| www.cacr.math.uwaterloo.ca | University of Waterloo Center for Cryptographic Research |
| www.hxMel.com | Cryptographic glossary and AES update |
| www.interhack.net/people/cmcurtin/ snake-oil-faq.html | What to watch out for! |

| | |
|---|---|
| www.isoc.org/internet/history | Internet Society history |
| www.jargon.org | The *New Hacker's Dictionary* |
| www.jya.com/cryptout.htm | Another view |
| www.w3.org/Security/Overview.html | World Wide Web security page |