

# Cryptography Reading Sources

## Books:

### *Cryptography*

- J. A. Buchmann, *Introduction to Cryptography*, Springer 2000 (QA268 .B83 2001, on reserve)
- N. Koblitz, *A Course in Number Theory and Cryptography*, Springer, 2nd ed., 1994 (QA241 .K672, on reserve)
- A. J. Menezes, P. C. van Oorschot & S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 2001 (QA76 .9 .A25 M43, available for free download at <http://www.cacr.uwaterloo.ca/hac/>)
- R. A. Mollin, *An Introduction to Cryptography*, CRC Press 2001 (QA268 .M65, on reserve) (see <http://www.math.ucalgary.ca/~ramollin/cryptopref.html>)
- R. A. Mollin, *RSA and Public Key Cryptography*, CRC Press 2003 (QA268 .M653 2003, on reserve) (see <http://www.math.ucalgary.ca/~ramollin/rsapkcpref.html>)
- D. R. Stinson, *Cryptography: Theory and Practice*, CRC Press (QA268 .S75, on reserve) 1st ed. 1995 (see <http://www.cacr.math.uwaterloo.ca/~dstinson/CTAP.html>), 2nd ed. 2002 (see <http://www.cacr.math.uwaterloo.ca/~dstinson/CTAP2/CTAP2.html>)
- A. Salomaa, *Public Key Cryptography*, Springer, 2nd ed., 1996 (QA76 .9 .A25 S26)
- W. Trapp & L. Washington, *Introduction to Cryptography with Coding Theory*, Prentice Hall 2002 (QA268 .T73 2002, on reserve)

### *Number Theory*

- E. Bach & J. Shallit, *Algorithmic Number Theory*, Vol. I, MIT Press 1996 (QA241 .B23 1996 V.1, on reserve)
- H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer 1999, (QA247 .C546 1993, on reserve) (see <http://www.math.u-bordeaux.fr/~cohen/> for lists of errata)
- R. Crandall & C. Pomerance, *Prime Numbers – a Computational Perspective*, Springer 2001 (QA246 .C73 2001, on reserve)
- H. Riesel, *Prime Numbers and Computer Methods for Factorization*, Birkhuser 1994 (QA246 .R54 1994, on reserve)
- H. C. Williams, *Édouard Lucas and Primality Testing*, Wiley 1998 (QA246 .W55 1998, on reserve)

## Periodicals & Proceedings:

- *Advances in Cryptology* (Proceedings of CRYPTO, EUROCRYPT, ASIACRYPT conferences, QA76 .9 .A25 XXXX)
- *Selected Areas in Cryptography* (SAC) and *Public Key Cryptography* Proceedings (QA76 .A1 L42)
- *Designs, Codes and Cryptography* (QA166.25 INTERNET)
- *Journal of Cryptology* (Z102 .5 .J68).
- *IEEE Transactions on Information Theory* (Q350 .I6)
- *Mathematics of Computation* (QA47 .M42)

## Web Sites

- Cryptography Pointers (<http://www.cs.ut.ee/~helger/crypto/>)
- Ron Rivest's Security Links (<http://theory.lcs.mit.edu/~rivest/crypto-security.html>)

- David Wagner's Crypto Links (<http://www.cs.berkeley.edu/~daw/crypto.html>)
- Cryptography Research, Inc. (<http://www.cryptography.com/resources/>)
- International Association for Cryptologic Research (<http://www.iacr.org>)
- NIST Cryptographic Toolkit (<http://csrc.nist.gov/CryptoToolkit/>)
- AES page (<http://csrc.nist.gov/encryption/aes/>)
- National Security Agency (<http://www.nsa.gov>)
- Bruce Schneiers news letter CRYPTOGRAM (<http://www.counterpane.com/crypto-gram.html>)

### **Recreational Reading**

- D. Kahn, *The Code Breakers*, 1967 (Z103 .K33 1967)
- S. Singh, *The Code Book*, Doubleday 2000 (Z103 .S56 2000)

---

This is by no means an exhaustive list. For further information consult:

<http://faculty.uaeu.ac.ae/~hamdy/cryptology.html>