

**Supplemental Readings**  
**CMSC-443 Cryptology, Alan T. Sherman, Spring 2011, UMBC**

Anderson, Ross, *Security Engineering: A Guide to Building Dependable Distributed Systems*, Wiley (2008), second edition. ISBN 978-0-470-06852-6, QA76.9.A25A54 2008 [A nice guide to security engineering]

Bernstein, Daniel J., Johannes Buchmann, Erik Dahmen, eds., *Post-Quantum Cryptography*, Springer (Berlin 2009). ISBN 978-3-540-88702-7, LC 2008937466 [Offers some alternatives to traditional cryptography to respond to threats from quantum computation]

Bishop, Matt. *Computer Security: Art and Science*, Addison-Wesley (2003). ISBN 0201440997, QA76.9.A25B56 2003

Ferguson, Niels, Bruce Schneier, and Tadayoshi Kohno, *Cryptography Engineering: Design Principles and Practical Applications*, Wiley (Indianapolis, 2010). ISBN 978-0-470-47424-2, LC 2010920648 [A nice guide to practioneers]

Gallager, Robert G., *Information Theory and Reliable Communication*, John Wiley (New York, 1968). ISBN W-471-29048-3 [Classic, thorough textbook on information theory]

Goldreich, Oded, *Foundations of Cryptography, Volume I: Basic Tools*, Cambridge University Press (2001). ISBN 0-521-79172-3 [A rigorous text to modern theoretical cryptography]

Goldreich, Oded, *Foundations of Cryptography, Volume II: Basic Applications*, Cambridge University Press (2004). ISBN 0-521-83084-2

Katz, Jonathan, and Yehuda Lindell, *Introduction to Modern Cryptography*, Chapman & Hall/CRC (Boca Raton, 2008). ISBN 978-1-58488-551-1, QA76.9.A25K36 2007 [An alternative to Stinson's text]

Kolitz, Neil, *A Course in Number Theory and Cryptography*, Springer-Verlag (New York, 1987). ISBN 3-540-96576-9, QA241.K672 1987 [Includes good treatment of elliptic curves]

Menezes, Alfred J., Paul C. van Oorschot, and Scott A. Vanstone, *Handbook of Applied Cryptography*, CDC Press (Boca Raton, 1997). QA76.9.A25M463 1996 [A comprehensive handbook based on material from the Crypto conferences; a good starting point for many topics.]

Schneier, Bruce, *Applied Cryptography* (John Wiley (1996), second edition. ISBN 0-471-12845-7 [A popular accessible introduction]

Shoup, Victor, *A Computational Introduction to Number Theory and Algebra*, Cambridge University Press (Cambridge, UK, 2009), second edition. ISBN 978-0-521-51644-0 [Excellent modern introduction to number theory]

Stinson, Douglas R., *Cryptography: Theory and Practice*, Chapman & Hall/CRC (Boca Raton, 2006), third edition. ISBN 978-1-58488-508-5 [Our text]

### ***Interesting Web Sites***

Pass, Rafael, Introduction to Cryptography

<http://www.cs.cornell.edu/courses/cs4830/2010fa/>

Cryptography [An interesting undergraduate course at Cornell]

wikipedia [Usually has accurate and up-to-date information on many cryptographic topics, with pointers to additional sources.]

Lecture slides from cryptology course at University of Washington:

<http://www.cs.washington.edu/education/courses/csep590/06wi/lectures/>

Michael Fischer, crypto course at Yale

<http://zoo.cs.yale.edu/classes/cs467/2010s/syllabus.html>

Excellent tutorial on elliptic curves:

<http://www.certicom.com/index.php/ecc-tutorial>

<http://courses.csail.mit.edu/6.857/2011/handouts>