Some Cryptography Reading Sources

For an excellent introduction to this material for the general reader, I recommend

- Simon Singh, *The code Book*, Doubleday, 1999

Technical Books

- J. A. Buchmann, *Introduction to Cryptography*, Springer, 2000
- R. A. Mollin, *An Introduction to Cryptography*, CRC Press, 2001
- R. A. Mollin, *RSA and Public-Key Cryptography*, CRC Press, 2002
- A. Salomaa, *Public Key Cryptography*, 2nd ed., 1996, Springer
- D. R. Stinson, *Cryptography: Theory and Practice*, 2nd Edition CRC Press, 2002
- Th.H. Barr, *Invitation to Cryptography*, Prentice Hall, 2001.
- P. Garret, *Making, Breaking Codes: Introduction to Cryptology*, Prentice Hall, 2000.
- W. Trappe and L.C. Washington, *Introduction to Cryptography with Coding Theory*, Prentice Hall, 2002.
- N. Koblitz, *A Course in Number Theory and Cryptography*, 2nd ed. in Graduate Texts in Mathematics, vol. 114, Springer-Verlag, 1994.
- B. Schneier, *Applied Cryptography*, Wiley, 2nd ed., 1996
- A. J. Menezes, P. C. van Oorshot and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997 (Also available for free download at: http://www.cacr.uwaterloo.ca/hac/)

Periodicals

- Advances in Cryptology (Proceedings of CRYPTO, EUROCRYPT, AISACRYPT conferences and others) Springer Lecture Notes in Computer Science
- *Designs, Codes, and Cryptography*, Kluwer Academic Publishers
- *Journal of Cryptology*, Academic Press
- *IEEE Transactions on Information Theory*

This is by no means an exhaustive list. For further information consult:
http://www.math.ucalgary.ca/~hamdy/cryptology.html