## Supplemental Reading

### Selected Textbooks

1. Beker, Henry; and Fred Piper, *Cipher Systems: The Protection of Communications*, John Wiley (New York, 1982).

2. Denning, Dorothy E. R., *Cryptography and Data Security*, Addison-Wesley (Reading, MA, 1983). [Current CMSC-443 text]

3. Rhee, Man Young, *Cryptography and Secure Communications*, McGraw-Hill (Singapore, 1994). [Current CMSC-652 text]

4. Stinson, Douglas R., *Cryptography: Theory and Practice*, CRC Press (Boca Raton, 1994). [in preparation]

### Other Textbooks

5. Brassard, Gilles, *Modern Cryptology: A Tutorial* in Lecture Notes in Computer Science, no. 325, G. Goos and J. Hartmanis, eds., Springer (New York, 1988).

6. Davies, Donald W.; and W. L. Price, *Security for Computer Networks: An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer*, John Wiley (Chichester, England, 1984).

7. Koblitz, Neal, *Number Theory and Cryptography*, Springer (New York, 1987).

8. Konheim, Alan G., *Cryptography: A Primer*, John Wiley (New York, 1981).

9. Meyer, Carl H.; and Stephen M. Matyas, *Cryptology: A New Dimension in Computer Data Security*, John Wiley (New York, 1982).

10. Patterson, Wayne, *Mathematical Cryptography for Computer Scientists and Mathematicians*, Roman and Littlefield (Favage, MD, 1987).

11. Seberry, Jennifer; and Josef Pieprzyk, *Cryptography: An Introduction to Computer Security*, Prentice Hall (Engewood Cliffs, NJ, 1988).

12. van Tilborg, H. C. A., *An Introduction to Cryptology*, Kluwer Academic Publishers (Hingham, MA, 1988).

13. Welsh, Dominic, *Codes and Cryptography*, Oxford University Press (Fairlawn, NJ, 1988).

**Collections**


14. Abrams, Marshall D.; and Harold J. Podell, *Tutorial: Computer and Network Security*, IEEE Computer Society Press (Los Angeles, CA, 1987).

15. Davies, Donald, *ed.*, *Tutorial: The Security of Data in Networks*, IEEE Computer Society Press (Los Angeles, CA, 1981).

16. Deavours, Cipher; David Kahn; Louis Kruh; Greg Mellon; and Brian Winkel, *eds.*, *Cryptology: Yesterday, Today, and Tomorrow*, Archtech House (Norwood, MA, 1987).

17. Longo, G., *ed.*, *Secure Digital Communications*, Springer (Vienna 1983).

18. Simmons, Gustavs J., ed., *Contemporary Cryptology: The Science of Information Integrity*, IEEE Press (1992).


**Fun/Accessible Reading**


19. Beutelspacher, Albrecht, *Cryptology*, transformation from German into English by J. Chris Fisher, The Mathematical Association of America, Spectrum Series (1994). [A modern Sinkov.]

20. Gaines, Helen Fouché, *Cryptanalysis: A Study of Ciphers and Their Solution*, Dover (New York, 1956). [Explanation of hand ciphers and how to break them.]

21. Schneier, Bruce, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, John Wiley (1993). [Written for PC community. Correctness of information not reliable. Second edition in preparation.]

22. Sinkov, Abraham, *Elementary Cryptanalysis, A Mathematical Approach*, The Mathematical Association of America, New Mathematical Library No. 22 (1966). [A delightful book written for gifted high school students.]


**Cryptanalysis**


23. Barker, Wayne G., *Cryptanalysis of the Simple Substitution Cipher with Word Divisions*, Aegean Park Press (Laguna Hills, CA).

24. Callimahos, Lambros D.; and William Friedman, *Military Cryptanalytics*, part II, vols. 1–2, Aegean Park Press (Laguna Hills, CA).

25. Deavours, Cipher; and Louis Kruh, *Machine Cryptography and Modern Cryptanalysis*, Archtech House (Noorwood, MA, 1985).

26. Friedman, William F., *Elements of Cryptanalysis*, Aegean Park Press (Laguna Hills, CA, 1976).

27. Friedman, William F., *Military Cryptanalysis*, Aegean Park Press (Laguna Hills, CA, 1980).

28. Friedman, William; and Lambros D. Callimahos, *Military Cryptanalytics*, part I: vols. 1–2, part II: vols. 1–2, Aegean Park Press (Laguna Hills, CA).

29. Kullbach, Solomon, *Statistical Methods in Cryptanalysis*, Aegean Park Press (Laguna Hills, CA, 1976).

30. Biham, E.; and A. Shamir, *Differential Cryptanalysis of the Data Encryption Standard*, Springer (Berlin, 1993).

**Selected Topics**

31. Cooper, James Arlin, *Computer & Communications Security: Strategies for the 1990's*, McGraw-Hill (New York, 1989).

32. Golomb, Solomon, *Shift Register Sequences*, Aegean Park Press (Laguna Hills, CA, 1982).

33. Kranakis, Evangelos, *Primality and Cryptography*, John Wiley (New York, 1986).

34. Menezes, Alfred J., *Elliptic curve public-key cryptosystems*, Kluwer Academic Publishers (Boston, 1993).

35. Rueppel, Rainer A., *Analysis and Design of Stream Ciphers*, Springer (New York, 1986).

36. Stallings, William, *Network and Internetwork Security: Principles and Practice*, Prentice Hall and IEEE Press (New York, 1995).

37. Wood, Patrick H.; and Stephen G. Kochan, *Unix System Security*, Hayden Book Co.

**Information Theory**

38. Gallager, Robert G., *Information Theory and Reliable Communication*, John Wiley (New York, 1968).

39. Shannon, Claude E.; and Waren Weaver, *The Mathematical Theory of Communication*, University of Illinois Press (Urbana, IL 1980).

**Algorithms and Complexity Theory**

40. Aho, Alfred; John E. Hopcroft; and Jeffrey Ullman, *The Design and Analysis of Computer Algorithms*, Addison-Wesley (Reading, MA, 1974).

41. Cormen Thomas; Charles Leiserson; and Ronald Rivest, *Introduction to Algorithms*, MIT Press (Cambridge, MA, 1989). [There is a nice chapter on number theory and RSA.]

42. Garey, Michael R.; and David S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*, W. H. Freeman (San Francisco, 1979).

43. Hopcroft, John E.; and Jeffrey D. Ullman, *Introduction to Automata Theory, Languages, and Computation*, Addison-Wesley (Reading, MA, 1979).

44. Knuth, Donald E., *The Art of Computer Programming*, Addison-Wesley (Reading, MA, 1973), vols. I–III.

**Discrete Mathematics**

45. Epp, Susanna S., *Discrete Mathematis with Applications*, Wadsworth (Belmont, CA, 1990).
46. Feller, William, *An Introduction to Probability Theory and its Applications*, vol. I, John Wiley (New York, 1968).
47. Herstein, I. N., *Topics in Algebra*, Blaisdell (New York, 1972).
48. Hoel, Paul G.; Port, Sidney C.; and Stone, Charles J., *Introduction to Probability Theory*, Houghton Mifflin (1971).
49. Larsen, Richard J; and Morris L. Marx, *An Introduction to Mathematical Statistics and its Applications*, Prentice-Hall (Englewood Cliffs, N.J., 1981).
50. LeVeque, *Fundamentals of Number Theory*, Addison-Wesley (Reading, MA, 1977).
51. Niven, Ivan; and Herbert S. Zuckerman, *An Introduction to the Theory of Numbers*, John Wiley (New York, 1980).
52. Roberts, Fred, *Applied Combinatorics*, Prentice-Hall (Englewood Cliffs, N.J., 1984).

**History**

53. Bamford, James, *The Puzzle Palace: A Report on NSA, America's most Secret Agency*, Houghton Mifflin (Boston, 1982).
54. Hodges, A., *Alan Turing: The Enigma*, Simon and Schuster (1983).
55. Kahn, David, *Kahn on Codes: Secrets of the New Cryptology*, Macmillan (New York, 1984).
56. Kahn, David, *The Codebreakers: The Story of Secret Writing*, Macmillan (New York, 1967).
57. Kozaczuk, Wladyslav, *Enigma: How the German Machine Cipher was Broken, and How it was Read by the Allies in World War Two*, edited and translated by Christopher Kasparek, University Publications of America (1984).
58. Parrish, T., *The Ultra Americans: The U.S. Role in Breaking Nazi Codes*, Stein and Day (New York, 1986).
59. Welchman, Gordon, *The Hut Six Story, Breaking the Enigma Codes*, McGraw-Hill (New York, 1982).
60. Winterbotham, F. W., *The Ultra Secret*, Futura (1975).

61. Yardly, Herbert O., *The American Black Chamber*, Bobbs-Merrill (1931).

**Journals Devoted to Cryptology**

62. *Journal of Cryptology*, Springer (New York, 1988 to date).

63. *Design, Codes, and Cryptography* Kluwer.

64. *Cryptologia*, published at the Rose-Hulman Institute of Technology (Terre Haute, IN, 1977 to date).

65. *Computers and Security*, Elsevier (New York, 1982 to date).

66. *Security Reviews*, published by Ross Anderson (Cambridge, UK).

**Special Journal Issues Devoted to Cryptology**

67. *ACM Computing Surveys*, **13** (September 1981).

68. *SIGACT News*, **15** (winter–spring 1983).

69. *SIAM Journal on Computing*, **17** (April 1988).

70. *Proceedings of the IEEE*, **76** (May 1988).

**Major Conferences for Technical Cryptology**

71. *Crypto*, sponsored since 1983 by the International Association for Cryptologic Research (1981 to date). 1982 proceedings published by Plenum Press; since 1983, proceedings published by Springer in the series *Advances in Cryptology: Proceedings of Crypto.*

72. *Eurocrypt*, sponsored since 1983 by the International Association for Cryptologic Research (1982 to date). Proceedings published by Springer, since 1984 in the series *Advances in Cryptology: Proceedings of Eurocrypt.* [See also related conferences *Asiacrypt* and *Auscrypt.*]

73. *ACM Conference on Computer and Communications Security*, sponsored by ACM SIGSAC (1993 to date). Proceedings published by ACM Press.

74. *IEEE Symposium on Security and Privacy (SSP)*, sponsored by the IEEE Technical Committee on Security and Privacy (1979 to date). Proceedings published by IEEE Computer Society Press.

75. *IFIP International Conference on Computer Security*, sponsored by the International Federation for Information Processing Technical Committee 11: Security and Protection (1983–present). Proceedings published by North-Holland.