# Appendix D

## Bibliography

1. W F Friedman. "The Index of Coincidence and Its Applications in Cryptography", Riverbank Publication No. 22, Riverbanks Labs, 1920. Reprinted by Aegean Park Press, 1987.
2. E. H. Hebern, "Electronic Coding Machine," U.S. Patent #1,510.441, 30 Sep 1924.
3. C. E. Shannon, "Communication Theory of Secrecy Systems," Bell System Technical Journal, v.28, n.4, 1949, pp. 656 – 715.
4. D. Kahn, *The Codebreakers: The story of Secret Writing*, New York: Macmillan Publishing Co., 1983.
5. J. L. Smith, "The Design of Lucifer A Cryptographic Device for Data Communication," IBM Research Report RC3326, 1971.
6. J. L. Smith, W. A. Notz, and P.R. Osseck, "An Experimental Application of Cryptography to a Remotely Accessed Data System," Proceedings of ACM Annual Conference, August 1972, pp. 282-290.
7. W. Diffie and M.E. Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, v.IT-22, n. 6, Nov 1976, pp. 644 – 654.
8. W. Diffie and M.E. Hellman, "Privacy and Authentication: An Introduction to Cryptography," Proceedings of the IEEE, v. 67, n. 3, Mar 1979, pp. 397-427.
9. L. R. Knudsen, "Block Ciphers – Analysis, Design, Applications," Ph. D. Dissertation, Aarthus University, Nov 1994.
10. P. Wayner, "Mimic Functions," Crytologia, v. 16, n. 3, Jul 1992. pp. 193-214.
11. P. Wayner, "Mimic Functions and Tractability," draft manuscript, 1993.
12. W. F. Friedman, *Elements of Cryptanalysis.* Laguana Hills, CA: Aegean Park Press, 1976.
13. H. F. Gines, *Cryptanalysis.* American Photographic Press, 1937, (Reprinted by Dover Publications, 1956.)
14. E. A. Williams. *An Invitation to Cryptograms*, New York: Simmon and Schuster, 1959.
15. R. Ball, *Mathematical Recreations and Essays.* New York: MacMillan, 1960.
16. A. Sinkov, *Elementary Cryptanalysis*, Mathematical Association of America, 1996.

17. A. Peleg and A. Rosenfield, "Breaking Substitution Ciphers using a Relaxation Algorithm," Communications of ACM, v.22, n. 11, Nov 1979, pp. 598-605.

18. A. G. Konheim, *Cryptography: A Primer*. New York: John Wiley & Sons, 1981.

19. G. W. Hart, "To Decode Short Cryptograms," *Communications of ACM*, v. 37, n. 9, Sep 1994, pp. 102-108.

20. D. Kahn, *The Codebreakers: The Story of Secret Writing*, New York: Macmillan Publishing Co., 1967.

21. F. Pratt, *Secret and Urgent*, Blue Ribbon Books, 1942.

22. W. F. Friedman, *Methods for the Solutions of Running-Key Ciphers*, Riverbank Publication No. 16, Riverbank Labs, 1981.

23. A. Scherbius, "Ciphering Machine," U.S. Patent #1,657,411. 24 Jan 1928.

24. W. G. Barker, Cryptanalysis of the Hagelin Cryptograph, Aegean Park Press, 1977.

25. C.A. Deavours and L. Kruh, Machine Cryptography and Modern Cryptanalysis, Norwood MA: Artech House, 1985.

26. W. Diffie and M.E. Hellman, "Privacy and Authentication: An Introduction to Cryptography," Proceedings of the IEEE, v. 67, n. 3, Mar 1979, pp. 397-427.

27. C. A. Deavours, "Black Chamber: A Column; How the British Broke Enigma," Cryptologia, v. 4, n.3, Jul 1980, pp.129-132.

28. A. G. Konheim, *Cryptography: A Primer*. New York: John Wiley & Sons, 1981.

29. R.L. Rivest, "Statistical Analysis of Hagelin Cryptography," Cryptologia, v. 5, n.1, Jul 1981, pp.27-32.

30. G. Welchman, *The Hut Six Story: Breaking the Enigma Codes*, New York McGraw-Hill, 1982.

31. B. C. W. Hagelin, *The Story of the Hagelin Cryptos*. Cryptologia, v. 18, n.3, Jul 1994, pp.204-242.

32. M. Abadi, J. Feigenbaum, and J. Kilan, "On Hiding Information from an Oracle." Proceedings of 19th ACM Symposium on the Theory of Computing, 1987, pp. 195 – 203.

33. M. Abadi, J. Feigenbaum, and J. Kilan, "On Hiding Information from an Oracle." Journal of Computer and System Sciences, v.39, n. 1, Aug 1989, pp. 21-50.

34. M. Abadi, R. Needham, "Prudent Engineering Practice for Cryptographic Protocols", Research Report 125, Digital Equipment Corporation Systems Research centre, Jun 1994.

35. C. M. Adams, " Simple and Effective Key Scheduling for Effective ciphers, "Workshop on Selected Areas on Cryptography – Workshop Record, Kingston, Ontario, 5-6, May 1994, 129 -129.

36. C. M. Adams and S. E. Tavares, "The Structured Design of Cryptographically Good S-Boxes" Journal of Cryptology v. 3, n. 1, 1990, pp. 27-41.

37. W. Adams and D. Shanks, "Strong Primality Test That are Not Sufficient," Mathematics of Computation, v. 39, 1982, pp. 255-300.

38. B. S. Adiga and P. Shankar, "Modified Lulee Cryptosystem", Electronic Letters v. 21, n. 18, 29 Aug 1985, pp. 794-795.'

39. L. M. Adleman, "A Subexponential Algorithm for the Discrete Logarithm Problem with Application to Cryptography, "Proceedings of IEEE 20th Annual Symposium of Foundations of Computer Science 1979, pp. 55-60..

40. AT & T, "T7001 Random Number Generator", Data Sheet, August 1986.

41. M. Beale and M. F. Monaghan, "Encryption Using Random Boolean Functions," Cryptography and Coding, H. J. Beker and F. C. Piper, Eds., Oxford: Clarendon Press, 1989, pp. 219-230.

42. P. Beauchemin, G. Brassard, C. Crepeau, C. Goutier, and C. Pomerance, "The Generation of Random Numbers that are Probably Prime," Journal of Cryptology, v. 1, n. 1, 1988, pp. 53-64.

43. S. M. Bellovin and M. Merritt, " An Attack on the Interlock Protocol When Used for Authentication," IEEE Transactions on Information Theory, v. 40,n. 1, Jan 1994, pp. 273-275.

44. S. M. Bellovin and M. Merritt, "Cryptographic Protocol for Secure Communications," U.S. Patent #5, 241,599,31 Aug 1993.

45. J. C. Benaloh, "Cryptographic Capsules: A Disjunctive Primitive for Interactive Protocols," Advances in Cryptology – CRYPTO '86 Proceedings, Springer-Verlag, 1987, pp. 213-222.

46. J. C. Benaloh, "Secret Sharing Homorphisms: Keeping Shares of a Secret Secret," Advances in Cryptology – CRYPTO '86 Proceedings, Springer-Verlag, 1987, 251-260.

47. A. Bender and G. Castagnoli, "On the implementation of Elliptic Curve Cryptosystems," Advances in Cryptology – CRYPTO '89 Proceedings, Springer-Verlag, 1990, pp. 186-192.

48. S. Berkovits, "How to Broadcast a Secret," Advances in Cryptology – CRYPTO '91 Proceedings, Springer-Verlag, 1991, pp. 535-541.

49. T. Berson, "Differential Cryptanalysis Mod $2^{32}$ with Applications to MD5," Advances in Cryptology – EUROCRYPT '92 Proceedings, 1992, pp. 71-80.

50. E. Biham and P. C. Kocher, "A Known Plaintext Attack on the PKZIP Encryption," K. U. Leuven Workshop on Cryptographic Algorithms, Springer-Verlag, 1995.

51. M. Bishop, "An Application for a Fast Data Encryption Standard Implementation," Computing Systems, v. 1, n. 3, 1988, pp. 221-254.

52. M. Blaze, and B. Schneier, "The MacGuffin Block Cipher Algorithm," K. U. Leuven Workshops on Cryptographic Algorithms , Springer-Verlag, 1995.

53. M. Blum, and S. Micali, "How to Generate Crytographically-Strong Sequences of Pseudo-Random Bits," SIAM Journal of Computing, v. 13, n. 4, Nov 1984, pp. 850-864.

54. H. Bonnenberg, A. Curiger, N. Felber, H. Kaeslin, and X Lai, "VLSI Implementation of a New Block Cipher," Proceedings of the IEEE International Conference on Computer Design: VLSI in Computers and Processors (ICCD 91), Oct 1991, pp. 510-513.

55. A. Curiger, H. Zimmermann, N. Felber, H. Kaeslin and W. Fichtner, "VINCI: VLSI Implementation of New Block Cipher IDEA," Proceedings of IEEE CICC '93 San Diego, CA, May 1993, pp. 15.5.1 – 15.5.4.

56. A. Curiger and B. Stuber, "Specification for IDEA Chip" Technical Report No. 92/03, Institut fur Integrierte Systeme. ETH Zurich, Feb 1992.

57. G.I. Davida, "Inverse of Elements of a Galois Field," Electronics Letters, v. 8, n. 21, 19 Oct 1972, pp. 518-520.

58. R.C. Fairfield, A. Matusevich, and J. Plany, "AN LSI Digital Encryption Processor (DEP)," IEEE Communications, v. 23, n. 7, Jul 1985, pp. 30-41.

59. P. Finch, "Study of Blowfish Encryption," Ph. D. Dissertation, Department of Computer Science, City University of New York Graduate School and University Center, Feb 1995.

60. S. Goldwasser and J. Kilian, "Almost All Primes Can Be Quickly Certified," Proceedings of the 18th ACM Symposium on the Theory of Computing, 1986, pp. 316-329.

61. P. L'Ecuyer, "Random Numbers of Simulation," Communications of the ACM, v.33, n. 10, Oct 1990, pp. 85-97.

62. G. Mayhew, "A Low Cost, High Speed Encryption System and Method," Proceedings of the 1994 IEEE Computer Society Symposium on Research in Security and Privacy 1994, pp. 147-154.

63. S. B. Morris, "Escrow Encryption," Lecture at MIT Laboratory for Computer Science, 2 June 1994.

64. National Institute of Standards and Technology, "Capstone Chip Technology," 30 Apr 1993.

65. R.L. Rivest, "RSA Chips (Present/Past/Future)," Advances in Cryptology: Proceedings of Eurocrypt 84, Springer-Verlag 1985, pp. 159-168.

66. R.L. Rivest, "The MD4 Message Digest Algorithm," RFC 1321, Apr 1992.

67. R.L. Rivest, "The MD5 Message Digest Algorithm," RFC 1321, Apr 1992.

68. R.L. Rivest, "Dr. Ron Rivest on Difficulty of Factoring," Ciphertext: The RSA Newsletter, v.1, n. 1, 1993, pp. 6,8.

69. R.L. Rivest, "The RC5 Encryption Algorithm," Dr. Dobb's Journal, v.20, n. 1, Jan 1995, pp. 146-148.

70. R.L. Rivest, "The RC5 Encryption Algorithm," K.U. Leuven Workshops on Cryptographic Algorithms, Springer-Verlag, 1995.

71. B. Schneier, "The Blowfish Encryption Algorithm," Dr. Dobb's Journal, v.19, n. 4, Apr 1994, pp. 38-40.

72. B. Schneier, "Protect Your Macintosh, Peachpit Press, 1994.

73. B. Schneier, "The GOST Encryption Algorithm", Dr. Dobb's Journal, v.20, n. 1, Jan 1995, pp. 123-124.

74. B. Yee, "Using Secure Coprocessor," Ph. D. Dissertation, School of Computer Science, Carnegie University, May 1994.

75. D. J. Wheeler and R. Needham, "TEA, A Tiny Encryption Algorithm," Technical Report 355, "Two Cryptographic Notes," Computer Laboratory, University of Cambridge, Dec 1994, pp. 1-3.