Appendix A

References

1. William Stallings, "Cryptography and Network Security", Third Edition, Pearson Education.
2. Bruce Schneier, *Applied Cryptograph.* Second Edition, Protocols, Algorithms, and Source Code in C, John Wiley & Sons Inc., 1996.
3. L.M. Adleman, C. Pomerance and R. S. Rumeley, "On Distinguishing Prime Numbers from Composite Numbers", Annals of Mathematics, v. 117, n. 1, 1983, pp. 173-206.
4. H. Fiestel, "Cryptography and Computer Privacy," Scientific American, v. 228, n.5, May 1973, pp. 15-23.
5. G. B. Agnew, "Random Sources of Cryptographic Systems," Advances in Cryptology: – EURCRYPT '87 Proceedings, Springer Verlag, 1988, pp. 77-81.
6. S. G. AK1 and H. Meijer, "A Fast Pseudo-Random Permutation Generator with Applications to Cryptology," Advances in Cryptology: – EURCRYPT '84 Proceedings, Springer Verlag, 1985, pp. 269-275.
7. W. Alexi, B.Z. Chor, O. Goldreich and C. P. Schnorr. "RSA and Rabin Functions: Certain Parts are as Hard as the Whole", SIAM Journal on Computing, v. 17, n.2, Apr 1988, pp. 194 -209.
8. W. Alexi, B.Z. Chor, O. Goldreich and C. P. Schnorr, "RSA and Rabin Functions: Certain Parts are as Hard as the Whole" Proceedings of the 25th IEEE Symposium on the Foundation of Computer Science, 1984, pp. 449-457.
9. R. J. Anderson, "Why Cryptosystems Fail," 1st ACM Conference on Computer and Communications Security ACM Press, 1993, pp. 215-227.
10. R. J. Anderson, "Why Cryptosystems Fail," Communications of the ACM, v.37, n. 11, Nov 1994, pp. 32-40.
11. J. Anderson, and R. Needham, "Robustness of Principles for Public Key Protocols," Advances in Cryptology: – EURCRYPT '95 Proceedings, Springer Verlag, 1995.
12. C. Asmuth and J. Bloom, "A Modular Approach to Key Safeguarding," IEEE Transactions on Information Theory, v.IT 29, n. 2. Mar 1983, pp. 208-210.
13. S. K. Banerjee, "High Speed Implementation of DES," Computers & Security, v.1, 1982, pp. 261-267.

14. E. Biham and A. Biryukov, "How to Strengthen DES Using Existing Hardware," Advances in Cryptology – ASIACRYPT '94 Proceedings, Springer-Verlag, 1995.

15. E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Crytosystems," Advances in Cryptology – CRYPTO '90 Proceedings, Springer-Verlag, 1991, pp. 2-21.

16. E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Crytosystems," Journal of Cryptology, v. 4, n. 1, 1991, pp. 3-72.

17. E. Biham and A. Shamir, "Differential Cryptanalysis of the Full 16-Round DES," Advances in Cryptology – CRYPTO '92 Proceedings, Springer-Verlag, 1993, pp. 487-496.

18. G. Brassard, "A Note on Complexity of Cryptography," IEEE Transactions on Information Theory, v. IT 25, n. 2, Mar 1979, pp. 232-233.

19. G. Brassard, "Relativized Cryptography," Proceedings of the IEEE 20th Annual Symposium on the Foundations of Computer Science, 1979, pp.383-391.

20. G. Brassard, ""Relativized Cryptography," IEEE Transactions on Information Theory, v. IT 29, n. 6, Nov 1983, pp. 877-894.

21. E. F. Brickell, and A.M. Odlyzko, "Cryptanalysis: A Survey of Recent Results," Proceedings of the IEEE v. 76, n. 5, May 1988. pp. 578-593.

22. E.F. Brikell, and A.M. Odlyzko, "Cryptanalysis: A Survey of Recent Results," Contemporary Cryptology: The Science of Information Integrity, G.J. Simmons, ed., IEEE Press, 1991, pp. 501-540.

23. T.R. Cain, and A.T. Sherman, "How to Break Gifford's Cipher," Proceedings of 2nd Annual ACM Conferences on Computer and Communication Security, ACM Press, 1994, pp. 198-209.

24. J.M. Carroll, "Do-it Yourself Cryptography," Computers and Security, v. 9, n.7, Nov 1990, pp. 613-619.

25. C. Connell, "An Analysis of New-DES: A Modified version of DES," Cryptologia, v. 14, n. 3, July 1990, pp. 217-223.

26. R.H. Cooper, and W. Patterson, "A generalization of Knapsack Method Using Galois Fields," Cryptologia, v. 8, n. 4, Oct 1984, pp. 343-347.

27. D. Coppersmith, "Data Encryption Standard (DES) and its Strength against Attacks," Technical Report RC 18613, IBM T.J. Watson Center, Dec 1992.

28. D. Coppersmith, "Data Encryption Standard (DES) and its Strength against Attacks," IBM Journal of Research and Development, v. 38, n. 3, May 1994, pp. 243-250.

29. C. Cauvreur and J.J. Quisquater, "An Introduction to Fast Generation of Large Prime Numbers," Philips Journal Research, v. 37, n. 5-6, 1982, pp. 231-264.

30. C. Cauvreur and J.J. Quisquater, "An Introduction to Fast Generation of Large Prime Numbers," Philips Journal Research, v. 38, 1983, pp. 77.

31. J. Daemen, and J. Vandewalle, "Block Cipher Based on Modular Arithmetic," Proceedings of Third Symposium on State and Progress of Research in Cryptography, Rome Italy, 15-16 Feb 1993, pp. 80-89.

32. J. Daemen, R. Govaerts, and J. Vandewalle, "A New Approach to Block Cipher Design," Fast Software Encryption, Cambridge Security Workshop Proceedings, Springer-Verlag, 1994, pp. 18-32.

33. D. E. Denning, "Data Encryption Standard: Fifteen Years of Public Scrutiny", Proceedings Sixth Annual Computer Security Applications Conference, IEEE Computer Society Press, 1990.

34. A. Di Porto and W. Wolfowicz, "VINO: A Block Cipher Including Variable Permutations," Fast Software Encryption Cambridge Security Workshop Proceedings, Springer-Verlag, 1994, pp. 205-210.

35. S. Even and O. Goldreich, "DES-Like Functions Can Generate the Alternating Group," IEEE Transactions on Information Theory, v. IT-29. n. 6, Nov 1983, pp. 863-865.

36. S. Even and O. Goldreich, "On the Power of Cascade Ciphers," ACM Transactions on Computer Systems, v. 3, n. 2, May 1985, pp. 108-116.

37. H. Gustafson, E. Dawson and B. Caelli, "Comparison of Block Ciphers," Advances in Cryptology – AUSCRYPT '90 Proceedings, Springer-Verlag 1990, pp. 208-220.

38. X. Lai and J. Massey, "A Proposal for New Block Encryption Standard," Advances in Cryptology – EUROCRYPT '90 Proceedings, Springer-Verlag, 1991, pp. 389-404.

39. Y. Ohnishi "A Study of Data Security," Master's Thesis Tohuku University, Japan 1988.

40. R.L. Rivest, "A Description of a Single-Chip Implementation of RSA Cipher," LAMDA Magazine, v.1, n. 3, 1980, pp. 14- 18.

41. M. J. B. Robshaw, "Block Ciphers" Technical Report TR-601, RSA Laboratories, Jul 1994.

42. B. Schneier, "One-Way Hash Functions," Dr. Dobb's Journal, v.16, n. 9, Sep 1991, pp. 148-151.

43. B. Schneier, "Description of a New Variable-length Key, 64-bit Block Cipher (Blowfish)," Fast software Encryption, Cambridge Security Workshop Proceedings, Springer-Verlag, 1994, pp. 191-204.

44. N. G. Das, "Statistical Methods in Commerce, Accountancy & Economics (Part II)", M. Das & Co.

45. Mandal J. K. and Dutta S., "A Space-Efficient Universal Encoder for Secured Transmission", International Conference on Modelling and Simulation (MS' 2000-Egypt), Cairo, April 11-14, 2000, pp-193-201.

46. Mandal J. K. and Dutta S., "A Universal Encryption Technique", Proceedings of the National Conference of Networking of Machines, Microprocessors, IT and HRD-Need of the Nation in the Next Millennium, Kalyani-741 235, Dist. Nadia, West Bengal, India, November 25-26,1999, pp-B114-B120.

47. Mandal J.K. and Dutta S., "A Universal Bit-Level Encryption Technique", Proceedings of the 7th State Science and Technology Congress, Jadavpur University, West Bengal, India, February 28 - March 1, 2000, pp-INFO2.

48. Dutta S., Mandal J. K., Mal S., "A Multiplexing Triangular Encryption Technique – A move towards enhancing security in E-Commerce", Proceedings of IT Conference (organized by Computer Association of Nepal), 26 and 27 January, 2002, BICC, Kathmandu.

49. Dutta S., Mandal J. K., A Microprocessor Based Cascaded Technique of Encryption, Proceedings of XXXVI Annual Convention, CSI 2001, Science City, Kolkata, November 20-24, 2001, pp. C269-275

50. J K Mandal, S Mal and S Dutta, " Security in E-Business – A Strategic Issue", National Seminar on Emerging Issues and Strategic Options Before Business in the Liberalized Regime", 7th March, 2001, pp 5-6

51. J K Mandal, S Mal and S Dutta, "Aspects of Storage Efficient Security in GIS Data" Workshop on Remote Sensing and GIS for Sustainable Development and Management in the Himalayas and Adjoining Areas" at NBU, West Bengal by Indian Society of Remote Sensing, Kolkata, Chapter, March 8-9, 2002, pp-24

52. S Mal, J K Mandal and S Dutta, "A Microprocessor Based Encoder for Secured Transmission" Conference on Intelligent Computing on VLSI, Kalyani Govt. Engg. College, 1-17 Feb, 2001, pp 164-169

53. S Mal, J K Mandal and S Dutta, "A Cryptographic Model for Secured Transmission of Messages", Proceedings of the National Conference on Applicable Mathematics, WMVC-2001, A.C. College of Commerce, Jalpaiguri, March 17-19,2001, pp-18-21.

54. S. Mal, J K Mandal and S Dutta, "A Microprocessor Based Generalized Recursive Pair Parity Encoder for Secured Transmission", J. Tech., July 2003, Vol. XXXVII, Nos. 1-2, pp. 11-20

55. Mandal J. K., Mal S., Dutta S., A 256 Bit Recursive Pair Parity Encoder for Encryption, accepted for publication in AMSE Journal, France, 2003

56. Michael Welschenbach, "Cryptography in C and C++", APRESS