Referências Bibliográficas

[1] Witten, I.H., Neal, R.M., Cleary, J.G. *Arithmetic coding for data compression*, Communications of the ACM, vol.30, issue 6, pgs. 520-540, 1987. 5.1, 5.2

[2] Burrows M., Wheeler., D.J. *A block sorting lossless data compression algorithm*, Technical Report 124, Digital Equipment Corporation, Palo Alto, California, 1994. 5.1

[3] Carvalho, D.B. *Segurança de Dados com Criptografia: Métodos e Algoritmos*, Express Book, 2000. 3.3

[4] Cormen, T. H., Leiserson, C. E., Rivest, R. L. *Introduction to Algorithms*, The MIT (The Massachusetts Institute of Technology) Press, 1990. 9.2, 9.3.3

[5] Gunter, C.G. *An Universal Algorithm for Homophonic Coding in Advances in Cryptology*, Eurocrypt-88, LNCS, vol. 330, 1988. 1, 3.4, 3.4, 8.2.4

[6] *Gutenberg Project (on-line)*, url: http://www.gutenberg.org. 6.3, 8.3

[7] Huffman, D. *A Method for the Construction of Maximum of Minimum Redundancy Codes*, Proc. IRE, 1098-1101, 1952. 4.2, 9.3.3

[8] Klein, S. T., Bookstein, A., Deerwester, S. *Storing Text Retrieval Systems on CD-ROM: Compression and Encryption Considerations*, ACM Transactions on Information Systems, vol. 7, no. 3, 1989. 5.2, 8.2, 9.3.3

[9] Klein, S.T., Fraenkel, A.S. *Complexity Aspects of Guessing Prefix Codes*, Algorithmica 12 409-419, 1989. 5.2, 9.2, 9.3.3

[10] Klein, S.T. *Skeleton Trees for the Efficient Decoding of Huffman Encoded Texts*, 8th Annual Symposium on Combinatorial Pattern Matching (CPM'97), 65-75, 1997. 9.5

[11] Massey, J.L., Kuhn, Y.J.B., Jendal, H.N. *An Information-Theoretic Treatment of Homophonic Substitution*, In Advances in Cryptology Eurocrypt-89, LNCS, vol. 434, 1989. 1, 3.4, 3.4, 3.4.1, 6.2.1, 7.3.3, 7.3.5, 8.2.4, 8.3

[12] Menezes, A.J., Oorschot, P.C., Vanstone, S.A. *Handbook of Applied Cryptography*, CRC Press, 1997. 2.5

[13] Milidiu, R.L., Mello, C.G., Fernandes J.R. *A Huffman-based text encryption algorithm*, SSI - Computer Security Symposium, 2000. 1, 5.3, 8.2.4

[14] Milidiu, R.L., Mello, C.G, Fernandes J.R. *Adding security to compressed information retrieval systems*, SPIRE - String Processing and Information Retrieval, 2001. 1, 5.3, 8.2.4

[15] Milidiu, R.L., Mello, C.G, Fernandes J.R. *Substituição Homofônica Rápida via Códigos de Huffman Canônicos*, Wseg - Workshop on Computer Systems Security, 2001. 1, 5.3, 8.2.4

[16] Milidiu, R.L., Laber, E.S., Moreno, L.O., Duarte, D.C. *A Fast Decoding Method for Prefix Codes*, Proceedings of DCC'03, pp.438, 2003. 1, 5.3, 10

[17] Milidiu, R.L., Mello, C.G. *Introducing security into prefix-free encoding schemes*, PUC-RioInf.MCC19/03 July, 2003. 1, 5.3, 10

[18] Milidiu, R.L., Mello, C.G. *Ramdomized Huffman codes*, PUC-RioInf.MCC49/04 December, 2004. 1, 3.4.1, 5.3

[19] Milidiu, R.L., Mello, C.G. *Adding Security to Prefix Codes*, PUC-RioInf.MCC50/04 December, 2004. 1, 5.3

[20] Milidiu, R.L., Mello, C.G. *A provably secure crypto-compression algorithm*, CIBSI 05 - 3o Congreso Iberoamericano de Seguridad Informática, Chile, 2005. 1, 5.3

[21] Milidiu, R.L., Mello, C.G. *Crypto-compression prefix coding*, DCC 2006 - Data Compression Conference, USA, 2006. 1, 5.3

[22] Moffat, A., Witten, I.H., Bell T.C. *Managing Gigabytes: Compressing and Indexing Documents and Images, second edition*, Academic Press, 1999. 1, 4.3.1, 5.1, 7.3.3, 7.4.3, 7.6, 9.2

[23] Moura, E., Navarro, G., and Ziviani, N. *Indexing compressed text*, Proceedings of the 4th South American Workshop on String Processing, 1997. 9.2, 9.5

[24] Nechvatal, J., Barker, E., Bassham, L. et al. *Report on the Development of the AES*, Computer Security Division, NIST IT Lab, 2000. 9.3.3

[25] Pessoa, A.A. *Construção Eficiente de Códigos Livres de Prefixo*, Dissertação de Mestrado, PUC-RJ, 1999. 7.6

[26] NIST. *A statistical test suite for random and pseudorandom number generators for cryptographic applications*, NIST Special Publication 800-22, 2001. 8.2.4, 8.3, 8.4

[27] NIST. *Advanced Encryption Standard (AES)*, Web page: http:csrc.nist.gov/encryption/aes/aes_home.htm 8.2.3

[28] Rivest, R.L., Mohtashemi, M., Gillman, D.W. *On Breaking a Huffman Code*, IEEE Transactions on Information Theory, vol. 42, no. 3, 1996. 5.2, 8.2.4, 9.3.1, 9.3.2, 9.3.3

[29] Schneier, B. *Applied Cryptography Second Edition: Protocols, Algorithms, and Source Code in C*, John Wiley & Sons, 1996. 3.5, 3.6, 3.8, 8.2.3

[30] Shannon, C. *Communication Theory of Secrecy Systems*, Bell Syst. Tech., vol. 28, no. 4, pp. 656-715, 1949. 2.4, 3.2.2, 7.3

[31] Stinson, D. *Cryptography: Theory and Practice*, CRC Press, 1995. 3.2.1

[32] Schneier, B. *Applied Cryptography Second Edition: protocols, algoritms and source code in C*, John Wiley & Sons, 1996. 3.2.1

[33] Wayner, P. *A Redundancy Reducing Cipher*, Cryptologia, 107-112, 1988. 5.2

[34] deMoura, Navarro, Ziviani, Baeza-Yates *Fast and Flexible Word Searching on Compressed Text*, ACM Trans Info Syst, 2000. 8.3

[35] Zobel, J., Williams, H.E. *Compact In-Memory Models for Compression of Large Text Databases*, SPIRE - String Processing and Information Retrieval, 1999. 9.5, 10