Bibliographie

[BD00] Dan Boneh and Glenn Durfee. Cryptanalysis of rsa with private key d less than $n^0.292$. *IEEE Transactions on Information Theory*, 46(4) :1339–1349, 2000.

[BM12] Gilles Bailly-Maitre. *Arithmétique et cryptologie*. Références sciences. Ellipses Marketing, 2012.

[BSTW86] Jon Louis Bentley, Daniel D. Sleator, Robert E. Tarjan, and Victor K. Wei. A locally adaptive data compression scheme. *Commun. ACM*, 29(4) :320–330, April 1986.

[Buc02] Johannes Buchmann. *Introduction to Cryptography*. Springer, 2002.

[CH86] Gordon V. Cormack and R. Nigel Horspool. Data compression using dynamic markov modelling. *The Computer Journal*, 30 :541–550, 1986.

[Cop94] Don Coppersmith. The data encryption standard (des) and its strength against attacks. *IBM Journal of Research and Development*, 38(3) :243–250, 1994.

[CT06] T.M. Cover and J.A. Thomas. *Elements of information theory*. Wiley-Interscience, 2006.

[CW84] John G. Cleary and Ian H. Witten. Data compression using adaptive coding and partial string matching. *IEEE Transactions on Communications*, 32(4) :396–402, April 1984.

[Fri87] William F. Friedman. *The index of coincidence and its applications in cryptanalysis*. Number 49 in A cryptographic series. Aegean Park Press, 1987.

[Gal78] Robert G. Gallager. Variations on a theme by huffman. *IEEE Transactions on Information Theory*, 24(6) :668–674, 1978.

[Gui03] Yann Guidon. Data compression : the "3r" algorithm. `http://ygdes.com/ddj-3r/ddj-3r_compact.html`, 2003.

[Kon07] Alan G. Konheim. *Computer Security and Cryptography*. Wiley-Interscience, New Jersey, 2007.

[Pap91] A. Papoulis. *Probability, random variables, and stochastic processes*. McGraw-Hill, 1991.

[Pub99] Federal Information Processing Standards Publication. Fips pub 46-3 "data encryption standard", October 1999.

[RM89] Jorma Rissanen and Kottappuram Mohammed Mohiuddin. A multiplication-free multialphabet arithmetic code. *IEEE Transactions on Communications*, 37(2) :93–98, 1989.

[Say06] Khalid Sayood. *Introduction to data compression*. Elsevier, Boston, 2006.

[Sha49] Claude Shannon. Communication theory of secrecy systems. *Bell Systems Techn. Journal*, 28 :656–719, 1949.

[SMB10] David Salomon, Giovanni Motta, and David Bryant. *Handbook of data compression*. Springer, London, 2010.

[SS82] James A. Storer and Thomas G. Szymanski. Data compression via textual substitution. *J. ACM*, 29(4) :928–951, October 1982.

[Sti06] Douglas Stinson. *Cryptography : Theory and Practice, Third Edition*. Chapman & Hall, CRC, 2006.

[Wel84] T. A. Welch. A technique for high performance data compression. *IEEE Trans. on Computer*, 17(6) :8–19, 1984.

[ZL77] Jacob Ziv and Abraham Lempel. A universal algorithm for sequential data compression. *IEEE Transactions on Information Theory*, 23 :337–343, 1977.

[ZL78] Jacob Ziv and Abraham Lempel. Compression of individual sequences via variable-rate coding. *IEEE Transactions on Information Theory*, 24(5) :530–536, 1978.