Références

[1] T. Autret, L. Bellefin et M.-L. Oble-Laffaire – *Sécuriser ses échanges électroniques avec une pki*, Eyrolles, 2002.

[2] E. Bach et J. Shallit – *Algorithmic number theory*, vol. 1, MIT Press, 1996.

[3] D. Baker et H. X. Mel – *La cryptographie décryptée*, CampusPress, 2001.

[4] J.-P. Barthélemy, G. Cohen et A. Lobstein – *Complexité algorithmique et problèmes de communications*, Masson, 1992.

[5] P. Barthélemy, R. Rolland et P. Véron – *Cryptographie principes et mises en œuvre*, Lavoisier, 2005.

[6] — , *Cryptographie : principes et mises en œuvre - 2e édition revue et augmentée*, Lavoisier, 2012.

[7] F. Bauer – *Decrypted secrets : methods and maxims of cryptology*, Springer-Verlag, 1997.

[8] A. Bensoussan, S. Martin et I. Pottier – *Cryptologie et signature électronique : aspects juridiques*, Hermès, 1999.

[9] E. Biham et A. Shamir – *Differential cryptanalysis of data encryption standard*, Springer-Verlag, 1993.

[10] H. Cohen – *A course in computational algebraic number theory*, Springer-Verlag, 1993.

[11] H. Cohen, G. Frey et R. Avanzi – *Handbook of elliptic and hyperelliptic curve cryptography : Theory and practice*, Chapman & Hall, 2005.

[12] R. Crandall et C. Pomerance – *Prime numbers : a computational perspective*, Springer-Verlag, 2001.

[13] J. Daemen et V. Rijmen – *The design of rijndael : Aes - the advanced encryption standard*, Springer-Verlag, 2002.

[14] I. Damgård – *Lectures on data security*, Lecture Notes in Computer Science, vol. 1561, Springer-Verlag, 1999.

[15] H. Delfs et H. Knebl – *Introduction to cryptography : principles and applications*, Springer-Verlag, 2002.

[16] M. Demazure – *Cours d'algèbre : primalité, divisibilité, codes*, Cassini, 1997.

[17] J.-G. Dumas, E. Tannier et J.-L. Roch – *Théorie des codes, compression, cryptage, correction*, Dunod, 2007.

[18] C. Féral-Schuhl – *Cyberdroit. le droit à l'épreuve de l'internet*, 3e éd., Dunod, 2002.

[19] O. Goldreich – *Modern cryptography, probabilistic proofs and pseudorandomness*, Springer-Verlag, 1999.

[20] — , *The Foundations of Cryptography, volume i*, Cambridge University Press, 2001.

[21] — , *The Foundations of Cryptography, volume ii*, Cambridge University Press, 2004.

[22] P. Guillot – *Courbes elliptiques, une présentation élémentaire pour la cryptographie*, Lavoisier, 2010.

[23] D. Hankerson, A. Menezes et S. Vanstone – *Guide to elliptic curve cryptography*, Springer-Verlag, 2004.

[24] J. Hirschfeld, G. Korchmáros et F. Torres – *Algebraic Curves over a Finite Field*, Princeton University Press, 2008.

[25] D. Kahn – *La guerre des codes secrets*, InterEditions, 1980.

[26] A. Knapp – *Elliptic curves*, Princeton University Press, 1992.

[27] N. Koblitz – *A course in number theory and cryptography*, Springer-Verlag, 1994.

[28] — , *Algebraic aspects of cryptography*, Springer-Verlag, 1998.

[29] R. Kumanduri et C. Romero – *Number theory with computer applications*, Prentice Hall, 1998.

[30] E. Larcher – *L'internet sécurisé*, Eyrolles, 2000.

[31] R. Lidl et H. Niederreiter – *Finite fields*, second éd., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997.

[32] M. Luby – *Pseudorandomness and cryptographic applications*, Princeton University Press, 1996.

[33] F. J. MacWilliams et N. J. A. Sloane – *The theory of error-correcting code*, North-Holland, 1977.

[34] W. Mao – *Modern cryptography*, Hewlett-Packard Company, 2004.

[35] B. Martin – *Codage, cryptologie et applications*, Presses Polytechniques et Universitaires Romandes, 2004.

[36] A. Menezes, P. van Oorschot et S. Vanstone – *Handbook of applied cryptography*, CRC Press, 1997.

[37] O. Papini et J. Wolfmann – *Algèbre discrète et codes correcteurs*, Springer-Verlag, 1995.

[38] R. Pastor-Satorras et A. Vespignani – *L'internet, structure et évolution*, Belin, 2004.

[39] J. Pieprzyk, T. Hardjono et J. Seberry – *Fundamentals of computer security*, Springer-Verlag, 2003.

[40] G. Pujolle – *Sécurité wi-fi*, Eyrolles, 2004.

[41] T. Saint Denis – *Bignum math : Implementing cryptographic multiple precision arithmetic*, Syngress, 2010.

[42] G. Schäfer – *Security in fixed and wireless networks : An introduction to securing data communications*, Wiley, Décembre 2003.

[43] B. Schneier – *Cryptographie appliquée*, International Thomson Publishing France, 1995.

[44] N. Sendrier – *Cryptosystèmes à clé publique basés sur les codes correcteurs d'erreurs*, Habilitation à diriger des recherches, Inria, 2002.

[45] J. Silverman – *The arithmetic of elliptic curves*, Springer-Verlag, 1986.

[46] S. Singh – *Histoire des codes secrets*, Éditions Jean-Claude Lattès, 1999.

[47] N. Smart – *Cryptography : an introduction*, MacGraw-Hill, 2003.

[48] W. Stallings – *Cryptography and network security, principles and practices*, Prentice Hall, 2003.

[49] M. Stamp et R. Low – *Applied cryptanalysis : Breaking ciphers in the real world*, John Wiley, 2007.

[50] J. Stern – *La science du secret*, Éditions Odile Jacob, 1998.

[51] D. Stinson – *Cryptographie théorie et pratique*, International Thomson Publishing France, 1996.

[52] C. Tavernier – *Les cartes à puce*, Dunod, 2002.

[53] S. Vaudenay – *A classical introduction to cryptography*, Springer, 2006.

[54] D. Vergnaud – *Exercices et problèmes de cryptographie*, Dunod, 2012.

[55] I. Woungang, S. Misra et S. C. Misra (éds.) – *Selected topics in information and coding theory*, Series on Coding Theory and Cryptology, vol. 7, World Scientific, 2010.

[56] G. Zemor – *Cours de cryptographie*, Cassini, 2000.