

Références

- [1] T. AUTRET, L. BELLEFIN & M.-L. OBLE-LAFFAIRE – *Sécuriser ses échanges électroniques avec une pki*, Eyrolles, 2002.
- [2] E. BACH & J. SHALLIT – *Algorithmic number theory*, vol. 1, MIT Press, 1996.
- [3] D. BAKER & H. X. MEL – *La cryptographie décryptée*, CampusPress, 2001.
- [4] J.-P. BARTHÉLEMY, G. COHEN & A. LOBSTEIN – *Complexité algorithmique et problèmes de communications*, Masson, 1992.
- [5] P. BARTHÉLEMY, R. ROLLAND & P. VÉRON – *Cryptographie principes et mises en œuvre*, Lavoisier, 2005.
- [6] F. BAUER – *Decrypted secrets : methods and maxims of cryptology*, Springer-Verlag, 1997.
- [7] A. BENSOUSSAN, S. MARTIN & I. POTTIER – *Cryptologie et signature électronique : aspects juridiques*, Hermès, 1999.
- [8] E. BIHAM & A. SHAMIR – *Differential cryptanalysis of data encryption standard*, Springer-Verlag, 1993.
- [9] H. COHEN – *A course in computational algebraic number theory*, Springer-Verlag, 1993.
- [10] H. COHEN, G. FREY & R. AVANZI – *Handbook of elliptic and hyperelliptic curve cryptography : Theory and practice*, Chapman & Hall, 2005.
- [11] R. CRANDALL & C. POMERANCE – *Prime numbers : a computational perspective*, Springer-Verlag, 2001.
- [12] J. DAEMEN & V. RIJMEN – *The design of rijndael : Aes - the advanced encryption standard*, Springer-Verlag, 2002.
- [13] I. DAMGÅRD – *Lectures on data security*, Lecture Notes in Computer Science, vol. 1561, Springer-Verlag, 1999.
- [14] H. DELFS & H. KNEBL – *Introduction to cryptography : principles and applications*, Springer-Verlag, 2002.
- [15] M. DEMAZURE – *Cours d'algèbre : primalité, divisibilité, codes*, Cassini, 1997.
- [16] J.-G. DUMAS, E. TANNIER & J.-L. ROCH – *Théorie des codes, compression, cryptage, correction*, Dunod, 2007.
- [17] C. FÉRAL-SCHUHL – *Cyberdroit. le droit à l'épreuve de l'internet*, 3e éd., Dunod, 2002.
- [18] O. GOLDBREICH – *Modern cryptography, probabilistic proofs and pseudo-randomness*, Springer-Verlag, 1999.
- [19] — , *The Foundations of Cryptography, volume i*, Cambridge University Press, 2001.

- [20] — , *The Foundations of Cryptography, volume ii*, Cambridge University Press, 2004.
- [21] P. GUILLOT – *Courbes elliptiques, une présentation élémentaire pour la cryptographie*, Lavoisier, 2010.
- [22] D. HANKERSON, A. MENEZES & S. VANSTONE – *Guide to elliptic curve cryptography*, Springer-Verlag, 2004.
- [23] J. HIRSCHFELD, G. KORCHMÁROS & F. TORRES – *Algebraic Curves over a Finite Field*, Princeton University Press, 2008.
- [24] D. KAHN – *La guerre des codes secrets*, InterEditions, 1980.
- [25] A. KNAPP – *Elliptic curves*, Princeton University Press, 1992.
- [26] N. KOBLITZ – *A course in number theory and cryptography*, Springer-Verlag, 1994.
- [27] — , *Algebraic aspects of cryptography*, Springer-Verlag, 1998.
- [28] R. KUMANDURI & C. ROMERO – *Number theory with computer applications*, Prentice Hall, 1998.
- [29] E. LARCHER – *L'internet sécurisé*, Eyrolles, 2000.
- [30] R. LIDL & H. NIEDERREITER – *Finite fields*, second éd., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997.
- [31] M. LUBY – *Pseudorandomness and cryptographic applications*, Princeton University Press, 1996.
- [32] F. J. MACWILLIAMS & N. J. A. SLOANE – *The theory of error-correcting code*, North-Holland, 1977.
- [33] W. MAO – *Modern cryptography*, Hewlett-Packard Company, 2004.
- [34] B. MARTIN – *Codage, cryptologie et applications*, Presses Polytechniques et Universitaires Romandes, 2004.
- [35] A. MENEZES, P. VAN OORSCHOT & S. VANSTONE – *Handbook of applied cryptography*, CRC Press, 1997.
- [36] O. PAPINI & J. WOLFMANN – *Algèbre discrète et codes correcteurs*, Springer-Verlag, 1995.
- [37] R. PASTOR-SATORRAS & A. VESPIGNANI – *L'internet, structure et évolution*, Belin, 2004.
- [38] J. PIEPRZYK, T. HARDJONO & J. SEBERRY – *Fundamentals of computer security*, Springer-Verlag, 2003.
- [39] G. PUJOLLE – *Sécurité wi-fi*, Eyrolles, 2004.
- [40] T. SAINT DENIS – *Bignum math : Implementing cryptographic multiple precision arithmetic*, Syngress, 2010.
- [41] G. SCHÄFER – *Security in fixed and wireless networks : An introduction to securing data communications*, Wiley, Décembre 2003.

- [42] B. SCHNEIER – *Cryptographie appliquée*, International Thomson Publishing France, 1995.
- [43] N. SENDRIER – *Cryptosystèmes à clé publique basés sur les codes correcteurs d’erreurs*, Habilitation à diriger des recherches, Inria, 2002.
- [44] J. SILVERMAN – *The arithmetic of elliptic curves*, Springer-Verlag, 1986.
- [45] S. SINGH – *Histoire des codes secrets*, Éditions Jean-Claude Lattès, 1999.
- [46] N. SMART – *Cryptography : an introduction*, MacGraw-Hill, 2003.
- [47] W. STALLINGS – *Cryptography and network security, principles and practices*, Prentice Hall, 2003.
- [48] M. STAMP & R. LOW – *Applied cryptanalysis : Breaking ciphers in the real world*, John Wiley, 2007.
- [49] J. STERN – *La science du secret*, Éditions Odile Jacob, 1998.
- [50] D. STINSON – *Cryptographie théorie et pratique*, International Thomson Publishing France, 1996.
- [51] C. TAVERNIER – *Les cartes à puce*, Dunod, 2002.
- [52] S. VAUDENAY – *A classical introduction to cryptography*, Springer, 2006.
- [53] I. WOUNGANG, S. MISRA & S. C. MISRA (éds.) – *Selected topics in information and coding theory*, Series on Coding Theory and Cryptology, vol. 7, World Scientific, 2010.
- [54] G. ZEMOR – *Cours de cryptographie*, Cassini, 2000.