

Notes et Références

[Buc06] J. Buchmann, “Introduction à la cryptographie”, DUNOD, 2006.

[Chi10] N. Chikouche, “Problèmes de sécurité dans les systèmes embarqués”, mémoire de magister, Université de M’sila, 2010.

[ChiC11] N. Chikouche, support de cours, master 1, Université de M’sila, 2010.

[Hor07] H. Hordegen, “Vérification des protocoles cryptographiques”, Comparaison des modèles symboliques avec une application des résultats — Etude des protocoles récursifs,” Thèse de Doctorat, Département de formation doctorale en informatique Ecole doctorale IAEM Lorraine, université Henri Poincaré – Nancy 1, 2007.

[Géné] “Générateur de nombres pseudo-aléatoires”, Site : http://fr.wikipedia.org/wiki/G%C3%A9n%C3%A9rateur_de_nombres_pseudo-al%C3%A9atoires#Historique_du_d.C3.A9veloppement_des_g.C3.A9n.C3.A9rateurs_pseudo-al.C3.A9atoires, Dernière modification de cette page le 11 mai 2012 à 21:39.

[Cryp] “Cryptology”, <Http://dictionnaire.phpmyvisites.net/definition-CRYPTOGRAPHIE-4339.htm>.

[InCr-09] “Initiation à la Cryptologie”, @rrobe, Mars 2009.

[Opé] “Opérateurs bit à bit, http”, [//bien-programmer.forum-actif.net.24/04/2009](http://bien-programmer.forum-actif.net.24/04/2009).

[Hug] H. Etiévant, “Génération de variables aléatoires avec l’API Random”, Dernière mise à jour : 20 mai 2004. <ftp://ftp-developpez.com/cyberzoide/java/random.pdf>

[Con] “Concaténation”, <http://fr.wikipedia.org/wiki/Concat%C3%A9nation#D.C3.A9finition>, Dernière modification de cette page le 26 mars 2012 à 13:43

[DH76] W. Diffie and M. E. Hellman, “New Directions in Cryptography,” IEEE Transactions on Information Theory, vol. 22(6), p.p.644-654, November 1976.

[NS78] R. Needham and M. Schroeder, “Using encryption for authentication in large networks of computers,” Communications of the ACM, vol. 1(12), pp.993–999, 1978.

[Rid]: “Radio-identification”, <http://fr.wikipedia.org/wiki/>.

[RF-p] “Radio Frequency Identification RFID”, dans le domaine de la logistique et de la traçabilité.

[RRe] “RFID_REE_J”, http://www.futura-sciences.com/fr/definition/t/informatique-3/d/simulation-informatique_11319/.

[NSer05] N. Seriot, “Les systèmes d’identification radio (RFID)”, Yverdon-les-Bains, 13 janvier 2005, seriot.ch/resources/talks_papers/rfid/rfid.pdf

- [SS07] P. Sood, and T. Sadek, “RFID – Applications Based Approach to Policy”, In 29th International conference of data protection and privacy commissioners, Office of the Privacy Commissioner of Canada. pp. 6-42, 2007.
- [Mah07] L.Mahdaoui, N.ABDT, “Pratique des systèmes d’informations UML outil du génie logiciel”, 2007.
- [Uap09] “UML 2-de l’apprentissage la pratique (cours et exercices)”, édition Ellipses, 2009.
- [Mu97] P-A.Muller, “Modélisation objet avec UML”, 1997.
- [Va07] P.Roques, F.Vallée, “UML 2 en action de l’analyse des besoins à la conception”, 4ème édition, 2007.
- [AmMy] A.Ghezi, M.Kerkeb, “Conception et implémentations d’un site web Dynamique pour le paiement électronique”, mémoire de fin d’études pour l’obtention du diplôme d’ingénieur d’état en informatique, université M’sila, 2009/2010.
- [Ne11] <http://www.netbeans.org> \07/09/2011.
- [Dou10] J-M Doudoux, “Développons en java”, Version 1.50, 2010.
- [Ver] “Verchip corporation”, <http://www.verichipcorp.com/>
- [WSRE03] S. Weis, S. Sarma, R. Rivest, and D. Engels. “Security and privacy aspects of low-cost radio frequency identification systems”, In D. Hutter, G. Muller, W. Stephan, and M. Ullmann, editors, International Conference on Security in Pervasive Computing – SPC 2003, vol. 2802 of LNCS, pp.454–469, Boppard, Germany, Springer-Verlag, March 2003.
- [HHMB07] J. Ha, J.Ha, S. Moon, C. Boyd, “LRMAP: Lightweight and Resynchronous Mutual Authentication Protocol for RFID System,” In: Stajano, F., Kim, H.-J., Chae, J.-S., Kim, S.-D. (eds.) ICUCT 2006. LNCS, Springer, Heidelberg, vol. 4412, p.p. 80-89, 2007.
- [RKKW05] K. Rhee, J. Kwak, S. Kim, D. Won, “Challenge-response based RFID authentication protocol for distributed database environment,” In: Hutter, D., Ullmann, M. (eds.) SPC 2005. LNCS, vol. 3450, 70–84. Springer, Heidelberg, 2005.
- [LAK06] S. Lee, T. Asano, and K. Kim. “RFID mutual authentication scheme based on synchronized secret information,” In Symposium on Cryptography and Information Security, Hiroshima, Japan, January 2006.
- [LB09] A.X.Liu, L.A.Bailey, PAP: A privacy and authentication protocol for passive RFID tags, Computer Communications, 2009.
- [Med] Mme R. MEDGHOUL. “Modélisation et simulation”, Supporte de cours de 4ème Année ING, university de Constantine.
- [U-6.0] “UML Diagramming Guide”, A Supplementary Guide to Pacestar UML Diagrammer 6.0 www.pacestar.com.

[MyAd] “MySQL Administrator 1.2.16”, <http://fr.wikipedia.org/wiki/MySQL> , Dernière modification de cette page le 11 juin 2012 à 16:07.

[MyC] “MySQL connector j”, <http://downloads.mysql.com/archives.php?p=mysql-connector-java-3.1&o=other>.

[My08] Sun acquires MySQL (<http://blogs.mysql.com/kaj/2008/01/16/sun-acquires-mysql/>), blogs.mysql.com.

[UEOr] “L'UE autorise le rachat de Sun par Oracle”, (<http://fr.reuters.com/article/frEuroRpt/idFRLDE60K18W20100121>).

[EuCU] “European Commission Unconditionally Approves Oracle’s Acquisition of Sun” (<http://www.oracle.com/us/corporate/press/043873>), Oracle.

[Ja-De] J-M Doudoux, “Développons en Java”.

[CryE] “Java™ Cryptography Extension (JCE)”, Guide de référence pour Java™ SDK 2, Standard Edition, v 1.4.

[ArCr] “Architecture de cryptographie”, (JCA) spécification API.