

## Bibliography:

- [1] Web site: Guide to Cryptography, The free and open software security community,  
[https://www.owasp.org/index.php/Guide\\_to\\_Cryptography#Cryptographic\\_Functions](https://www.owasp.org/index.php/Guide_to_Cryptography#Cryptographic_Functions).
- [2] Web site: Network Associates International, « Introduction à la cryptographie, Gatwickstraat 25 NL-1043 GL Amsterdam » <http://www.nai.com>.
- [3] Web site: Microsoft Research, Cryptography Research, <http://research.microsoft.com/en-us/groups/crypto/>.
- [4] Web site: « Difference between symmetric key encryption and public key encryption », <http://www.differencebetween.com/difference-between-symmetric-key-encryption-and-vs-public-key-encryption/>.
- [5] Web Site: Maplesoft, « Caesar Cipher », <http://www.maplesoft.com/support/help/Maple/view.aspx?path=MathApps/CaesarCipher>.
- [6] Web Site: Crypto Museum, <http://www.cryptomuseum.com/crypto/vigenere/>.
- [7] Web Site: « Understanding Cryptography in Modern Military Communications », <http://www.idga.org/communications-engineering-and-it/articles/understanding-cryptography-in-modern-military-comm/>.
- [8] Web Site: Wolfram MathWorld, « Diffie-Hellman Protocol », <http://mathworld.wolfram.com/Diffie-HellmanProtocol.html>.
- [9] Web Site: ECRIM NEWS Online Edition, « Hight speed Quantum Key Distribution and Beyond », <http://ercim-news.ercim.eu/en85/special/high-speed-quantum-key-distribution-and-beyond>.
- [10] Web Site: Atmel, Bits & Pieces, « Symmetric VS. Asymmetric Encryption: Which Way is Better? » <http://blog.atmel.com/2013/03/11/symmetric-vs-asymmetric-encryption-which-way-is-better/>.
- [11] Jacques Stem, Louis Grandboulan, Phong Nguyen, David Pointcheval « Conception et preuves d'algorithmes cryptographique » Edition 2004.
- [12] Web Site: eHow, David Dunning, « What Is the Difference Between Stream Ciphers & Block Ciphers? » [http://www.ehow.com/info\\_12040172\\_difference-between-stream-ciphers-block-ciphers.html](http://www.ehow.com/info_12040172_difference-between-stream-ciphers-block-ciphers.html).
- [13] Web Site: CRYPTO-IT, [http://www.crypto-it.net/eng/theory/modes\\_of\\_block\\_ciphers.html](http://www.crypto-it.net/eng/theory/modes_of_block_ciphers.html).
- [14] Web Site: Entrust Datacard, « Securing Digital Identities & Information », <https://www.entrust.com/digital-signatures/>.
- [15] Web Site Experts Exchange, Giovanni Heward, « Cryptanalysis and Attacks », <http://www.experts-exchange.com/articles/12460/Cryptanalysis-and-Attacks.html>.

- [16] Web Site: Computer Hope, Free computer help and information,  
<http://www.computerhope.com/jargon/m/mitma.htm>.
- [17] François-Xavier Standaert, « Introduction to Side-Channel Attacks” Chapter 2 ».
- [18] « Announcing the ADVANCED ENCRYPTION STANDARD (AES) » Federal Information Processing Standards Publication 197, November 26, 2001.
- [19] R. Jain, R. Jejurkar, S.Chopade, S. Vaidya, M.Sanap « AES Algorithm Using 512 Bit Key Implementation for Secure Communication » International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE), March 2014, Rahuri Factory, India, pp 3516-3522.
- [20] DJ. E. Goumidi, F. Hachouf, « Modified confusion-diffusion based satellite image cipher using chaotic standard » logistic and sine maps, 2nd European Workshop on Visual Information Processing (EUVIP), 2010, 5-6 July 2010, Paris, France, pp: 204-209.
- [21] J. J. Tay, M. M. Wong, I. Hijazin, « Compact and Low Power AES Block Cipher Using Lightweight Key Expansion Mechanism and Optimal Number of S-Boxes » IEEE International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS), 2014, 1-4 December 2014, Kuching, Malaysia, pp: 108-114.
- [22] D. R Grandh, V.Kamalakannan, R.Balamurugan, S.Tamilselvan, « FPGA Implementation of Enhanced Key Expansion Algorithm for Advanced Encryption Standard » International Conference on Contemporary Computing and Informatics (IC3I), 2014, 27-29 November 2014, Mysore, India, pp: 409-413.
- [23] D. Chen, D. Qing, D. Wang, « AES Key Expansion Algorithm Based on 2D Logistic Mapping » 5th International Workshop on Chaos-fractals Theories and Applications (IWCFTA), 2012, 18-21 October 2012, Dalian, China, pp: 207-211.