Zoznam použitej literatúry

1. LEVICKÝ, Dušan. *Kryptografia a bezpečnosť komunikačných sietí*. Košice: Elfa, 2016. ISBN 978-80-8086-254-1.
2. *Dev C++: Integrated Development Environment for the C/C++ programming language* [online] [cit. 2017-06-30]. Dostupné z: `https://sourceforge.net/projects/orwelldevcpp/`.
3. TSIOMBIKAS, John. *Practical Makefiles, by example* [online] [cit. 2017-06-30]. Dostupné z: `http://nuclear.mutantstargoat.com/articles/make/mktut.pdf`.
4. DRUTAROVSKÝ, Miloš. *Kryptografia pre vstavané procesorové systémy: doplňujúce materiály a zdrojové kódy* [online] [cit. 2017-09-01]. Dostupné z: `http://aplikovanakryptografia.fei.tuke.sk/`.
5. CANNON, John J.; CATHERINE, Playoust. *First Steps in Magma* [online]. University of Sydney, School of Mathematics and Statistics, 1996 [cit. 2017-06-30]. Dostupné z: `http://magma.maths.usyd.edu.au/magma/pdf/first.pdf`.
6. *Magma Calculator: Magma Computational Algebra System* [online]. Australia: University of Sydney [cit. 2017-06-30]. Dostupné z: `http://magma.maths.usyd.edu.au/calc/`.
7. *OpenSSL: Binaries* [online] [cit. 2017-06-30]. Dostupné z: `https://wiki.openssl.org/index.php/Binaries`.
8. *mbed TLS* [online]. ARM Limited [cit. 2017-06-30]. Dostupné z: `https://tls.mbed.org/`.
9. *OpenSSL: Command Line Help* [online] [cit. 2017-06-30]. Dostupné z: `https://wiki.openssl.org/index.php/Command_Line_Utilities`.
10. *OpenSSL: Libcrypto API* [online] [cit. 2017-06-30]. Dostupné z: `https://wiki.openssl.org/index.php/Libcrypto_API`.
11. *MDK Microcontroller Development Kit* [online]. Germany: ARM GmbH [cit. 2017-06-30]. Dostupné z: `http://www.keil.com/mdk5/`.
12. *PK51 Professional Developer's Kit* [online]. Germany: ARM GmbH [cit. 2017-06-30]. Dostupné z: `www.keil.com/c51/`.

13. *ARM Keil Microcontroller Tools* [online]. Germany: ARM GmbH [cit. 2017-06-30]. Dostupné z: https://www.keil.com/download/product/.

14. MENEZES, Alferd J.; OORSCHOT, Paul C.; VANSTONE, Scott A. *Handbook of Applied Cryptography.* 1st ed. New York: CRC Press, 1996. ISBN 0-8493-8523-7. Dostupné tiež z: http://cacr.uwaterloo.ca/hac/.

15. DAEMEN, Joan; RIJMENT, Vincent. *AES Proposal: Rijndael* [online]. 1999 [cit. 2017-06-30]. Dostupné z: http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf.

16. TRENHOLME, Sam. *Tables for all 128 possible generators in Rijndael's galois field* [online] [cit. 2017-06-30]. Dostupné z: http://www.samiam.org/logtables.txt.

17. GASPAR, Lubos; DRUTAROVSKY, Milos; FISCHER, Viktor; BOCHARD, Nathalie. Efficient AES S-boxes implementation for non-volatile FPGAs. In: DANEK, Martin; KADLEC, Jiri; NELSON, Brent E. (eds.). *Proceedings of the Field Programmable Logic and Applications.* IEEE, 2009, s. 649–653. FPL 2009. ISBN 978-1-4244-3892-1. Dostupné tiež z: http://dx.doi.org/10.1109/FPL.2009.5272532.

18. MITSURU, Matsui; YUMIKO, Murakami. AES Smaller Than S-Box: Minimalism in Software Design on Low End Microcontroller. In: EISENBARTH, T.; OZTURK, E. (eds.). *Proceedings of the International Workshop on Lightweight Cryptography for Security and Privacy.* Springer, 2015, s. 51–66. LigtSec 2014. ISBN 978-3-319-16362-8. Dostupné tiež z: http://dx.doi.org/10.1007/978-3-319-16363-5_4.

19. DAEMEN, Joan; RIJMEN, Vincent. *The Design of Rijndael: AES – The Advanced Encryption Standard.* New York: Springer-Verlag, 2002. ISBN 3-540-42580-2.

20. FISCHER, Viktor; DRUTAROVSKY, Milos; CHODOWIEC, Pawel; GRAMAIN, Francois. InvMixColumn decomposition and multilevel resource sharing in AES implementations. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems.* 2005, vol. 13, no. 2, s. 989–992. Dostupné tiež z: http://dx.doi.org/10.1109/TVLSI.2005.853606.

21. PETRVALSKY, Martin; DRUTAROVSKY, Milos. Constant-weight coding based software implementation of DPA countermeasure in embedded microcontroller. *Microprocessors and Microsystems.* 2016, vol. 47, s. 82–89. Dostupné tiež z: https://doi.org/10.1016/j.micpro.2016.01.002.

22. BASSHAM, Lawrence E. *The Advanced Encryption Standard Algorithm Validation Suite (AESAVS: Recommendation for the Entropy Sources Used for Random Bit Generation* [online]. U.S.Department of Commerce/National Institute of Standards and Technology, 2002 [cit. 2017-06-30]. Dostupné z: http://csrc.nist.gov/groups/STM/cavp/documents/aes/AESAVS.pdf.

23. *FIPS PUB 186-4: Digital Signature Standard (DSS)* [online]. U.S.Department of Commerce/National Institute of Standards and Technology, 2013 [cit. 2017-06-30]. Dostupné z: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf.

24. CONTE, Brad. *Implementation of SHA-1 in C* [online]. 2006 [cit. 2017-06-30]. Dostupné z: http://bradconte.com/sha1_c.

25. CONTE, Brad. *Implementation of SHA-256 in C* [online]. 2006 [cit. 2017-06-30]. Dostupné z: http://bradconte.com/sha256_c.

26. SAARINEN, Markku-Juhani O. *Tiny_sha3 – Very small, readable implementation of the FIPS 202 and SHA3 hash function* [online]. 2015 [cit. 2017-06-30]. Dostupné z: https://github.com/mjosaarinen/tiny_sha3.

27. KELLER, Sharon S.; BASSHAM, Lawrence E. *The Secure Hash Algorithm 3 Validation System (SHA3VS): Recommendation for the Entropy Sources Used for Random Bit Generation* [online]. U.S.Department of Commerce/-National Institute of Standards and Technology, 2016 [cit. 2017-06-30]. Dostupné z: http://csrc.nist.gov/groups/STM/cavp/documents/sha3/sha3vs.pdf.

28. BARTKEWITZ, Timo. *Building Hash Functions from Block Ciphers, Their Security and Implementations Properties* [online]. 2009 [cit. 2017-06-30]. Dostupné z: https://www.emsec.rub.de/media/crypto/attachments/files/2011/03/bartkewitz.pdf.

29. PRENEEL, Bart. MASH Hash Functions (Modular Arithmetic Secure Hash). In: HENK, C. A. van Tilborg; SUSHIL, Jajodia (eds.). *Encyclopedia of Cryptography and Security*. Springer US, 2011, s. 761–761. ISBN 978-1-4419-5906-5. Dostupné tiež z: http://dx.doi.org/10.1007/978-1-4419-5906-5.

30. BROWN, Daniel R.L. *ECOH: the Elliptic Curve Only Hash* [online]. 2008 [cit. 2017-06-30]. Dostupné z: https://ehash.iaik.tugraz.at/uploads/a/a5/Ecoh.pdf.

31. BROWN, Daniel R.L. *ECOH2* [online]. 2009 [cit. 2017-06-30]. Dostupné z: http://csrc.nist.gov/groups/ST/hash/sha-3/Round1/documents/ECOH_Comments.pdf.

32. HALCROW, Michael A.; FERGUSON, Niels. *A Second Pre-image Attack Against Elliptic Curve Only Hash (ECOH)* [online]. 2009 [cit. 2017-06-30]. Dostupné z: https://eprint.iacr.org/2009/168.pdf.

33. *Certicom – Elliptic Curve Cryptography (ECC)* [online] [cit. 2017-06-30]. Dostupné z: https://www.certicom.com/content/certicom/en/ecc.html.

34. *Linear Congruential Generator* [online]. Wikipedia [cit. 2017-06-30]. Dostupné z: https://en.wikipedia.org/wiki/Linear_congruential_generator.

35. KNUTH, Donald E. *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*. 3rd ed. New York: Addison-Wesley, 1998. ISBN 0-201-89684-2.

36. *OpenSSL – TLS/SSL and crypto library: Source Code* [online] [cit. 2017-06-30]. Dostupné z: https://github.com/openssl/openssl.

37. STRENZKE, Falko. An Analysis of OpenSSL's Random Number Generator. In: FISCHLIN, Marc; CORON, Jean-Sébastien (eds.). *Advances in Cryptology – EUROCRYPT 2016*. Springer, 2016, s. 644–6669. LNCS 9665. ISBN 978-3-662-49889-7. Dostupné tiež z: http://dx.doi.org/10.1007/978-3-662-49890-3_25.

38. *Random Number Generation, Documentation and Software: NIST Statistical test Suite* [online]. NIST [cit. 2017-06-30]. Dostupné z: http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html.

39. BROWNM, Robert G. *Dieharder: A Random Number Test Suite* [online] [cit. 2017-06-30]. Dostupné z: http://webhome.phy.duke.edu/~rgb/General/dieharder.php.

40. *FIPS PUB 140-2: Security Requirements for Cryptographic Modules* [online]. U.S.Department of Commerce/National Institute of Standards and Technology, 2001 [cit. 2017-06-30]. Dostupné z: https://doi.org/10.6028/NIST.FIPS.140-2.

41. *NIST Statistical test Suite Package* [online]. NIST [cit. 2017-06-30]. Dostupné z: http://csrc.nist.gov/groups/ST/toolkit/rng/documents/sts-2.1.2.zip.

42. *NIST Special Publication 800-90B, second draft: Recommendation for the Entropy Sources Used for Random Bit Generation* [online]. U.S.Department of Commerce/National Institute of Standards and Technology, 2016 [cit. 2017-06-30]. Dostupné z: http://csrc.nist.gov/publications/drafts/800-90/sp800-90b_second_draft.pdf.

43. KILLMANN, Wolfgang; SCHINDLER, Werner. *A proposal for: Functionality classes for random number generators* [online]. Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, 2011 [cit. 2017-06-30]. Dostupné z: https://cosec.bit.uni-bonn.de/fileadmin/user_upload/teaching/15ss/15ss-taoc/01_AIS31_Functionality_classes_for_random_number_generators.pdf.

44. JOYE, Marc; YEN, Sung-Ming. The Montgomery Powering Ladder. In: KALISKI, Burton S.; KOÇ, Cetin K.; PAAR, Christof (eds.). *Cryptographic Hardware and Embedded Systems - CHES 2002: 4th International Workshop Redwood Shores, CA, USA, August 13–15, 2002*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, s. 291–302. ISBN 978-3-540-36400-9. Dostupné tiež z: http://dx.doi.org/10.1007/3-540-36400-5_22.

45. HANKERSON, Darrel; MENEZES, Alfred; VANSTONE, Scott. *Guide to Elliptic Curve Cryptography*. New York: Springer-Verlag, 2004. ISBN 0-387-95273-X.

46. BERNSTEIN, Daniel J. *A state-of-the-art Diffie-Hellman function: How do I use Curve25519 in my own software?* [online] [cit. 2017-06-30]. Dostupné z: https://cr.yp.to/ecdh.html.

47. BERNSTEIN, Daniel J.; LANGE, Tanja. *Explicit-Formulas Database* [online] [cit. 2017-06-30]. Dostupné z: http://www.hyperelliptic.org/EFD/.

48. BARR, Michael. *CRC Series, Part 3: CRC Implementation Code in C/C++* [online] [cit. 2017-06-30]. Dostupné z: https://barrgroup.com/Embedded-Systems/How-To/CRC-Calculation-C-Code.

49. *Polynomial Representations of Cyclic Redundancy Checks* [online]. Wikipedia [cit. 2017-06-30]. Dostupné z: https://en.wikipedia.org/wiki/Polynomial_representations_of_cyclic_redundancy_checks.

50. KOOPMAN, Philip; CHAKRAVARTY, Tridib. Cyclic Redundancy Code (CRC) Polynomial Selection For Embedded Networks. In: *Proceedings of the 2004 International Conference on Dependable Systems and Networks* [online]. Washington, DC, USA: IEEE Computer Society, 2004, s. 145–154 [cit. 2017-06-30]. DSN '04. ISBN 0-7695-2052-9. Dostupné z: https://users.ece.cmu.edu/~koopman/roses/dsn04/koopman04_crc_poly_embedded.pdf.

51. KOOPMAN, Philip. *Best CRC Polynomials* [online] [cit. 2017-06-30]. Dostupné z: https://users.ece.cmu.edu/~koopman/crc/.

52. BARR, Michael. *CRC Series, Part 3: Surce Code in C* [online] [cit. 2017-06-30]. Dostupné z: http://www.barrgroup.com/code/crc.zip.

53. ROSS, Williams D. *LZRW Compression Algorithms History* [online]. 1997 [cit. 2017-06-30]. Dostupné z: http://www.ross.net/compression/.

54. ZIV, Jacob; LEMPEL, Abraham. A Universal Algorithm for Sequential Data Compression. *IEEE Transactions on Information Theory* [online]. 1977, vol. 23, no. 3, s. 337–343 [cit. 2017-06-30]. ISSN 0018-9448. Dostupné z: http://dx.doi.org/10.1109/TIT.1977.1055714.

55. ROSS, Williams D. An Extremely Fast Ziv-Lempel Data Compression Algorithm. In: *Proceedings of the 1991 Data Compression Conference* [online]. Snowbird, UT, USA: IEEE, 1991, s. 362–371 [cit. 2017-06-30]. DCC '91. ISBN 0-8186-9202-2. Dostupné z: http://dx.doi.org/10.1109/DCC.1991.213344.

56. FINNERAN, Scott; MILLER, Peter. *SRecord Package: Collection of Powerful Tools for Manipulating EPROM Load Files* [online] [cit. 2017-06-30]. Dostupné z: http://srecord.sourceforge.net/.

57. *NIST Special Publication 800-57 Part 1 Revision 4: Recommendation for Key Management* [online]. U.S.Department of Commerce/National Institute of Standards and Technology, 2016 [cit. 2017-06-30]. Dostupné z: http://dx.doi.org/10.6028/NIST.SP.800-57pt1r4.

58. MCGREW, David A.; VIEGA, John. *The Galois/Counter Mode of Operation (GCM)* [online] [cit. 2017-06-30]. Dostupné z: http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/gcm/gcm-spec.pdf.

59. BOSMA, Wieb; CANNON, John; PLAYOUST, Catherine; STEEL, Allan. *Solving Problems with Magma.* Australia: University of Sydney, 1999. Dostupné tiež z: http://magma.maths.usyd.edu.au/magma/pdf/examples.pdf.

60. NEEDHAM, Roger M.; WHEELER, David J. *Tea extrensions.* 1997. Dostupné tiež z: `http://www.cix.co.uk/~klockstone/xtea.pdf`.

61. *XTEA* [online]. Wikipedia [cit. 2017-06-30]. Dostupné z: `https://en.wikipedia.org/wiki/XTEA`.

62. *ARM mbed: Source Code* [online]. ARM Limited [cit. 2017-06-30]. Dostupné z: `https://tls.mbed.org/source-code`.

63. MISOCZKI, Rafael. et al. *TinyCrypt Cryptographic Library* [online] [cit. 2017-06-30]. Dostupné z: `https://github.com/01org/tinycrypt`.

64. POPOVEC, Peter. *OSEID – Open source smartcard/token with pkcs15 structure, RSA and ECC* [online] [cit. 2017-07-31]. Dostupné z: `https://sourceforge.net/projects/oseid/`.

65. BÁN, Jaroslav. *ACL – ARM cryptographic library* [online] [cit. 2017-07-31]. Dostupné z: `https://github.com/medvid/acl`.

Register