

# 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: doplnujúce 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/calcul/>.
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\\_Uutilities](https://wiki.openssl.org/index.php/Command_Line_Uutilities).
10. *OpenSSL: Libcrypto API* [online] [cit. 2017-06-30]. Dostupné z: [https://wiki.openssl.org/index.php/Libcrypto\\_API](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/](http://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. LightSec 2014. ISBN 978-3-319-16362-8. Dostupné tiež z: [http://dx.doi.org/10.1007/978-3-319-16363-5\\_4](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](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](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](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](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](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](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](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](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](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](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.y.p.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](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](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

## A

- AES, 17, 39, 44, 153
  - AES128, 58, 70, 144
  - AES128 ECB, 92
  - AES192, 58, 70
  - AES256, 58, 70
  - dešifrovanie, 59
  - inverzný, 59
  - Rijndael, 42
- AES GF, 48
- algebraický systém, 13, 15
  - grupa, 13
    - aditívna, 15
    - multiplikatívna, 15
  - konečné pole, 13
  - okruh, 13, 15
  - podgrupa, 140
- algoritmus, 10
  - Diffie-Hellman, 139
  - ECIES, 153
  - ElGamal, 153
  - Euklidov, 28, 35
    - rozšírený, 108
  - binárny, 36, 108
  - gcd, 28
  - LZ77, 133
  - LZRW1, 133, 156
  - rozšírený Euklidov, 35, 36, 51, 94
  - RSA, 93
- ALU, 26
- ANSI, 2, 5
- aritmetika
  - celočíselná, 28, 34
  - polynomiálna, 51
  - modulárna, 39
- ARM, 10, 27
  - ARM7TDMI, 10
  - Cortex-M0, 10

- Cortex-M0+, 10
  - Kinetis, 10
  - Cortex-M3, 10
- assembler, 15, 31, 136, 160
- ASIC, 1, 30
- asymetrická šifra, 3
  - ECC, 17
  - RSA, 17
- asymetrický algoritmus, 7
- autentizácia, 144, 153
  - ďalšie autentizované dáta, 146

## B

- bajt, 25
- Barrettova redukcia, 98
- bezpečnosť
  - 128-bitová, 141
  - ekvivalentná, 105, 106, 140, 142
  - kryptografická, 105
  - porovateľná, 105
- binárny, 40
- bit, 26, 74
- blok, 20
- Blumovo číslo, 8, 78
- bod na EC, 110
  - Haasov teorém, 111
  - nekonečno, 110, 111
  - počet bodov, 111
  - súradnice, 110
- bootloader, 59, 155

## C

- C++, 5
- C51, 10, 24
- Certicom, 72
- certifikát, 9
- CRC

- CRC8, 127
- CRC16, 127
- CRC32, 127
- generačný polynóm, 126
- chybné slovo, 128
- implementácia v jazyku C, 129
- kódy, 125
- kontrolný súčet, 125
- Koopman, 126
- optimálne polynómy, 128
- súčet, 125, 144
- zvyšok po delení, 127
- cyklus, 11, 60
- Č**
- časový útok, 5
- čínska veta o zvyškoch, 93
- číslica, 28, 30
- číslo
  - celé, 26
  - doplnkový kód, 29
  - faktorizácia, 77, 78, 81, 105
  - Fermatovo, 81, 94
  - hexadecimálne, 29, 45
  - multiplikatívne inverzné, 35, 94
  - náhodné, 140
  - nesúdeliteľné, 35, 36
  - nezáporné, 32
  - neznamienkové, 19, 26
  - prirodzené, 26
  - pseudonáhodné, 140
  - špeciálne, 35
  - štandardná reprezentácia, 100
  - záporné, 29
  - záporné MP, 27
  - znamienko, 29
  - znamienkové, 26, 27
- čítač, 17
- D**
- dešifrovanie, 20
- DEV C++, 5, 74
- digitálny podpis, 28
- DSA, 140
- ECDSA, 149
  - generovanie kľúčov, 150
  - overenie podpisu, 150
  - systémové parametre, 149
- dĺžka slova
  - 32 bitov, 107
- double, 2
- E**
- EC
  - Curve25519, 107
  - inverzný (opačný) bod  $-P$ , 111
  - Jacobiho súradnice
    - $2P$ , 121
    - $P + Q$ , 122
  - NIST Curve P-256, 115
    - bod  $P$ , 115
    - počet bodov, 115
    - rád krivky, 115
  - operácia
    - analytické vzťahy, 111
    - dvojnásobok bodu  $2P$ , 111
    - geometrická interpretácia, 111
    - sčítane bodov  $P + Q$ , 111
  - operácie
    - dvojnásobok bodu  $2P$ , 111
    - geometrická interpretácia, 112
  - počet bodov, 111
  - prvočíselná, 110, 151
  - prvočíselná NIST, 111, 122
  - rád, 149
  - rád krivky, 111
  - súradnice
    - afinné, 111, 119, 149
    - Chudnovského, 119
    - Jacobiho, 120
    - projektívne, 113
    - zmiešané, 120
- ECC, 2, 25, 72, 105, 153
- ECIES
  - dešifrovanie, 154
  - overenie kľúča, 154
  - šifrovanie, 154
- eliptická krivka, 2, 5
- endián, 25
  - malý, 25
  - veľký, 25
- energetické nároky, 3



entropia, 66, 76, 84, 91, 141  
 exponent, 22, 102  
   dešifrovací, 20, 93, 101  
   šifrovací, 20, 94

**F**

firmvér, 10, 151, 155  
 float, 2  
 FPGA, 1, 30, 160  
 funkcia  
   AddRoundKey, 57  
   gf256\_mul, 47  
   hašovacia, 65  
   HMAC, 153  
   InvMixColumn, 55, 59  
   InvSubBytes, 49  
   KDF, 71, 141, 153  
   MixColumn, 55, 59  
   mod, 14  
   printf, 5, 11  
   putchar, 5, 11  
   rand, 73  
   RAND\_add, 82  
   RAND\_bytes, 82  
   srand, 75  
   SubBytes, 49  
   xtime, 41, 56

**G**

Galoisovo pole, 4, 15  
   operácie, 106  
 gcc, 6  
 gcd, 35  
 GCM, 59  
 generátor, 44, 48  
   AES, 53  
   AES GF, 49  
   lineárny kongruentný, 74  
   Mitchellov a Moorov, 75  
   v  $\mathbb{GF}(q)$ , 139  
 GF, 5  
   AES, 41, 146  
   diskrétny logaritmus, 139  
   GCM  $\mathbb{GF}(2^{128})$ , 144  
   generátor, 44, 139  
   inverzia, 113

optimalizované pre ECC, 107  
    $\mathbb{GF}(2^{255} - 19)$ , 107  
    $p_{192}$ , 107, 108  
    $p_{224}$ , 107, 108  
    $p_{256}$ , 107, 109  
    $p_{384}$ , 107, 109  
    $p_{512}$ , 107, 109

GNU, 5

grupa, 15  
   abelovská, 111  
   aditívna, 15  
   multiplikatívna, 15, 140  
   rád grupy, 140

**H**

Hammingova váha, 128  
 hašovacia funkcia, 3, 65, 141, 153  
   Davies – Meyer, 68  
   digitálny podpis, 151  
   ECOH, 72  
   Hirose, 70  
   MASH, 71  
   Matyas – Meyer – Oseas, 68  
   Miyaguchi – Preneel, 69  
   RSA, 71  
   SHA1, 65, 82, 83  
   SHA2, 65  
   SHA3, 65  
 Hello World, 6, 10, 72  
 hexadecimálny, 55  
 hierarchia operácií v ECC, 106

**I**

IDE, 2, 5, 10  
 IEEE, 2  
 inverzia, 35  
   multiplikatívna, 16, 49  
 IoT, 3, 10, 39

**J**

jazyk C, 2, 18  
   CRC funkcie, 129  
   NIST test suite, 91  
   SHA funkcie, 153  
   volatile, 18

**K**

Keil, 10  
 kľúč, 145
 

- rundový, 57
- súkromný, 20, 93, 139, 140
  - generovanie podpisu, 150
- tajný, 77
- veľkosť, 105
- verejný, 20, 140
  - verifikácia, 153
- XTEA, 128 bitov, 156

 knižnica, 4, 6, 10, 15, 35
 

- Mbed TLS, 27, 34, 156, 159
- MDK, 75
- Microlib, 75
- OpenSSL, 82
- PolarSSL, 159
- SHA funkcií, 153
- tinyECC, 160

 kompresia
 

- algoritmus LZ77, 133
- LZRW1, 133, 134
- Ros Williams, 133

 konečné pole, 4, 15  
 koprocesor, 4, 39, 67, 77  
 krokovanie, 5  
 kryptografia, 14
 

- asymetrická, 105
- ľahká (lightweight), 39, 160
- postkvantová, 160

 kryptografické primitívum, 4, 65, 151

**L**

LFSR, 52  
 Linux, 7  
 logaritmus, 47  
 LZRW1, 133
 

- dekompresia v jazyku C, 135
- kompresia v jazyku C, 136

**M**

MAC, 144  
 Magma, 2, 7
 

- algebra, 7
- funkcia
  - div, 142

ElementToSequence, 152  
 EllipticCurve, 113  
 ExtendedGCD, 36  
 FactoredOrder, 151  
 GF(p), 116  
 llog2, 142  
 IntegerRing, 152  
 Intseq, 29  
 IsPrime, 79  
 IsProbablePrime, 79  
 mod, 110  
 Modexp, 23, 38, 104  
 Modinv, 152  
 Order, 116  
 Random, 110  
 RandomPrime, 80  
 RationalPoints, 113  
 Reverse, 29  
 time, 80  
 kalkulačka, 7, 20, 36, 77  
 make, 5, 6
 

- makefile, 6

 manuál, 7  
 matica
 

- afinnej transformácie, 51
- konštantná, 55
- stavov, 55–57

 Matlab, 2, 7  
 MCU, 1
 

- 8-bitové, 39
- 8051, 10, 15, 24, 64
  - ADuC842, 10
  - ADuC836, 24, 64
- ARM Cortex-M0, 58
- ARM7TDMI, 160
- AT Mega, 160
- ATiny, 58
- Kinetis, 10
- MSP430, 58
- RL78, 58

 MDK, 10  
 množina, 13  
 mód
 

- CFB, 59
- CTR, 59, 144
- GCM, 59, 144

- OFB, 59  
 modulárna aritmetika, 4, 13, 14, 20, 35  
 modulárna mocnina, 139  
 modulárna redukcia, 14, 34, 74  
 modulárne násobenie, 4, 96  
 modulárne umocňovanie, 21, 93, 94, 96,  
     98, 99, 114  
 modulo operácia  
     implicitná, 17  
 modulo redukcia, 96  
 Monte Carlo test, 61, 66  
 Montgomeryho  
     násobenie, 97, 98  
     oblasť, 35, 96, 98, 100  
     rebrík, 5, 100, 119  
     redukcia, 35, 96, 97  
     umocňovanie, 97  
 MP  
     delenie, 31  
     modulárna aritmetika, 34, 93  
     modulárna inverzia, 35  
     modulárne násobenie, 34  
     modulárne odčítanie, 34  
     modulárne sčítanie, 34  
     odčítanie, 30  
     sčítanie, 30  
     súčin, 30  
 MP číslo, 26  
 m-súbor, 7  
 MSW, 32  
 multiplikatívna inverzia, 16  
 Murphyho zákon, 19  
  
**N**  
 náhodné čísla, 73  
 naivná implementácia, 5, 100, 101  
 násobenie  
     klasické modulárne, 102  
     pomocou logaritmickej tabuľky, 47  
     v AES GF, 47  
 násobička, 27, 98, 99, 146  
 nástroj, 7  
 neznamienkové číslo, 19  
 NIST  
     odporúčanie, 140, 142  
  
**O**  
 obmedzenia, 3  
 okno, 102  
     konzola, 5  
     s premenlivou šírkou, 102  
     terminálové, 7–10, 85, 147  
 okruh, 15  
 OpenSSL, 2, 9, 82  
 operácia  
     algebraická, 49  
     aritmetická, 13  
     binárna, 13, 111  
     delenia, 14, 35  
     delenie ireducibilným, 41  
     elementárna, 106, 122  
     inverzia, 28, 36, 49  
     *k*-násobok bodu, 106  
     modulárna inverzia, 14  
     multiplikatívna inverzia, 36  
     na EC  
         dvojnásobok bodu, 106  
         súčet bodov, 106  
     násobenie, 14, 15, 41  
         v AES GF, 48  
     odčítanie, 41  
     sčítanie, 14, 15, 41  
     súčin, 15  
     súčin matíc, 55  
     XOR, 41, 43, 83, 144, 146  
     základná, 14, 28, 40  
 operand, 15  
 optimalizácia, 3, 4, 18, 39  
  
**P**  
 pamäť, 25, 34, 39, 56, 57, 75  
      dátová, 102  
     EEPROM, 130  
     EPROM, 130  
     Flash, 44, 60  
     organizácia, 25  
     programová, 59, 60, 67  
     RAM, 19, 44, 103  
 PC, 2, 5, 6  
 PLL, 11  
 podmonožina, 13  
 pole, 26

- polynóm
    - binárny, 53
    - CCITT, 126
    - CRC16, 126
    - generačný, 126
    - generačný pre GCM  $\text{GF}(2^{128})$ , 146
    - ireducibilný, 40, 41, 44, 49, 51, 145
      - AES, 53
    - vyjadrenie
      - Koopmanove, 126
      - priame, 126
      - reverzné, 126
  - postranný kanál, 4, 44
  - prekladač, 15
  - premenná
    - int, 15
    - long, 15
    - stavová, 74
  - pretečenie, 18, 19
  - pretypovanie, 14
  - príkaz
    - podmieneny, 55
  - príkazový riadok, 9
  - príkazy, 9
  - príklad, 20, 29, 36, 41–43, 48, 53, 78, 81, 84, 89, 95, 98, 99, 102, 110, 113, 116, 117, 120, 123, 131, 141, 147, 151
  - PRNG, 8, 73
    - BBS, 78
    - Blum – Blum – Shub, 78
    - kryptograficky bezpečný, 76, 141
    - OpenSSL, 82
    - perióda, 76
    - RSA, 81
    - s čítačom, 77
    - seed, 76
    - stav, 83
  - program, 5, 18
    - aplikačný, 155
    - Hello World, 10
  - protokol, 10
  - prvočíslo, 15, 44, 73, 93, 116
    - NIST, 107, 108
    - primitívny koreň, 139
  - prvok
    - inverzný, 15, 51
    - neutrálny, 15
- R**
- RAM, 3
  - RNG, 3, 66, 85
    - ideálny, 85
  - rovnica
    - EC, 110
    - kubická, 110
    - Weierstrassova, 110
  - RSA, 2, 5, 13, 20, 25, 35, 71, 93, 105
    - dešifrovanie, 20, 101
      - s využitím CRT, 94
    - modul, 93
    - operand, 93
    - súkromný kľúč, 94
    - šifrovanie, 20
  - rýchlosť, 39
- S**
- S-box, 49, 52, 56
    - inverzný, 51
  - sekunda, 19
  - spotreba, 4
  - SSL, 9
  - súkromný kľúč, 5
  - symetrická šifra, 3
    - AES, 17
- Š**
- šifra
    - AES, 39
    - bloková, 77
    - RSA, 93
    - symetrická, 39
    - XTEA, 156
  - šifrovanie, 20
- T**
- tabuľka, 45, 56, 60, 102
    - exponenciálna, 44, 45, 47
    - inicializácia, 103
    - inverzná logaritmickeá, 44
    - inverzný S-box, 49
    - logaritmickeá, 44
    - S-box, 49

T-box, 56  
 T-box, 56, 57, 60  
   inverzný, 58  
 teória čísel, 7  
 test  
   autokorelačný, 85, 87  
   deterministický, 80  
   dieharder, 85  
   FIPS, 87  
   frekvenčný, 85, 86  
   NIST, 85, 91  
   pokerový, 85, 86  
   pravdepodobnostný, 80  
   prvočíslo, 79  
   rovnakých reťazcov, 85, 87  
   sériový, 85, 86  
   štatistický, 85  
 testovací vektor, 7, 156  
 testovanie  
   prvočíselnosti na báze EC, 79  
 TLS, 9  
 transformácia, 4, 49, 96  
   afinná, 49, 51, 53  
   InvMixColumn, 55  
   MixColumn, 55  
   nelienárna, 56  
   stĺpca, 56  
 TRNG, 60, 66, 73, 84, 91, 141

**U**

UART, 11  
 úlohy  
   doplňujúce, 12, 23, 32, 38, 62, 72,  
     92, 104, 123, 138, 157  
 umocňovanie  
   binárne  
     sprava doľava, 22  
     zlava doprava, 23  
   Montgomeryho rebrík, 101  
     zlava doprava, 101  
   s kľzavým oknom, 102, 103  
   s využitím tabuliek, 101  
   s  $w$ -bitovým oknom  
     so šírkou  $w$ -bitov, 101, 102  
     zlava doprava, 101  
 Unix, 6

útok, 44  
   hrubou silou, 105  
   matematické metódy, 105  
 uzavretosť, 15

**V**

vektor, 40  
 VHDL, 1, 160  
 $\mu$ Vision, 10, 24, 64  
 volatile, 18  
 vstavaný, 4  
 vstavaný systém, 4

**W**

Windows, 5  
 WinRAR, 84, 132, 138

**X**

XOR, 55, 57  
 XTAL, 24, 64  
 xtime, 42, 44, 45, 59

**Z**

základ, 28, 98  
 zákon  
   asociatívny, 15, 43  
   distributívny, 43  
   komutatívny, 111  
 zásobník, 1, 27  
 zavádzací kód, 59, 155  
 zdieľané tajomstvo, 143  
 znamienko, 32  
 zvýšená presnosť, 26  
 zvyšková číselná sústava, 4, 93  
   CRT, 93