# **Hashovací algoritmy a jejich využití**

## **Citace**

1. ŠTRÁFELDA, Jan. *Co je hash či hashování*. Online. Https://www.strafelda.cz/. [2008], aktualizováno 13.01.2025. Dostupné z: <https://www.strafelda.cz/hash>. [cit. 2025-01-19].
2. RIVEST, Ronald. *The MD5 Message-Digest Algorithm*. Online. INTERNET ENGINEERING TASK FORCE [IETF]. IETF Datatracker. 1992. Dostupné z: <https://datatracker.ietf.org/doc/html/rfc1321>. [cit. 2025-01-19].
3. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY [NIST]. *Secure Hash Standard (SHS)*. Online. Https://nvlpubs.nist.gov/. Srpen 2015. Dostupné z: [https://web.archive.org/web/20161126003357/http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf](https://web.archive.org/web/20161126003357/http:/nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf). [cit. 2025-01-19].
4. EASTLAKE, D. a JONES, P. *US Secure Hash Algorithm 1 (SHA1)*. Online. INTERNET ENGINEERING TASK FORCE [IETF]. Computer Security Resource Center (CSRC). Září 2001. Dostupné z: <https://datatracker.ietf.org/doc/html/rfc3174>. [cit. 2025-01-19].
5. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY [NIST]. *Secure Hashing*. Online. INTERNET ENGINEERING TASK FORCE [IETF]. Computer Security Resource Center (CSRC). Říjen 2007, aktualizováno 5. května 2011. Dostupné z: [https://web.archive.org/web/20110625054822/http://csrc.nist.gov/groups/ST/toolkit/secure\_hashing.html](https://web.archive.org/web/20110625054822/http:/csrc.nist.gov/groups/ST/toolkit/secure_hashing.html). [cit. 2025-01-19].
6. CORPORATE FINANCE INSTITUDE (CFI). *Hash Function*. Online. CORPORATE FINANCE INSTITUDE (CFI). Corporate Finance Institude. [2022]. Dostupné z: <https://corporatefinanceinstitute.com/resources/cryptocurrency/hash-function/>. [cit. 2025-01-20].
7. KRČMÁŘ, Petr. SHA-1 není bezpečná, Google ukázal kolizi. Online. *Root*. 2017, s. 1. Dostupné z: <https://www.root.cz/clanky/sha-1-neni-bezpecna-google-ukazal-kolizi/>. [cit. 2025-01-19].
8. *The hash function RIPEMD-160*. Online. DEPARTEMENT ELEKTROTECHNIEK (ESAT). <Https://www.esat.kuleuven.be>. [2005], aktualizováno 13. února 2012. Dostupné z: <https://homes.esat.kuleuven.be/~bosselae/ripemd160.html>. [cit. 2025-01-20].
9. CORPORATE FINANCE INSTITUDE (CFI). *Hash Function*. Online. CORPORATE FINANCE INSTITUDE (CFI). Corporate Finance Institude. [2022]. Dostupné z: <https://corporatefinanceinstitute.com/resources/cryptocurrency/hash-function/>. [cit. 2025-01-20].
10. UNIVERSITY OF CAMBRIDGE. *Fast CRC32 in Software*. Online. UNIVERSITY OF CAMBRIDGE. Department of Computer Science and Technology. 1994. Dostupné z: <https://www.cl.cam.ac.uk/research/srg/projects/fairisle/bluebook/21/crc/crc.html>. [cit. 2025-01-20].
11. *Cyclic redundancy check: Cyklický redundantní součet*. Online. In: Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, listopad 2004. Dostupné z: <https://en.wikipedia.org/wiki/Cyclic_redundancy_check>. [cit. 2025-01-20].
12. *Laureates of the Japan Prize*. Online. Japan Prize. [2012]. Dostupné z: <https://www.japanprize.jp/en/prize_prof_1999_peterson.html>. [cit. 2025-01-20].
13. DEFUSE SECURITY. *Salted Password Hashing - Doing it Right*. Online. DEFUSE SECURITY. Crack Station. [2012], aktualizováno 28. září 2021. Dostupné z: <https://crackstation.net/hashing-security.htm>. [cit. 2025-01-21].
14. OŠŤÁDAL, Radim. *Teoretický základ a přehled kryptografických hashovacích funkcí*. PDF. Brno, 2012. Dostupné z: <https://is.muni.cz/www/ostadal/hash_overview.pdf>. [cit. 2025-01-22].
15. KOZLÍK, Andrew. *Hashovací funkce*. PDF, Není uveden druh práce. Praha: Univerzita Karlova, Matematicko fyzikální fakulta, [2024]. Dostupné také z: <https://www.karlin.mff.cuni.cz/~kozlik/udk_mat/hash.pdf>.
16. NORD VPN. *Cookie hash*. Online. NORD VPN. Nord VPN. Dostupné z: <https://nordvpn.com/cybersecurity/glossary/cookie-hash/>. [cit. 2025-01-22].
17. KASPERSKY LAB. *Brute Force Attack: Definition and Examples*. Online. KASPERSKY LAB. Kaspersky. [2019]. Dostupné z: <https://www.kaspersky.com/resource-center/definitions/brute-force-attack>. [cit. 2025-01-23].
18. STAHIE, Silviu. RTX 4090 8-Card Rig Cracks Random and Powerful Eight-Character Passwords in 48 Minutes. Online. *Bitdefender*. 20 října 2022, s. 1. Dostupné z: <https://www.bitdefender.com/en-us/blog/hotforsecurity/rtx-4090-8-card-rig-cracks-random-and-powerful-eight-character-passwords-in-48-minutes>. [cit. 2025-01-23].
19. CHICK3NMAN. *Hashcat v6.2.6 benchmark*. Online. MICROSOFT. Github. 2022, aktualizováno února 2024. Dostupné z: <https://gist.github.com/Chick3nman/32e662a5bb63bc4f51b847bb422222fd>. [cit. 2025-01-23].
20. KASPERSKY LAB. *Brute Force Attack: Definition and Examples*. Online. KASPERSKY LAB. Kaspersky. [2019]. Dostupné z: <https://www.kaspersky.com/resource-center/definitions/brute-force-attack>. [cit. 2025-01-23].
21. VAIDEESWARAN, Narendran. NTLM Explained. Online. *CrowdStrike*. 2011, s. 4. Dostupné z: <https://www.crowdstrike.com/en-us/cybersecurity-101/identity-protection/windows-ntlm/>. [cit. 2025-01-23].
22. BAKER, Kurt. Pass-the-Hash Attack. Online. *CrowdStrike*. 2011. Dostupné z: <https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/pass-the-hash-attack/>. [cit. 2025-01-23].
23. MICROSOFT. *Prohlídka jazyka C#*. Online. MICROSOFT. Prohlídka jazyka C#. 1975, aktualizováno 2024. Dostupné z: <https://learn.microsoft.com/cs-cz/dotnet/csharp/tour-of-csharp/overview>. [cit. 2025-01-13].
24. ŠTRÁFELDA, Jan. *Co je hash či hashování*. Online. Https://www.strafelda.cz/. [2008], aktualizováno 13.01.2025. Dostupné z: <https://www.strafelda.cz/hash>. [cit. 2025-01-13].
25. WIKIPEDIE. *Cyclic redundancy check*. Online. WIKIMEDIA COMMONS. Wikipedie. 2010, aktualizováni 12. 09. 2024. Dostupné z: <https://en.wikipedia.org/wiki/Cyklick%C3%BD_redundantn%C3%AD_sou%C4%8Det>. [cit. 2025-01-13].