# **Hashovací algoritmy a jejich využití**

„Jazyk C# je multiplatformní jazyk pro obecné účely, který vývojářům umožňuje produktivní práci při psaní vysoce výkonného kódu. S miliony vývojářů je jazyk C# nejoblíbenějším jazykem .NET. Jazyk C# má širokou podporu v ekosystému a všech úlohách .NET. Na základě objektově orientovaných principů zahrnuje mnoho funkcí z jiných paradigmat, nikoli z nejméně funkčního programování. Funkce nízké úrovně podporují scénáře vysoké efektivity bez psaní nebezpečného kódu. Většina modulů runtime a knihoven .NET je napsaná v jazyce C# a pokroky v jazyce C# často využívají všechny vývojáře .NET.“ [3]

Hashe dokážou zpracovat jakékoliv množství dat a vrátit jenom určitou délku, to ovšem znamená menší problémy. Různé vstupní data mohou vracet stejnou hodnotu hashe, což v případě, že používáme hashe pro ukládání hesel znamená velký bezpečnostní problem. Šance kdy se něco takového může stát je závislá na délce výstupního hashe, a proto se v případech, kde by to mohlo znamenat velký problem, používají delší hashe, jako třeba SHA-256 či SHA-512. [3] Pravděpodobnost si můžeme sami kalkulovat pomocí jednoduchého zvorečku.

CRC32 je hashovací algorithmus určený k dělání checksum souborů a dat. Skoro vůbec se nepoužívá pro ukládání hesel. Chtěl bych tento algoritmus použít, protože je používán v několika velice důležitých protokolech: „ISO 3309 (HDLC), ANSI X3.66 (ADCCP), FIPS PUB 71, FED-STD-1003, ITU-T V.42, ISO/IEC/IEEE 802-3 (Ethernet), SATA, MPEG-2, PKZIP, Gzip, Bzip2, POSIX cksum, PNG, ZMODEM atd.“ [4]

## **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. 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].
7. 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].
8. 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].
9. 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].