# **Hashovací algoritmy a jejich využití**

„Formálně jde o funkci *h*, která převádí vstupní posloupnost [bitů](https://cs.wikipedia.org/wiki/Bit) (či [bytů](https://cs.wikipedia.org/wiki/Bajt)) na posloupnost pevné délky *n* bitů. Z definice plyne existence [*kolizí*](https://cs.wikipedia.org/wiki/Kolize_(informatika)), to znamená dvojic vstupních dat (*x*,*y*), *x* ≠ *y*, takových, že *h*(*x*) = *h*(*y*), tj. dvojice různých vstupních dat může mít stejný otisk. Kolize jsou nežádoucí, ale v principu se jim nelze vyhnout, protože počet možných různých vstupních zpráv je větší než počet možných různých otisků. Vhodnou volbou funkce lze snížit pravděpodobnost, že nastane kolize pro podobná data.“ [1]

„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.“ [2]

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. WIKIPEDIE. *Hašovací funkce*. Online. Wikimedia Commons. Wikipedie. 2001, aktualizováno 11.09.2023. Dostupné z: <https://cs.wikipedia.org/wiki/Ha%C5%A1ovac%C3%AD_funkce>. [cit. 2025-01-13].
2. 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].
3. 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].
4. 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].