João Vítor Nunes,
Josué Nascimento,
Raul Rodrigues,
Pedro Pacheco,
Victor Vasconcellos

# Aplicativo para ensino de algoritmos de hashing

# Problema

**Criar um aplicativo para o ensino de algoritmos de *hashing***

A fim de ensinar de maneira interativa e visual o funcionamento e aplicação de algoritmos de hashing nós criaremos um aplicativo de ensino.

# Algoritmos de Hashing

- *"O Hashing refere-se ao processo de geração de uma saída (output) de tamanho fixo a partir de uma entrada (input) de tamanho variável. Isto é feito através do uso de fórmulas matemáticas conhecidas como funções hash (implementado como algoritmos de hashing)."*

# Complexidade

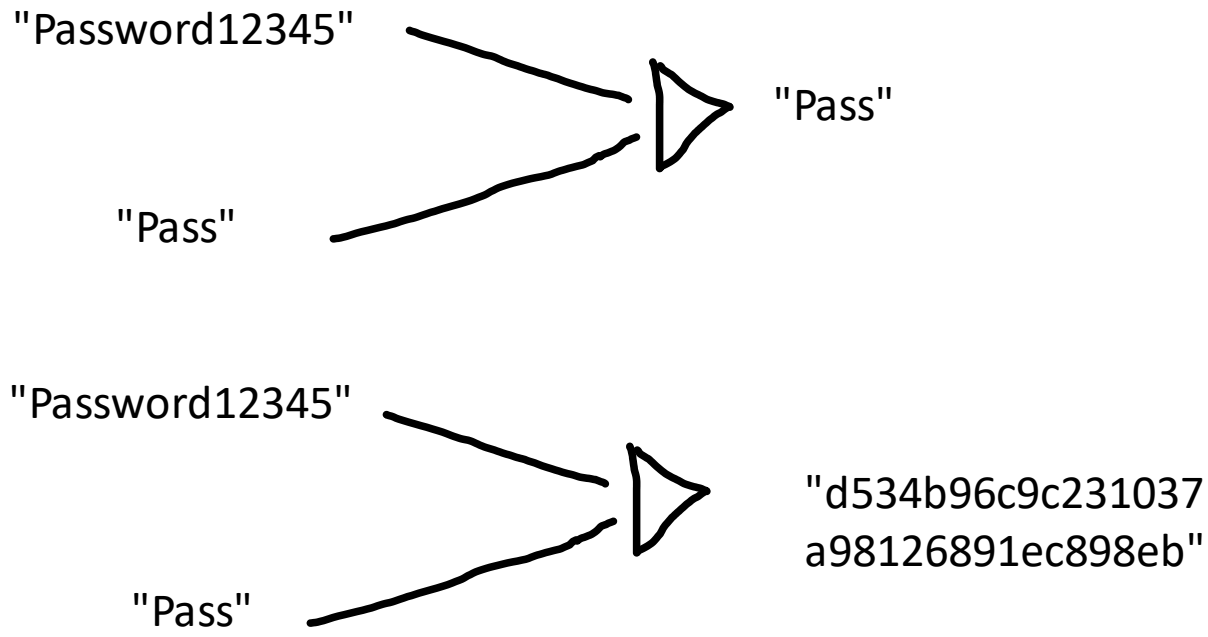
- Conflitos
- MD5
- Segurança

# Colisões

Colisões no contesto de segurança de informação

*"In computer science, a collision or clash is a situation that occurs when two distinct pieces of data have the same hash value, checksum, fingerprint, or cryptographic digest."*

Al-Kuwari, Saif; Davenport, James H.; Bradford, Russell J. (2011). "Cryptographic Hash Functions: Recent Design Trends and Security Notions"
https://eprint.iacr.org/2011/565/20120106:203023



# Hash rate

"One basic requirement of any cryptographic hash function is that it should be computationally infeasible to find two distinct messages that hash to the same value. Collisions can be found in seconds with a home computer.
The weaknesses of MD5 have been exploited in the field, most infamously by the Flame malware in 2012."

MD5 vulnerable to collision attacks
https://www.kb.cert.org/vuls/id/836068

| Method | Hashes per second |
|---|---|
| MD5 | 668896 |
| SHA-1 | 597014 |
| SHA-256 | 588235 |
| SHA-3 (224-bit) | 331674 |
| Bcrypt | 336 |

https://asecuritysite.com/encryption/htest

# Outras aplicabilidades de Hashing

- Message Digest
- Verificação de senha
- Estruturas de dados (Linguagem de programação)
- Operação de compilação
- …

# Referências bibliográficas


- https://www.devmedia.com.br/criptografia-md5/2944
- https://www.2brightsparks.com/resources/articles/introduction-to-hashing-and-its-uses.html
- https://www.geeksforgeeks.org/applications-of-hashing/
- Hashing Algorithms and Security – Computerphile
- SHA: Secure Hashing Algorithm - Computerphile
- https://academy.binance.com/pt/articles/what-is-hashing