Cursul nr. 13

STRUCTURI DE DATE neliniare

Tabele si functii de dispersie

Lector dr. Dorin IORDACHE

Agenda

01

Tabela hash

02

Functii hash

Tabele hash

01

Hash

Tabela hash

Structura de date a tabelului Hash stochează elemente în perechi **cheie-valoare** unde:

Cheie - întreg unic care este utilizat pentru indexarea valorilor

Valoare - date care sunt asociate cu chei.

Cheie	Data

Funcții hash

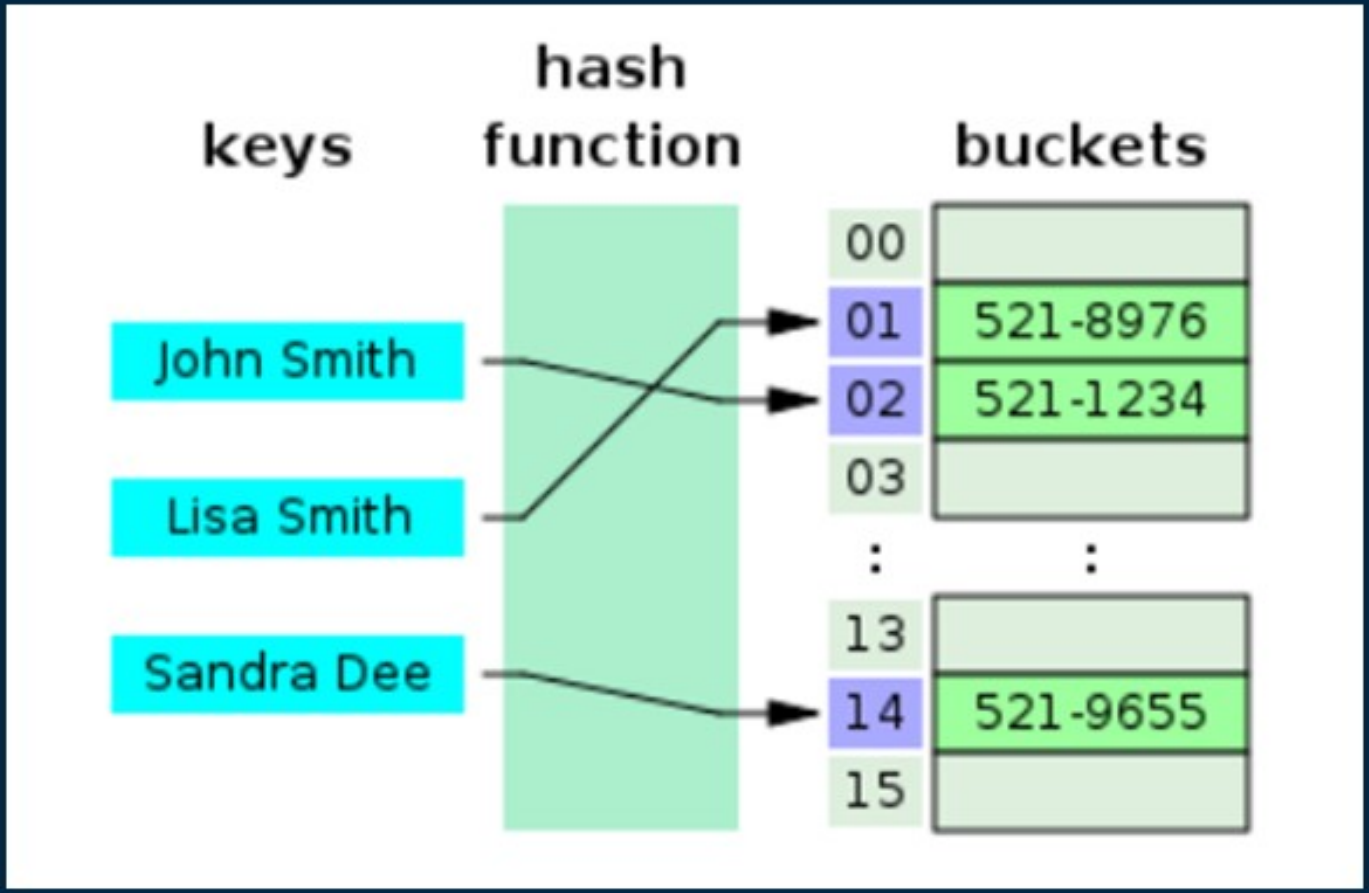
Într-o tabelă hash, un nou index este procesat folosind cheile. Elementul corespunzător acelei chei este stocat în index. Acest proces se numește hashing.

Fie k o cheie și **h(x)** o funcție **hash**.

Atunci **h(k)** va calcula un nou **index** pentru a stoca elementul legat cu k.

Tabela Hash

structura de date care mapează cheile la valori.



https://en.wikipedia.org/wiki/Hash_table

Tabela hash

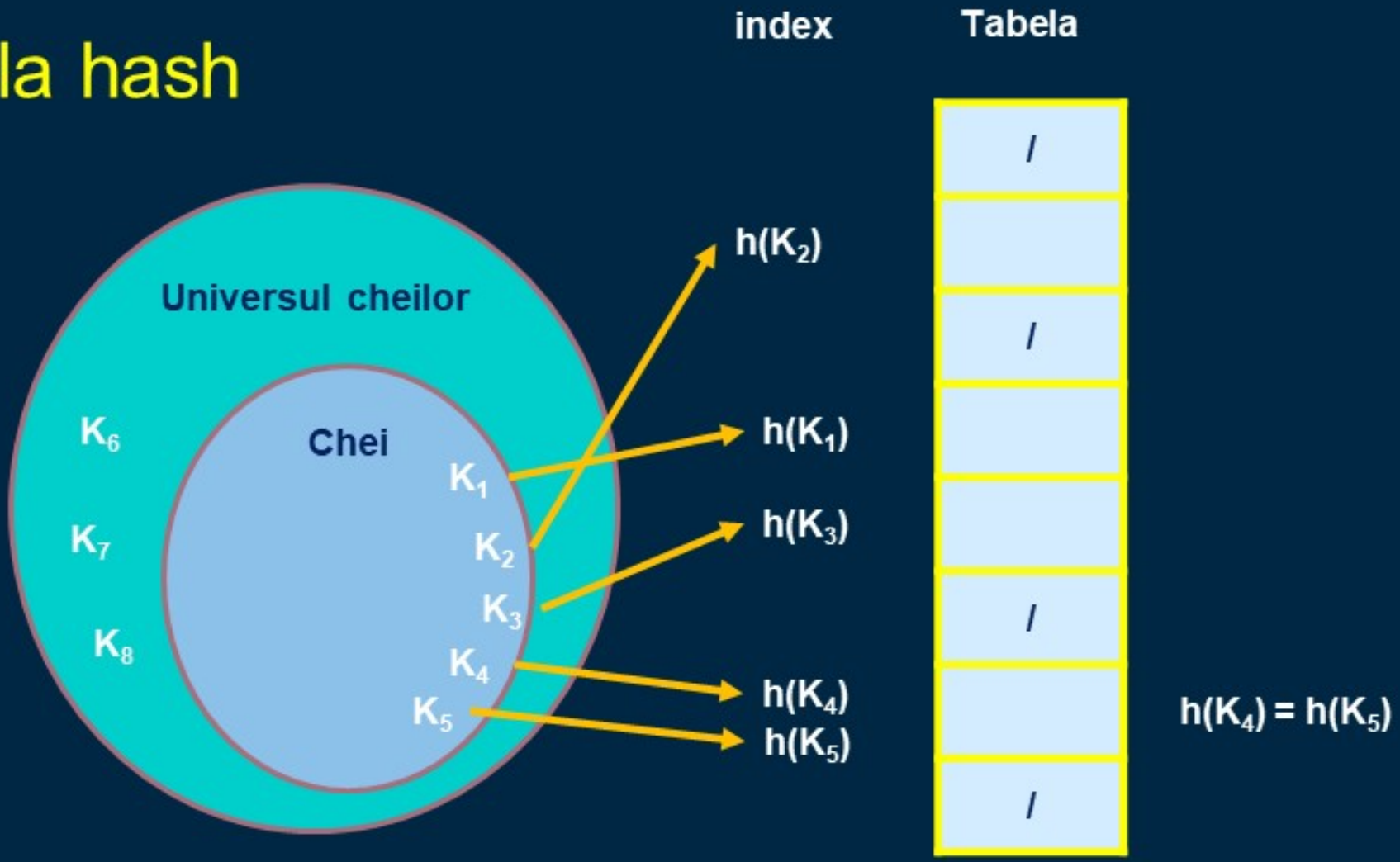
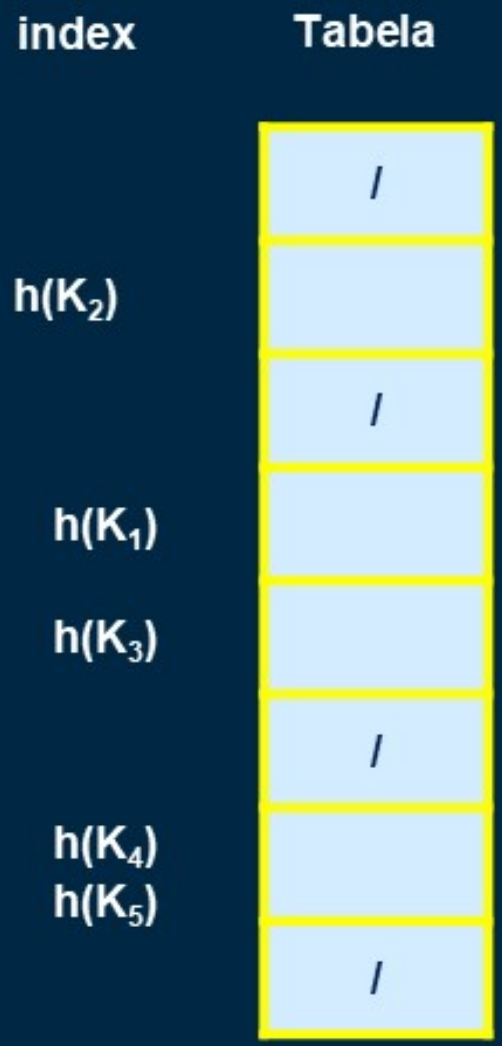

index
Tabela
Universul cheilor
Chei
K_6
K_7
K_8
K_1
K_2
K_3
K_4
K_5
$h(K_2)$
$h(K_1)$
$h(K_3)$
$h(K_4)$
$h(K_5)$
/
/
/
/
$h(K_4) = h(K_5)$

Tabela hash



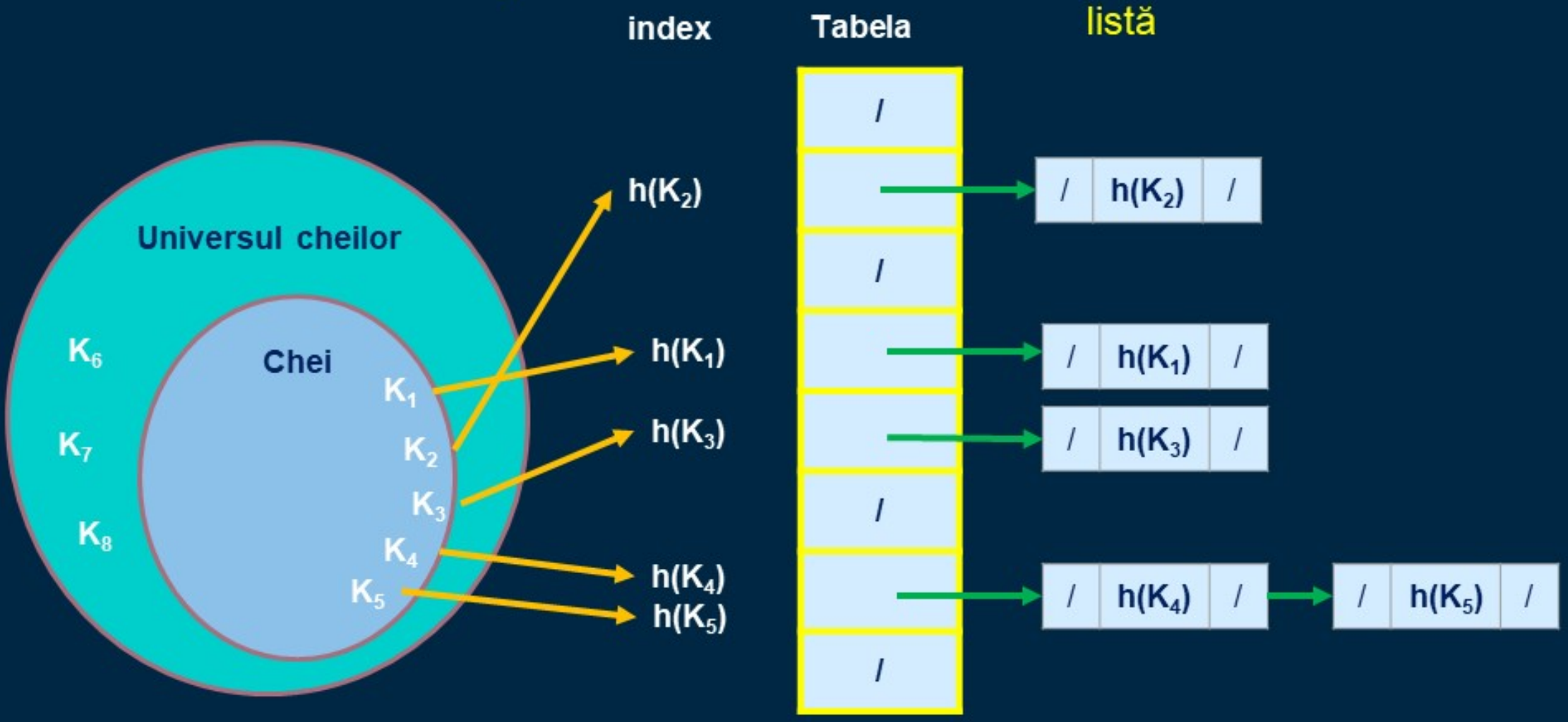
Coliziune = funcția hash generează același index pentru mai multe chei rezultă

Rezolvare coliziuni:

- **Înlănțuire** (atașare liste)
- **Adresare deschisă**: sondare liniară/cadratică și hashing dublu

$h(K_4) = h(K_5)$ coliziune

Coliziuni – înlănțuire



Hash table - exemplu

Date de intrare:
List = [11, 21, 24, 27, 29]

h(x) = [x % 10]

Aplicații ale hash table

- implementarea tablorurilor asociativi, ce au nume diferite în diferite limbaje de programare.

- actualizarea și stocarea unor algoritmi cu scopul creșterii vitezei de calcul.

- structuri de date bazate stocate pe HDD

- indexare a bazelor de date.

- Implementarea memoriei cache pentru a accelera accesul la date

- Implementarea obiectelor în diferite limbaje, ca: Python, JavaScript și Ruby.

Funcții hash

02

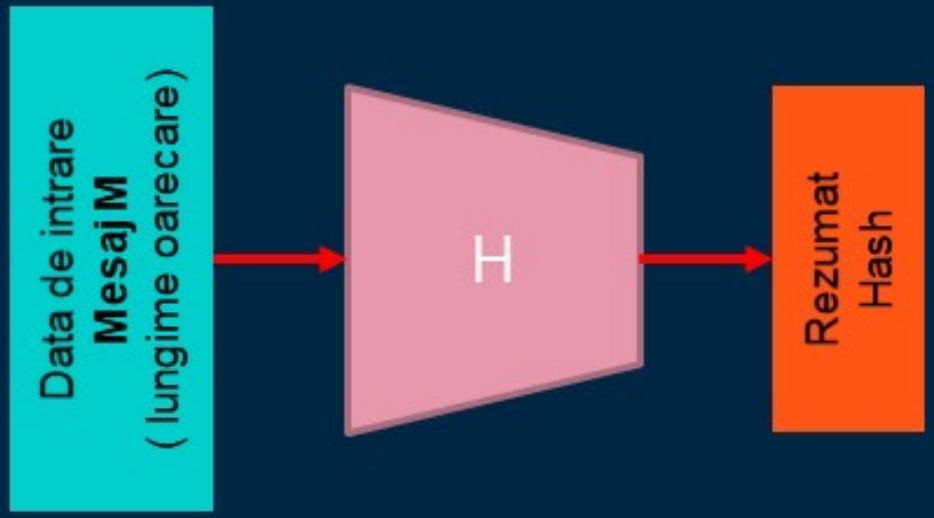
Funcții hash - definire

- = o funcție matematică care convertește o valoare numerică de intrare într-o altă valoare numerică comprimată.
- Intrarea în funcția hash este de lungime arbitrară, dar ieșirea este întotdeauna de lungime fixă

- Ieșirea = **mesage digest (rezumat)** sau pur și simplu valoare **hash**.

Funcții hash - definire

- = un identificator unic pentru orice anumit conținut.
- = un proces care preia date text simplu de orice dimensiune și le convertește într-un text cifrat unic de o anumită lungime.
- = un algoritm criptografic unidirecțional care mapează o intrare de orice dimensiune la o ieșire unică de o lungime fixă de biți.



Funcții hash – proprietăți

- = **Determinism** — întotdeauna ieșirea are dimensiunea identică, indiferent de dimensiunea intrării
- = **Nu este inversabilă** — procesul nu este inversabil, adică transformarea hash este one-way.
- = **Rezistență la coliziune** — probabilitate redusă de apariție a coliziunilor (coliziune - 2 intrări diferte să genereze aceeași ieșire)
- = **Efect de avalanșă** — orice modificare adusă unei intrări va avea ca rezultat o schimbare masivă a ieșirii
- = **Viteza de calcul hash** — operează într-un timp de execuție rezonabil.

Funcții hash - scop

- Asigurarea integrității datelor
- Securizarea împotriva modificărilor neautorizate
- Protejarea parolele stocate
- Funcționează la viteze diferite pentru a se potrivi cu diferite scopuri.

Funcții hash - scop

- Asigurarea integrității datelor
  - criptografia cu cheie publică, modalitate prin care se poate identifica dacă datele au fost modificate după ce au fost semnate, sau ca mijloc de verificare a identității.

- Securizarea împotriva modificărilor neautorizate
  - semnalează că mesajul a fost alterat (fără să știm și de către cine)
- Protejarea parolele stocate
  - stocarea aprolelor într/un format indescifrabil, dar verificabil
- Funcționează la viteze diferite pentru a se potrivi cu diferite scopuri.

Funcții hash - tipuri

- **Secure Hash Algorithm (SHA)** —familie de hashuri conține variantele SHA-1, SHA-2 , SHA-3 , **SHA-256**.
- **Message Digest (MD)** —familie de hashuri contine variantele MD2, MD4, MD5 și MD6.
- **Windows NTHash** - hash Unicode sau NTLM, folosit în mod obișnuit de sistemele de operare Windows

Aplicatii funcții hash

- Blocuri de date în criptomonede și alte tehnologii blockchain.
- Integritatea datelor software-ului, e-mailurilor și documentelor.
- Parole și stocarea hash-urilor de parole (mai degrabă decât parolele în sine) în bazele de date online.

https://www.fileformat.info/tool/hash.htm

Exemple

Results	
Original text	Salut
Original bytes	53:61:6c:75:74 (length=5)
Adler32	05ca020a
CRC32	7ee6d8b2
Haval	6696b0151a6be8123390d3f43423b585
MD2	acb89887d575ae0bbdb27b9ecfa11097
MD4	73941c1ca18127b17eccc73bf9463530
MD5	af4fef1bc0861ca2824db7315f844327
RipeMD128	77016a236df6f2a5906d185ae641cc18
RipeMD160	17ecf275beb9e965c6d037ae68c125305af13c28
SHA-1	9f57098c5534762dd32802302db78ada1ba864f5
SHA-256	75c4ec0328d2ec2e8cc1cfecda70808ab55a68645a100cd7b88b18ed9d44fd5d
SHA-384	55394275c9a5cdb62ea1aeb8d28b3ab8e97e5b23c050f5eef98dfe57a55355961c20522248afcc450009f59fdbfbd3f1
SHA-512	086035264d1272e19c8e5dcdd465ff4ed59c3d85f4bc3cd2d925254b99f7ef211a509b6cd75863dbf0357b452088d79401254fb0581286e2020ee7cb9da2eafc
Tiger	85d8635d01c4f0724723df15c229b67d0fb2ef0177651146
Whirlpool-0	09cdba9a2bf1502199fbc10120745fe7fed02e8955e6da0cc5cfa7e8b9b796da5573391ac977d287814ad11a0cff42edd3db7ecaaaf6abfbc42ba4205b7244ec null
Whirlpool-T	4ca9f4020711fa1eceaa20697094b62bd03b2d522df2df265cc0b42563f839d0e41e6ff03e696d418a5a610e7e6a8436b41ef2fd2b3c406ae7d41ccbe46a4c26
Whirlpool	fc44148170bacf313ad30479ee2125327c2da7550f88ca1dcf039af0e0425ee55e4675a5f9d96543aa9306b3e0ad047f2d5827bd4851d3045a409ef74fac3e23

Exemplu

SHA256

Salut

Hash

75c4ec0328d2ec2e8cc1cfecda70808ab55a68645a100cd7b88b18ed9d44fd5d

SHA-256	75c4ec0328d2ec2e8cc1cfecda70808ab55a68645a100cd7b88b18ed9d44fd5d

https://virtual-academy.ro/Crypto/sha256.html

Intrebari?

dorin.lordache@365.univ-ovidius.ro

Mulțumesc

CREDITS: This presentation template was created by Slidesgo, including icons by Flaticon, and infographics & images by Freepik