



# Cyber Summer School

Lector dr. Dorin IORDACHE

**Brute Force attack**

25-28.06.2024  
Facultatea de Matematică și Informatică

## Provocare

dpplo6++renpqwh) wywzaiu\*nk+Ynulpk+aq\*ljc

100-44 BC

Termen de rezolvare:

Joi, 27.06.2024 ora 16.00

**Warm-up**





Parola = cheie pentru a proteja dispozitivele și conturile online de orice acces neautorizat.

Cu toate acestea, majoritatea utilizatorilor încă *reutilizează parolele*, ceea ce duce la *scurgeri ale datelor*.

**Peste 80% din scurgerile de date rezultă din parole slabe sau folosite în mod repetat.**



**USD 4.45  
million**

The global average cost of a data breach in 2023 was USD 4.45 million, a 15% increase over 3 years.

**51%**

51% of organizations are planning to increase security investments as a result of a breach, including incident response (IR) planning and testing, employee training, and threat detection and response tools.

**USD 1.76  
million**


The average savings for organizations that use security AI and automation extensively is USD 1.76 million compared to organizations that don't.

<https://www.ibm.com/reports/data-breach>



## Password Statistics 2024 (Top Highlights)

- 30% of global data breaches result from weak passwords, with a notable 81% of company data breaches specifically attributed to poor password practices.
- 34% of users change their passwords once a month.
- Employees use the same password an average of 13 times.
- More than 6 million data records were exposed in the first quarter of 2023.
- 30% of internet users use Password Managers to track their passwords.



No. of characters used in password

Share of Americans

Up to 8 characters

16%

Between 8 to 11 characters

64%


Over 12 characters

20%

<https://www.statista.com/statistics/1305713/average-character-length-of-a-password-us/>

Sr.No.	Password	Count
1	123456	4.5 million
2	admin	4 million
3	12345678	1.37 million
4	123456789	1.21 million
5	1234	969,81
6	12345	728,414
7	password	710,321
8	123	528,086
9	Aa123456	319,725
10	1234567890	302,709





Here are further details about the inspirations that Americans use for their passwords.

- 22% use their own name.
- 33% use a pet's name.
- 14% use their children's names.
- 15% use a spouse or partner's name.

<https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/PasswordCheckup-HarrisPoll-InfographicFINAL.pdf>

[Alte statistici privitor la parole](#)



**Methods used to manage passwords**

**Percentage of Internet Users**

Have memorized password	55%
Written on Paper	32%
Use Password Manager	30%
Documented on Computer	23%
Stored in Email	20%

<https://bitwarden.com/resources/world-password-day/>

## Password management software

## Market Share

LastPass	23.30%
1Password	4.50%
Dashlane	3.96%
Keeper	3.38%
RoboForm	3.26%
Others	61.6%

LogMeOnce - free

<https://www.statista.com/statistics/1331322/password-management-market-share/>

## Summary: 10 Password Statistics for 2024

1. In 2023, 3 in 4 people globally were at risk of hacking
2. The average cost of data breaches reached \$4.45 million in 2023
3. 85% of people worldwide reuse passwords across multiple sites
4. "123456" was ranked as the most common password of the year, used 4 out of 5 times in 2023
5. Hackers can crack 17 out of the world's 20 most common passwords in less than a second
6. 40% of people are unaware if their passwords have ever been breached
7. Passwords make up almost 20% of the dark web listings
8. Compromised credentials facilitated 19% of breaches in 2023
9. Approximately 29% of boomers use unique passwords for every account
10. Passkeys are 40% faster than passwords



<https://passwordmeter.com/>

<https://haveibeenpwned.com/Passwords>



# Brute Force attack

# Avertisement

Ca și în alte cursuri, este posibil să întâlniți exemple de instrumente și tehnici aplicate unor adrese IP și resurse web reale.

**Nu executați niciodată niciunul dintre aceste instrumente și tehnici împotriva acestora!!!!**

# SHA 256

**Secure Hash Algorithm 256 (SHA-256) = funcție unidirecțională proiectată pentru securizarea informațiilor digitale.**

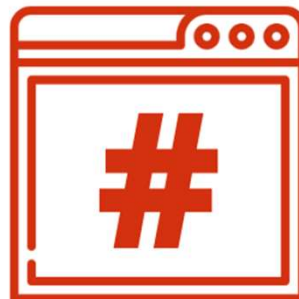


# Hash

## Hashing Algorithm



**Plain Text**



**Hash Function**



**Hashed Text**

## SHA-256

SHA-256 = funcție de calcul a rezumatului (semnătură) *hashing* similară cu SHA-1 sau MD5.

SHA-256 = un șir de caractere de dimensiune fixă ( 256 biți)

Rezumatul este unic - nu poate fi decriptat.

Cu toate acestea, poate fi *fisurat* prin forță brută sau comparând cu rezumatul unor șiruri cunoscute.

Hello = 185f8db32271fe25f561a6fc938b2e264306ec304eda518007d1764826381969

Generare SHA26 = <http://bit.ly/2vFsqst>



# SHA-256

SHA256("DATA") =

**c97c29c7a71b392b437ee03fd17f09bb10b75e879466fc0eb757b2c4a78ac938**

Modificati data de intrare ( concatenand la "DATA" valori numerice), astfel incat:

Spre exemplu: "DATA1" = 003edc2c0f73d673a8b7a76340f5e53cb9659efe68921389a853bd4e84ed5ed1

Rezumatul SHA256 sa inceapă:

- cu o cifra 0,
- cu 00
- 000

# SHA-256

SHA256(" ? ") =

**5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8**

# SHA-256

Fie urmatoarele secvente:

- 75c4ec0328d2ec2e8cc1cfecda70808ab55a68645a100cd7b88b18ed9d44fd5d
- 031c456c313a718d48a59c224a6512cbcb2b857855318357ca79ec3bcdd0d440
- 00cb39f035ccddb76a2d0563365d6985897a4cc69c96ccec1eb362e11ec719ac
- 093291ebfd9c14f9a1ede9d70e20061838c8b7d73bb8a4d246767b49476283cd
- 00d052af744e31cf2e1f32157d90c2efc7e208f2c2fe379012f4db9c0e902ad0
- 15bf0d0589f0cbd5209860f277426508717be0b8e1e8ea50d019b675197985cf

**Căutați o metodă de a afla mesajele de intrare (pentru fiecare) în parte !!!**

Download: <https://virtual-academy.ro/Crypto/valuesMD.txt>

# SHA-256

SHA256(" ? ") =

**5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8**

```
.\john.exe --format=raw-sha256 --wordlist=..\rockyou.txt ..\BlackTechHashes.txt
```

```
.\john.exe --format=raw-sha256 ..\BlackTechHashes.txt --show
```



Mulțumesc pentru atenție !

[dorin.iordache@365.univ-ovidius.ro](mailto:dorin.iordache@365.univ-ovidius.ro)