

# Contrasenyas I: Usuaris

Associació Hacking Lliure

25 d'octubre de 2017



# Índex

- 1 Presentació
- 2 Context
- 3 Complexitat
- 4 Factors d'autenticació
- 5 Gestors de contrasenyes
- 6 Alternatives a les contrasenyes
- 7 Conclusió

- 1 Presentació
- 2 Context
- 3 Complexitat
- 4 Factors d'autenticació
- 5 Gestors de contrasenyes
- 6 Alternatives a les contrasenyes
- 7 Conclusió

## Hacking Lliure

- Associació de Hacking Ètic i Seguretat Informàtica
- Gestada a les acaballes del 2016 per estudiants de la facultat
- Constituïda formalment a principis del 2017
- UB & Catalunya
- Presentació oficial: 27/02/17

# Índex

- 1 Presentació
- 2 Context**
- 3 Complexitat
- 4 Factors d'autenticació
- 5 Gestors de contrasenyes
- 6 Alternatives a les contrasenyes
- 7 Conclusió

# Problema 1: Contrasenyas trivials


00000


T'expliquem tot el que et cal saber sobre contrasenyes.


Dc. 25.10.17

12.15h - 13.30h

Aula B3 - Fac. Matemàtiques i Informàtica de la UB

 [hackinglliure.org](http://hackinglliure.org)

 [info@hackinglliure.org](mailto:info@hackinglliure.org)

 [@HackingLliure](https://twitter.com/HackingLliure)

# Problema 1: Contrasenyas trivials

121216

T'expliquem tot el que et cal saber sobre contrasenyes.

Dc. 25.10.17

12.15h - 13.30h

Aula B3 - Fac. Matemàtiques i Informàtica de la UB

[hackinglliure.org](https://hackinglliure.org)

[info@hackinglliure.org](mailto:info@hackinglliure.org)

[@HackingLliure](https://twitter.com/HackingLliure)

# Problema 1: Contrasenyas trivials


## PasswOrd


T'expliquem tot el que et cal saber sobre contrasenyes.


Dc. 25.10.17

12.15h - 13.30h

Aula B3 - Fac. Matemàtiques i Informàtica de la UB

 [hackinglliure.org](http://hackinglliure.org)

 [info@hackinglliure.org](mailto:info@hackinglliure.org)

 [@HackingLliure](https://twitter.com/HackingLliure)



# Problema 1: Contrasenyas trivials

abc123€


T'expliquem tot el que et cal saber sobre contrasenyes.


Dc. 25.10.17

12.15h - 13.30h

Aula B3 - Fac. Matemàtiques i Informàtica de la UB

 [hackinglliure.org](http://hackinglliure.org)

 [info@hackinglliure.org](mailto:info@hackinglliure.org)

 [@HackingLliure](https://twitter.com/HackingLliure)

# Problema 1: Contrasenyes trivials

# 1234aaA#


T'expliquem tot el que et cal saber sobre contrasenyes.


Dc. 25. 10. 17

12. 15h - 13. 30h

Aula B3 - Fac. Matemàtiques i Informàtica de la UB

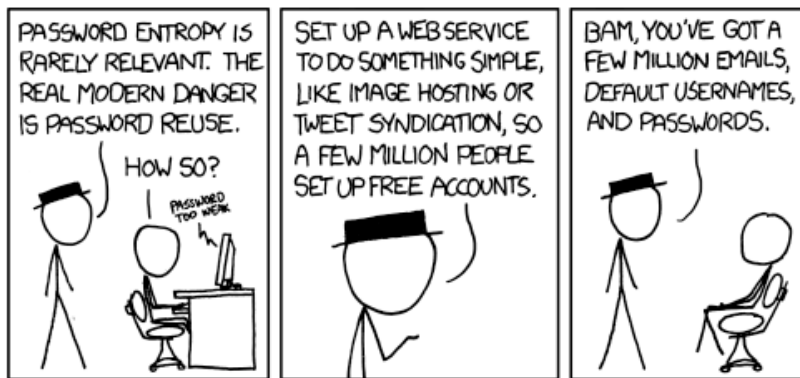
 [hackinglliure.org](http://hackinglliure.org)

 [info@hackinglliure.org](mailto:info@hackinglliure.org)

 [@HackingLliure](https://twitter.com/HackingLliure)

# Problema 2: Reutilització de contrasenyes

## Password Reuse



<https://xkcd.com/792/>

## Problema 2: Reutilització de contrasenyes

*"[...] the researcher came up with a password reuse rate of between 31% (best-case scenario) and 49% (higher estimate)."*

- [Softpedia.com](#) about an study at University of Cambridge

# Problema 3: Data Leaks

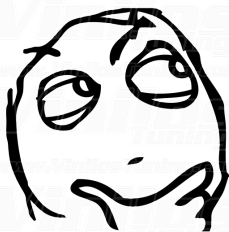
#	Count	Ciphertext	Plaintext
1.	1911938	EQ7fIpT7i/Q=	123456
2.	446162	j9p+HwtWWT86aMjgZFLzYg==	123456789
3.	345834	L8qbAD3jl3jioxG6CatHBw==	password
4.	211659	BB4e6X+b2xLioxG6CatHBw==	adobe123
5.	201580	j9p+HwtWWT/ioxG6CatHBw==	12345678
6.	130832	5djv7ZCI2ws=	qwerty
7.	124253	dQi0asWPYvQ=	1234567
8.	113884	7LqYzKVeQ8I=	111111
9.	83411	PMDTbP0LZxu03SwrFUvYGA==	photoshop
10.	82694	e6MPXQ5G6a8=	123123
11.	76910	j9p+HwtWWT8/HeZN+3oiCQ==	1234567890
12.	76186	diQ+ie23vAA=	000000
13.	70791	kCcUSCmonEA=	abc123
14.	61453	ukxzEcXU6Pw=	1234
15.	56744	5wEAIhH22i4=	adobe1
16.	54651	WqflwJFYW3+PsZVFZo1Ggg==	macromedia
17.	48850	hjAYSdUA4+k=	azerty
18.	47142	rpkvF+oZzQvioxG6CatHBw==	iloveyou
19.	44281	xz6PIeGzr6g=	aaaaaa
20.	43670	Ypsmk6AXQTK=	654321

<https://stricture-group.com/files/adobe-top100.txt>

- 1 Presentació
- 2 Context
- 3 Complexitat**
- 4 Factors d'autenticació
- 5 Gestors de contrasenyes
- 6 Alternatives a les contrasenyes
- 7 Conclusió

# Complexitat en contrasenyes

Què és una bona contrasenya?



Una bona contrasenya és aquella  
que **NO** pots recordar



# Complexitat en contrasenyes

Les contrasenyes són susceptibles a atacs de força bruta. És a dir, provar totes les combinacions de lletres, nombres i símbols.

Com més complexa\* sigui una contrasenya, més costarà de trobar, oi?

# Complexitat en contrasenyes

Ens acostumen a dir. . .

- Mínim 8 caràcters
- Majúscules
- Minúscules
- Dígits
- Símbols

# Complexitat en contrasenyes


1234aaA#


T'expliquem tot el que et cal saber sobre contrasenyes.


Dc. 25. 10. 17

12. 15h - 13. 30h

Aula B3 - Fac. Matemàtiques i Informàtica de la UB

 [hackinglliure.org](http://hackinglliure.org)

 [info@hackinglliure.org](mailto:info@hackinglliure.org)

 [@HackingLliure](https://twitter.com/HackingLliure)

# Complexitat en contrasenyes

D E M O

# Complexitat en contrasenyes

Utilitzant unes quantes paraules com a contrasenya obtenim una bona mida, però cal tenir en compte els atacs de diccionari (força bruta amb paraules en comptes de lletres).

# Complexitat en contrasenyes

Ens acostumen a dir...

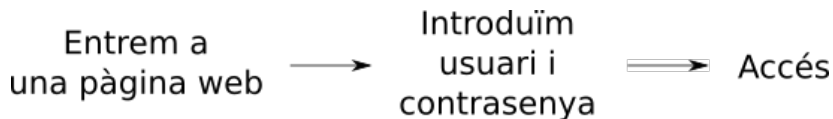
- Mida gran ( $\geq 16$ ), diferents tipus de caràcters
- A ser possible, utilitzar contrasenyes generades aleatòriament
- Evitar formació de contrasenyes amb dades personals
- Generador:
  - <https://www.grc.com/passwords>
  - <https://www.random.org/passwords> (només fins a 24 caràcters)

# Índex

- 1 Presentació
- 2 Context
- 3 Complexitat
- 4 Factors d'autenticació**
- 5 Gestors de contrasenyes
- 6 Alternatives a les contrasenyes
- 7 Conclusió

# Factors d'autenticació

Un exemple senzill:





# Factors d'autenticació

Si algú aconsegueix saber la contrasenya, podrà entrar al nostre compte quan vulgui (fins que ens n'adonem i la canviem).

# Factors d'autenticació

Si algú aconsegueix saber la contrasenya, podrà entrar al nostre compte quan vulgui (fins que ens n'adonem i la canviem).

La solució és demanar més credencials a banda de la contrasenya. És a dir, que algú amb l'usuari i contrasenya (i res més) no pugui accedir.

# Factors d'autenticació



# Factors d'autenticació



Exemples: targeta de coordenades bancàries, SMS al mòbil, aplicació d'autenticació...

# Factors d'autenticació

- ✓ Facebook, Twitter i Google ofereixen doble factor d'autenticació.
- ✓ Google ens proporciona maneres còmodes utilitzant un dispositiu Android: Authenticator.
- ✓ Llistat de webs: <https://twofactorauth.org/>

# Factors d'autenticació



## Two Factor Auth (2FA)

List of websites and whether or not they support [2FA](#).

Add your own favorite site by submitting a pull request on the [GitHub repo](#).

Q Search websites



Backup and Sync



Banking



Cloud Computing



Communication



Cryptocurrencies



Developer



Domains



Education



Email

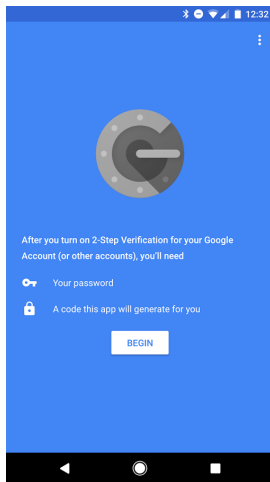


Entertainment



<https://twofactorauth.org>

# Factors d'autenticació



<https://www.google.com/landing/2step/>

Com evitar el robatori de múltiples comptes si hi ha un *leak*?

- Utilitzar contrasenyes diferents en diferents llocs web
- Si l'empresa (o administradors del web) en qüestió són seriosos, prendran mesures de contenció: comunicat als usuaris, rotació forçada de contrasenyes als comptes afectats
- Utilitzar **';-have i been pwned?**



# Data Leaks

The screenshot shows the homepage of the website 'have i been pwned?'. The site has a dark blue header with a navigation menu containing links for Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. The main content area is a teal gradient with a large white rounded rectangle containing the text ';-have i been pwned?'. Below this is a subtitle: 'Check if you have an account that has been compromised in a data breach'. A search bar is positioned below the subtitle, with the placeholder text 'email address or username' and a 'pwned?' button. At the bottom, a dark blue footer displays four statistics: 245 pwned websites, 4,792,153,725 pwned accounts, 56,419 pastes, and 53,743,186 paste accounts.

;-have i been pwned?

Check if you have an account that has been compromised in a data breach

email address or username **pwned?**

245	4,792,153,725	56,419	53,743,186
pwned websites	pwned accounts	pastes	paste accounts

<https://haveibeenpwned.com>

# Índex

- 1 Presentació
- 2 Context
- 3 Complexitat
- 4 Factors d'autenticació
- 5 Gestors de contrasenyes**
- 6 Alternatives a les contrasenyes
- 7 Conclusió

# Gestors de contrasenyes

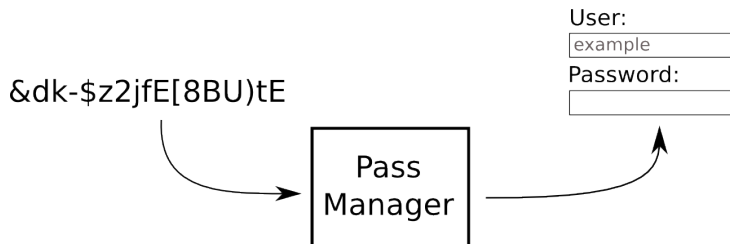
## Gestor de contrasenyes

Un gestor de contrasenyes és un software que ens permet generar, emmagatzemar i accedir a contrasenyes

# Gestors de contrasenyes

## Gestor de contrasenyes

Un gestor de contrasenyes és un software que ens permet generar, emmagatzemar i accedir a contrasenyes



# Gestors de contrasenyes no convecionals

## Gestor de contrasenyes determinista

Un *gestor de contrasenyes determinista* es caracteritza pel fet generar les contrasenyes a partir d'una *funció criptogràfica determinista*, en comptes d'emmagatzemar les generades.

- ✓ No necessita emmagatzemar contrasenyes
- ✓ Pot ser utilitzat en diferents dispositius sense cap sincronització
- ✗ Per a aconseguir rotació de contrasenyes, necessitem sincronitzar uns contadors
- ✗ No pot emmagatzemar dades diferents a contrasenyes aleatòries generades per la funció
- ✗ Un atacant pot generar totes les teves contrasenyes només sabent la *master key*

# Gestors de contrasenyes no convecionals

## Gestor de contrasenyes determinista

Un *gestor de contrasenyes determinista* es caracteritza pel fet generar les contrasenyes a partir d'una *funció criptogràfica determinista*, en comptes d'emmagatzemar les generades.

- ✓ No necessita emmagatzemar contrasenyes
- ✓ Pot ser utilitzat en diferents dispositius sense cap sincronització
- ✗ Per a aconseguir rotació de contrasenyes, necessitem sincronitzar uns contadors
- ✗ No pot emmagatzemar dades diferents a contrasenyes aleatòries generades per la funció
- ✗ Un atacant pot generar totes les teves contrasenyes només sabent la *master key*

# Gestors de contrasenyes no convecionals

## Gestor de contrasenyes determinista

Un *gestor de contrasenyes determinista* es caracteritza pel fet generar les contrasenyes a partir d'una *funció criptogràfica determinista*, en comptes d'emmagatzemar les generades.

- ✓ No necessita emmagatzemar contrasenyes
- ✓ Pot ser utilitzat en diferents dispositius sense cap sincronització
- ✗ Per a aconseguir rotació de contrasenyes, necessitem sincronitzar uns contadors
- ✗ No pot emmagatzemar dades diferents a contrasenyes aleatòries generades per la funció
- ✗ Un atacant pot generar totes les teves contrasenyes només sabent la *master key*

# Gestors de contrasenyes no convecionals

## Gestor de contrasenyes determinista

Un *gestor de contrasenyes determinista* es caracteritza pel fet generar les contrasenyes a partir d'una *funció criptogràfica determinista*, en comptes d'emmagatzemar les generades.

- ✓ No necessita emmagatzemar contrasenyes
- ✓ Pot ser utilitzat en diferents dispositius sense cap sincronització
- ✗ Per a aconseguir rotació de contrasenyes, necessitem sincronitzar uns contadors
- ✗ No pot emmagatzemar dades diferents a contrasenyes aleatòries generades per la funció
- ✗ Un atacant pot generar totes les teves contrasenyes només sabent la *master key*



# Gestors de contrasenyes no convecionals

## Gestor de contrasenyes determinista

Un *gestor de contrasenyes determinista* es caracteritza pel fet generar les contrasenyes a partir d'una *funció criptogràfica determinista*, en comptes d'emmagatzemar les generades.

- ✓ No necessita emmagatzemar contrasenyes
- ✓ Pot ser utilitzat en diferents dispositius sense cap sincronització
- ✗ Per a aconseguir rotació de contrasenyes, necessitem sincronitzar uns contadors
- ✗ No pot emmagatzemar dades diferents a contrasenyes aleatòries generades per la funció
- ✗ Un atacant pot generar totes les teves contrasenyes només sabent la *master key*

# Gestors de contrasenyes no convecionals

## Gestor de contrasenyes determinista

Un *gestor de contrasenyes determinista* es caracteritza pel fet generar les contrasenyes a partir d'una *funció criptogràfica determinista*, en comptes d'emmagatzemar les generades.

- ✓ No necessita emmagatzemar contrasenyes
- ✓ Pot ser utilitzat en diferents dispositius sense cap sincronització
- ✗ Per a aconseguir rotació de contrasenyes, necessitem sincronitzar uns contadors
- ✗ No pot emmagatzemar dades diferents a contrasenyes aleatòries generades per la funció
- ✗ Un atacant pot generar totes les teves contrasenyes només sabent la *master key*

# Recomanacions sobre gestors de contrasenyes

## Característiques que valorarem en un gestor de contrasenyes

- **No determinista**
  - De codi obert
  - Permet la rotació (canvi) de contrasenyes
  - Amb capacitat per guardar tot tipus de dades
  - Ofereix control i configuració a l'usuari
  - Utilitza "bona" criptografia
  - Permet generar contrasenyes amb molta entropia
  - Integració amb el navegador

# Recomanacions sobre gestors de contrasenyes

## Característiques que valorarem en un gestor de contrasenyes

- No determinista
- De codi obert
- Permet la rotació (canvi) de contrasenyes
- Amb capacitat per guardar tot tipus de dades
- Ofereix control i configuració a l'usuari
- Utilitza "bona" criptografia
- Permet generar contrasenyes amb molta entropia
- Integració amb el navegador

# Recomanacions sobre gestors de contrasenyes

## Característiques que valorarem en un gestor de contrasenyes

- No determinista
- De codi obert
- Permet la rotació (canvi) de contrasenyes
- Amb capacitat per guardar tot tipus de dades
- Ofereix control i configuració a l'usuari
- Utilitza "bona" criptografia
- Permet generar contrasenyes amb molta entropia
- Integració amb el navegador

# Recomanacions sobre gestors de contrasenyes

## Característiques que valorarem en un gestor de contrasenyes

- No determinista
- De codi obert
- Permet la rotació (canvi) de contrasenyes
- Amb capacitat per guardar tot tipus de dades
- Ofereix control i configuració a l'usuari
- Utilitza "bona" criptografia
- Permet generar contrasenyes amb molta entropia
- Integració amb el navegador

# Recomanacions sobre gestors de contrasenyes

## Característiques que valorarem en un gestor de contrasenyes

- No determinista
- De codi obert
- Permet la rotació (canvi) de contrasenyes
- Amb capacitat per guardar tot tipus de dades
- Ofereix control i configuració a l'usuari
- Utilitza “bona” criptografia
- Permet generar contrasenyes amb molta entropia
- Integració amb el navegador

# Recomanacions sobre gestors de contrasenyes

## Característiques que valorarem en un gestor de contrasenyes

- No determinista
- De codi obert
- Permet la rotació (canvi) de contrasenyes
- Amb capacitat per guardar tot tipus de dades
- Ofereix control i configuració a l'usuari
- Utilitza “bona” criptografia
- Permet generar contrasenyes amb molta entropia
- Integració amb el navegador



# Recomanacions sobre gestors de contrasenyes

## Característiques que valorarem en un gestor de contrasenyes

- No determinista
- De codi obert
- Permet la rotació (canvi) de contrasenyes
- Amb capacitat per guardar tot tipus de dades
- Ofereix control i configuració a l'usuari
- Utilitza “bona” criptografia
- Permet generar contrasenyes amb molta entropia
- Integració amb el navegador

# Recomanacions sobre gestors de contrasenyes

## Característiques que valorarem en un gestor de contrasenyes

- No determinista
- De codi obert
- Permet la rotació (canvi) de contrasenyes
- Amb capacitat per guardar tot tipus de dades
- Ofereix control i configuració a l'usuari
- Utilitza “bona” criptografia
- Permet generar contrasenyes amb molta entropia
- Integració amb el navegador

# Recomanacions sobre gestors de contrasenyes

## Closed Source

LastPass  
DashLane

## Open Source



KeePassXC



Usability

Privacy & Security

# Exemple d'utilització de KeePassXC

D E M O

# Índex

- 1 Presentació
- 2 Context
- 3 Complexitat
- 4 Factors d'autenticació
- 5 Gestors de contrasenyes
- 6 Alternatives a les contrasenyes**
- 7 Conclusió

Per què és tan complicat tractar correctament contrasenyes?



Per què és tan complicat tractar correctament contrasenyes?



No tenim cap altra opció més simple?

# Login mitjançant email

El lloc web només demana l'email de l'usuari quan aquest hi vol accedir



# Login mitjançant email

El lloc web només demana l'email de l'usuari quan aquest hi vol accedir

L'usuari rebrà al seu email un link o contrasenya temporal d'un sol ús que li permetrà entrar al seu compte

# Login mitjançant email

El lloc web només demana l'email de l'usuari quan aquest hi vol accedir

L'usuari rebrà al seu email un link o contrasenya temporal d'un sol ús que li permetrà entrar al seu compte

Això equival a utilitzar l'email com hem vist amb els factors d'autenticació, però com a mètode primari per a fer login

# Índex

- 1 Presentació
- 2 Context
- 3 Complexitat
- 4 Factors d'autenticació
- 5 Gestors de contrasenyes
- 6 Alternatives a les contrasenyes
- 7 Conclusió**

# Conclusió

- Contrasenyes segures (llargues, complexes)
- No reutilitzar-les
- Activar 2FA
- Subscriu-re's a *';-have i been pwned?*
- Gestor de contrasenyes

## **My \$50,000 Twitter Username Was Stolen Thanks to PayPal and GoDaddy**

Gràcies per la vostra atenció



<https://hackinglliure.org>

<https://twitter.com/hackinglliure>

[info@hackinglliure.com](mailto:info@hackinglliure.com)