It’s time to talk about passwords

these are nice tips

Why do we even need passwords?

- To prove who you are on the internet. (Paired with public identity, I.E Username)
- To keep secrets from others. (Icloud?)
- To get access to restricted resources (Mails?, VPN login)

What happens if someone gets your password?

- Steal your secrets (Icloud, or spisorvis secret recipes)
  - Blackmail you?
- Impersonate you
  - Send a mail from your account?
- Steal your valuables?
  - No more bitcoinsss (or bank account)

So I should make 1 really good password?

- No, this is really bad.
  - Using 1 hard password everywhere is almost as bad as using a weak one everywhere.
- Passwords gets leaked online

Biggest data breaches

1. Adobe
2. Adult Friend Finder
3. Canva
4. Dubsmash
5. eBay
6. Equifax
7. Heartland Payment Systems
8. LinkedIn
9. Marriott International
10. My Fitness Pal
11. MySpace
12. NetEase
13. Sina Weibo
14. Yahoo
15. Zynga

Why can hackers steal my password?

- Because service providers are fucking stupid
- Password databases gets stolen from big sites where you signed up.
- Hackers now have your password.

So how can we do this a bit better?

Introduction to Hashing

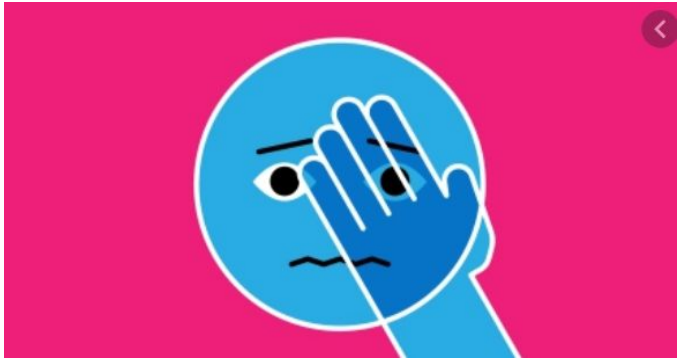
Don’t store passwords in the database, but store them as the result of a salted hash

+

Storing passwords securely. 1st Idea

SELECT * FROM USERS;

id	*mail*	*password*
1	ehorni20@student.aau.dk	MolotovErSød123!



Storing passwords securely. 2nd idea

SELECT * FROM USERS;

id	*mail*	*password*
1	ehorni20@student.aau.dk	e0506ed60502047839582f5f7c358c75

Hmmmmmmmmmmmmmmmmm

Storing passwords securely. 2nd idea

SELECT * FROM USERS;

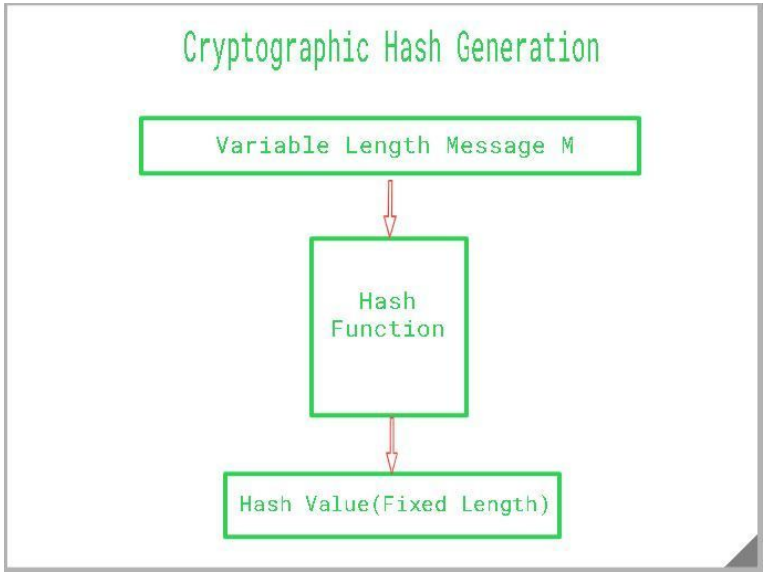
id	*mail*	*password*
1	ehorni20@student.aau.dk	e0506ed60502047839582f5f7c358c75

HASHFUNCTION

Hmmmmmmmmmmmmmmmmm

WHAT THE FUCK IS A HASHFUNCTION?

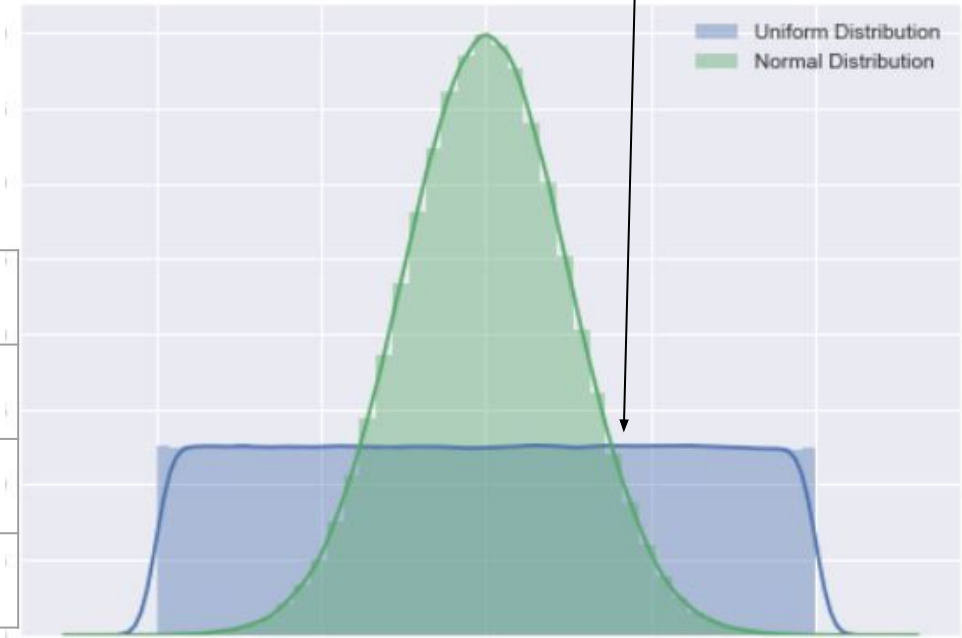
- A **hash function** is any function that can be used to map data of arbitrary size to fixed-size values.
- Any change to the input produces significant change to the output
- Hashing is a **one way** function, and is irreversible
- It is **infeasible** to find out which input produces a specific output.
- It is **infeasible** to find two inputs that produces the same output.



WHAT THE FUCK IS A HASHFUNCTION 2?

- The output of many calls to the hash function should approximate towards a uniform distribution
- A small change to the input will produce a large change in the output

Input	Output
Molotov1	39bfede469a7556f162c8ba0d2169e3c
Molotov2	b2c5fd190a56a956aa9f990a723367f3
	bf9222142df61c434d658b6986419fc3



Storing passwords securely. 2nd idea

SELECT * FROM USERS;

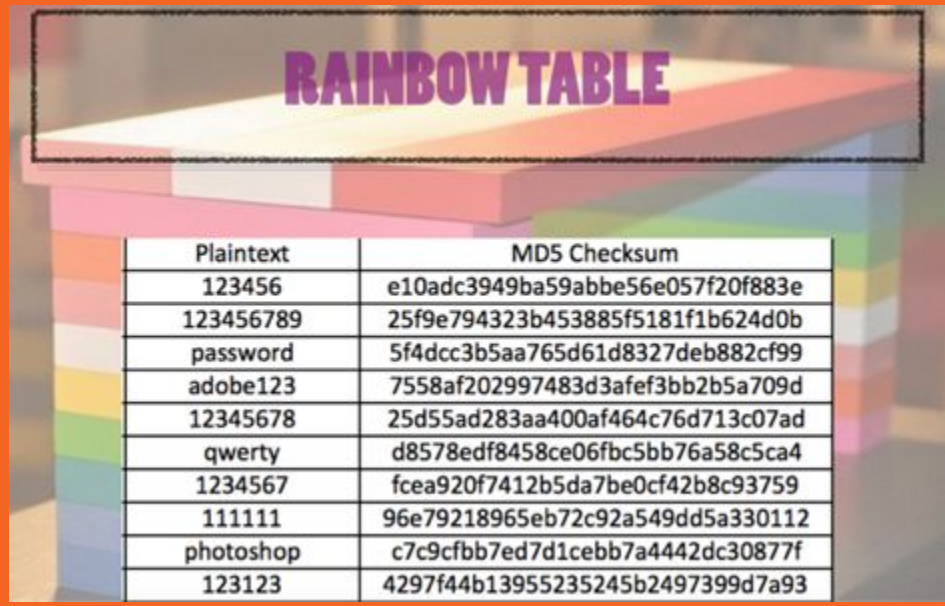
id	*mail*	*password*
1	ehorni20@student.aau.dk	e0506ed60502047839582f5f7c358c75

Store the hash instead of the password

This is still really bad :-)

Attackers will use a rainbow table

Basically a big list of passwords and their hashes



Plaintext	MD5 Checksum
123456	e10adc3949ba59abbe56e057f20f883e
123456789	25f9e794323b453885f5181f1b624d0b
password	5f4dcc3b5aa765d61d8327deb882cf99
adobe123	7558af202997483d3afef3bb2b5a709d
12345678	25d55ad283aa400af464c76d713c07ad
qwerty	d8578edf8458ce06fbc5bb76a58c5ca4
1234567	fcea920f7412b5da7be0cf42b8c93759
111111	96e79218965eb72c92a549dd5a330112
photoshop	c7c9cfbb7ed7d1cebb7a4442dc30877f
123123	4297f44b13955235245b2497399d7a93

So when hackers get the database, they just in their rainbow table.

(Will get a lot of the passwords this way)

The fix

Some random value
prepended to the pass

kills rainbowtables

Storing passwords securely. 3rd Idea

SELECT * FROM USERS;

id	*mail*	*Salt*	*password*
1	ehorni20@student.aau.dk	‘abcdefg123’	e0506ed60502047839582f5f7c358c75

Store the SALTED hash instead of the password

Living example

*“Yo man, Here is my password: **Penge123**, Can i log into TFT please?”*

“Yo let me check”

Living Example

```
1.   See input              : Penge123!
2.   Add salt               :
     abcdefg123Penge123!
3.   Take hash              : e0506ed60502047…
4.   Check if they match    : MATCH
```

id	*mail*	*Salt*	*password*
1	Madsdam@cbs.dk	‘abcdefg123’	e0506ed60502047839582f5f7c358c75

Living example

“bro you can log in”

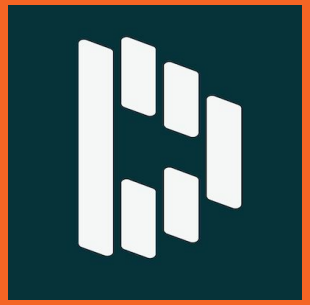
“nice”

This is the best we can do

but it still sucks

Always protecting passwords is impossible.

So what do we do??



Use a password manager

- Different passwords for every single site
- Just keep 1 password very secret!
- Assume Password managers are not compromised.