Hashfunktioner og salt!

Hvad er problemet med denne tabel?

(uden `password` kolonnen)

id	brugernavn	password	hashed_password
#	enter text	enter text	enter text
1	"malene"	12345	"d098470589829ee3c27420978d6407dd03230a514
2	"admin"	"admin"	"8c6976e5b5410415bde908bd4dee15dfb167a9c873fc
3	"peter@mail.dk"	"qwerty"	"65e84be33532fb784c48129675f9eff3a682b27168c0
4	"olebent@haderslev.dk"	"password"	"5e884898da28047151d0e56f8dc6292773603d0d6aa
5	"mette"	"password"	"5e884898da28047151d0e56f8dc6292773603d0d6aa

Hash funktionen er deterministisk

"olebent@haderslev.dk"	"password"	"5e884898da28047151d0e56f8dc6292773603d0d6aa
"mette"	"password"	"5e884898da28047151d0e56f8dc6292773603d0d6aa

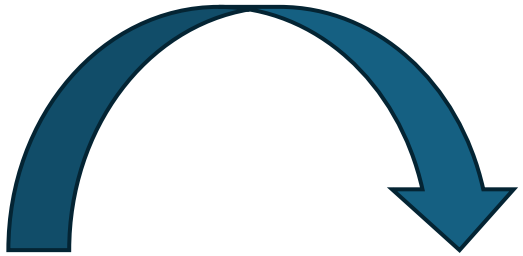
Problemer

1) Hvis hackeren har held til at gætte Ole Bent's password, så har hackeren også Mettes password.

2) Hvis der er mange ens hashværdier: Det kan være tegn på, at websiden har et default password.

Rainbow attacks

+ hashfunktion



Sammenlign hash-værdi med hash-værdien fra den stjålne password-tabel.

Hash table

Ord fra ordbogen + tilfældige strenge + mest brugte passwords	Hash-værdi
…	…
…	…
…	…
…	…

Sammenlign hash-værdi med hash-værdien fra den stjålne password-tabel.

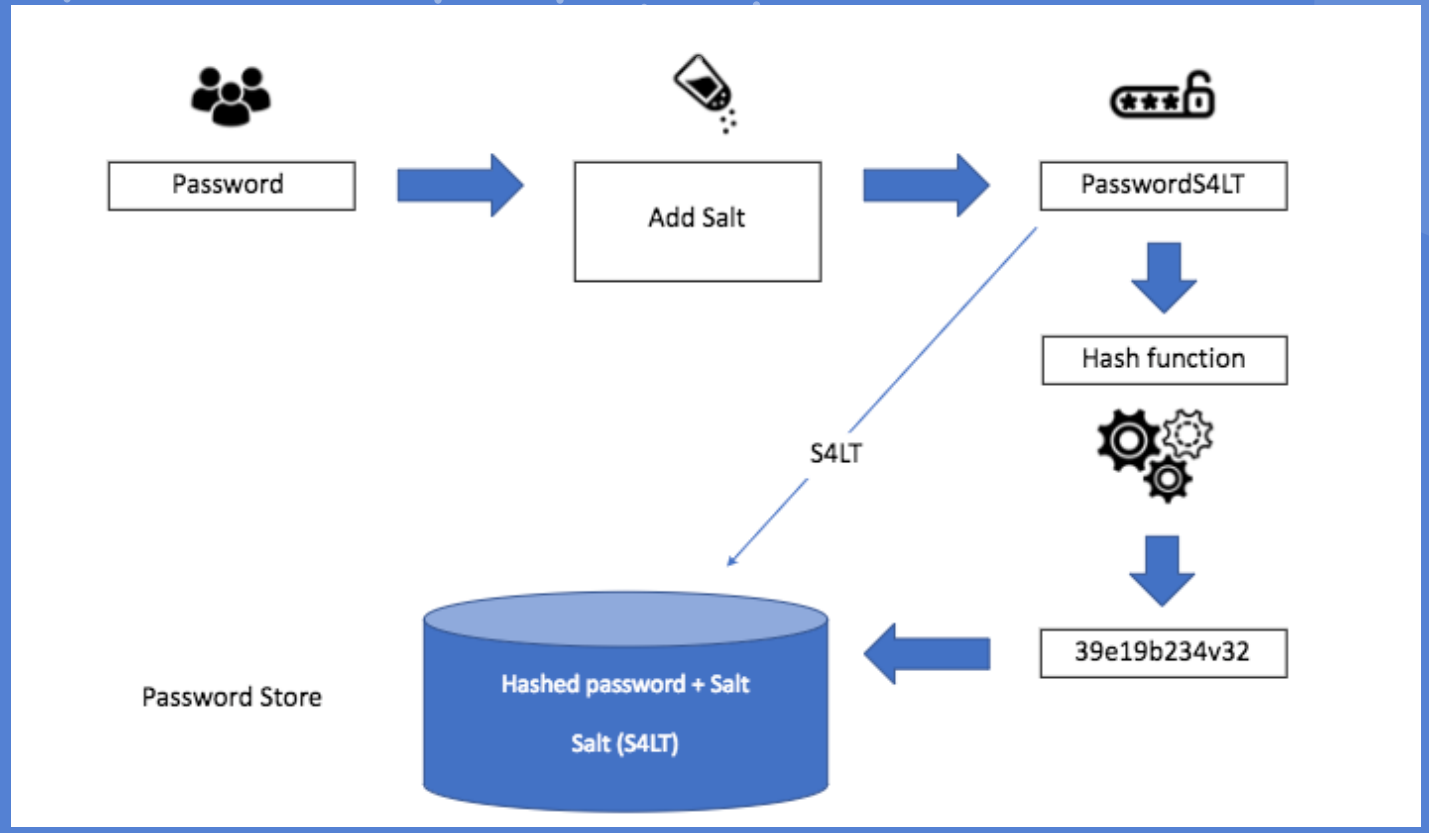
- Fordel: Pre-computed
- Ulempe: Hash tabellen fylder meget

Løsningen er...

Salt

- Salt: Til hver bruger generes et tilfældigt ord/tal (det er der metoder til at gøre smart og sikkert)

- Salt: Får hashfunktionen til at se ikke-deterministisk ud



Hvorfor er det smart?

Password	p4s5w3rdz	p4s5w3rdz	p4s5w3rdz	p4s5w3rdz
Salt	-	-	et52ed	ye5sf8
Hash	f4c31aa	f4c31aa	lvn49sa	z32i6t0

Den nye tabel med salt

id	brugernavn	password	salt	hash_incl_salt
#	enter text	enter text	enter text	enter text
1	"malene"	"12345"	555	"5d10159a84dcf991bad3d7a463e2c7d3c244080afe84
2	"admin"	"admin"	29	"0219ee3bbf6349d10f6850f60a7114be81858d97d9c3
3	"peter@mail.dk"	"qwerty"	343	"deb7ff579536972bc86d4c7df861fa951b6ef21edeaf43
4	"olebent@haderslev.dk"	"password"	462	"dceb275af153f81979e06594e1ebed73180b54f3e5a85
5	"mette"	"password"	656	"5ef34b1a52fcfdd4766627606fc073a2e3fc5523bc690