Lab 4

> ## Password-hashing (iterative hashing, salt, memory-hard functions)

Osnovni koncepti za sigurnu pohranu lozinki:

- klasične (brze) kriptografske hash funkcije
- specijalizirane (spore i memorijski zahtjevne) kriptografske funkcije za sigurnu pohranu zaporki
- Pre-computed dictionary attack →pohranjuje se lista kandidata za lozinke, lozinke se hashiraju te se uspoređuju s hashom tražene lozinke
- da bi se spriječili takvi napadi koriste se iterativno hashiranje i **salt lozinke**
- sol je niz karaktera,znakova koji se dodaju na kraj lozinke i time se otežava napadaču da dođe do lozinke pretraživanjem po rječniku
- hash fje. su puno brže od specijaliziranih te je za što precizniji rezultat potrebo napraviti što više iteracija