Opbevaring af kodeord

I opbevaring af kodeord er der normalt tre metoder, som man snakker om, plain text, krypteret og og haset.

Plain text er i nomalt text, man tager bare kode ordoredt og skriver det ned, vis opbevare ens kodeord på en stiky note eller på en pairs blok, vil det normalt blive betrketet som at være i plain text. Dette er ikke sikker måde at opbevare kloder på, vis en for ad gang til stikky noten, pairs blokken eller Word dokumentet vile de kunne læse koden oden probemer.

Krypteing er hvor man tager kodeordet og skifter tegne ud med andre, metoden til hvordan vælger nye tegn er ikke bare tilfældigt, men der er mange forskelige metoder, nogle mere simple end andre. En vigtig ting ved kryptering, er at når en tekst kan man også dekryptere den så man for den originale tekst igen, ved at gøre det omvendte da teksten blev krypteret. Måske den mest simple metode er cæsarmetoden, hvor man tager og skifter bokstaverne med det næste bokstav i alfabetet, så vis der er et ”A” i kodeordet ville det blivet skiftet ud med ”B”, for at dekryptere med cæsarmetoden bedtes bogstevet ud med bogstevet der kommer før det i alfabetet så ”B” bliver til ”A”. Der mange andre metoder til at kryptere en tekst og de stærkeste metoder gør brug af computer algoritmer, men kan altid dekrypteres tilbage til origal teksten.

Hasing mindes om kryptering, men den største forskel er at hasing ikke kan dekryptes ved at omvende hasings algoritmen,

<https://www.it.ucsb.edu/secure-compute-research-environment-user-guide/password-best-practices>

<https://auth0.com/blog/hashing-passwords-one-way-road-to-security/>

<https://www.sailpoint.com/identity-library/password-management-best-practices/>