

# ◆ Lærerveiledning - Trygg lagring av passord

*Kurs: Python*

*Tema: Tekstbasert, Kryptografi*

*Fag: Programmering*

*Klassetrinn: 8.-10. klasse, Videregående skole*

## Om oppgaven

Denne oppgaven inngår i en serie om kryptografi, og handler om hvordan man kan lagre passord på en trygg måte, noe som igjen forklarer hvorfor man bør lage passordene sine på spesielle måter. Det anbefales å gå gjennom følgende oppgaver før man starter på denne:

- ☐ Hemmelige koder (../hemmelige\_koder/hemmelige\_koder.html)
- ☐ Hash-funksjoner (../hash-funksjoner/hash-funksjoner.html)

Det kan være en fordel å repetere leksjonen om ordbøker,

- ☐ Ordbøker (../ordboeker/ordboeker.html)

Oppgaven er ikke testet på hele målgruppen, så tilbakemeldinger på nivået og egnede trinn er velkomne.

## Oppgaven passer til:

**Fag:** Programmering

**Anbefalte trinn:** 8. trinn--VG3

**Tema:** Kryptografi, passord, IT-sikkerhet

**Tidsbruk:** Dobbeltime

## Kompetansemål

- ☐ **Valgfag programmering:** Prinsipper som ligger til grunn for god programmeringspraksis inngår også i hovedområdet, deriblant forklaring og dokumentasjon av løsninger og programkode; vurdering og analyse av egen og andres programkode (Fra hovedområdene)
- ☐ **Valgfag programmering:** omgjøre problemer til konkrete delproblemer

## Forslag til læringsmål

- ☐ Elevene forstår hvorfor passord ikke bør lagres i klartekst
- ☐ Elevene forstår hvorfor man bør salte passord
- ☐ Elevene forstår hvorfor man ikke ønsker å bruke raske funksjoner for å hashe passord.

## Forslag til vurderingskriterier

- ☐ Eleven oppnår middels måloppnåelse ved å fullføre oppgaven
- ☐ Eleven oppnår høy måloppnåelse ved å etterpå kunne forklare hvorfor noen passord er bedre enn andre, og hvorfor enkle erstatningsteknikker som "l" til "1" og "e" til "3" ikke gir ekstra sikkerhet

## Forutsetninger og utstyr

- ☐ **Forutsetninger:** God kjennskap til Python. Gjennomført tidligere oppgaver som beskrevet over.
- ☐ **Utstyr:** Datamaskin med Python 3.4 eller høyere installert

# Fremgangsmåte

Vi har dessverre ikke noen konkrete tips, erfaringer eller utfordringer tilknyttet denne oppgaven enda.

Denne leksjonen er noe mer krevende programmeringsmessig enn de fleste andre leksjonene i kryptografi-serien. Den bør likevel være gjennomførbar fordi den krever forholdsvis liten egeninnsats, og vil forhåpentligvis være spennende fordi den er så tett innpå det som er *best practice* i den virkelige verden.

## Variasjoner

## Eksterne ressurser

- ☐ Fra kanalen *Computerphile* på YouTube: Password Cracking - Computerphile (<https://www.youtube.com/watch?v=7U-RbOKanYs>)

Lisens: CC BY-SA 4.0 (<http://creativecommons.org/licenses/by-sa/4.0/deed>)