Python

◆ 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, IT1, IT2

Anbefalte trinn: 8. trinn--VG3

Tema: Kryptografi, passord, IT-sikkerhet

Tidsbruk: Dobbeltime

Kompetansemål

- [ ] **IT1, VG2**: lese, strukturere, analysere og kommentere programkode
- [ ] **IT1, VG2**: utforske trusler mot datasikkerheten og kjenne til beskyttende tiltak for noen av disse
- [ ] **IT2, VG3**: beskrive hvordan data kan beskyttes ved hjelp av tilgangskontroll og kryptering
- [ ] **IT2, VG3**: kartlegge og analysere trusler, sårbarheter og risiko i informasjonssystemer
- [ ] **Programmering, 10. trinn**: bruke grunnleggende prinsipper i programmering, slik som variabler, løkker, vilkår og funksjoner, og reflektere over bruken av disse
- [ ] **Programmering, 10. trinn**: analysere problemer, gjøre dem om til delproblemer og gjøre rede for hvordan noen av delproblemene kan løses med programmering

Forslag til læringsmål

- [ ] Elevene forstå 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

- [ ] *Vi har dessverre ikke noen variasjoner tilknyttet denne oppgaven enda.*

Eksterne ressurser

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