Python

Lærerveiledning - Diffie-Hellman nøkkelutveksling

Kurs: Python
Tema: Tekstbasert, Kryptografi
Fag: Matematikk, Programmering
Klassetrinn: 8.-10. klasse, Videregående skole

Om oppgaven

Denne oppgaven inngår i en serie om kryptografi, og viser hvordan man kan bli enig om en delt hemmelighet. Det anbefales å gå gjennom følgende oppgaver før man starter på denne:

- Hemmelige koder (../hemmelige_koder/hemmelige_koder.html)
- Primtall og effektivitet (../primtall/primtall.html)
- Tilfeldige tall (../tilfeldige_tall/tilfeldige_tall.html)

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

Oppgaven passer til:

Fag: Programmering, matematikk, IT

Anbefalte trinn: 8. trinn--VG3

Tema: Kryptografi, primtall, IT-sikkerhet

Tidsbruk: Dobbeltime

Kompetansemål

- **Programmering, 10. trinn**: analysere problemer, gjøre dem om til delproblemer og gjøre rede for hvordan noen av delproblemene kan løses med programmering

- [ ] **Matematikk, 8. trinn**: bruke potenser og kvadratrøtter i utforsking og problemløsing og argumentere for fremgangsmåter og resultat
- [ ] **Matematikk, 8. trinn**: lage og forklare regneuttrykk med tall, variabler og konstanter knyttet til praktiske situasjoner
- [ ] **IT1, VG2**: planlegge og implementere brukergrensesnitt
- [ ] **IT1, VG2**: lage og bruke egne og andres funksjoner med og uten parametre og returverdier
- [ ] **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

Forslag til læringsmål

- [ ] Elevene behersker modulo-regning
- [ ] Elevene kan forklare hvordan nøkkelutveksling fungerer, og hvorfor det fungerer som en kryptering
- [ ] Elevene kan lese, forstå og endre andres programkode
- [ ] Elevene får til å genere nøkler sammen

Forslag til vurderingskriterier

- [ ] Eleven oppnår middels måloppnåelse ved å fullføre oppgaven til og med steg 3.
- [ ] Eleven oppnår høy måloppnåelse ved å fullføre stegene 4 og 5. Kun de aller sterkeste elevene forventes å få til utfordringen på slutten av steg 5.

Forutsetninger og utstyr

- [ ] **Forutsetninger**: God kjennskap til Python, noe matematisk modenhet. Gjennomført tidligere oppgaver som beskrevet over.
- [ ] **Utstyr**: Datamaskin med Python installert

Fremgangsmåte

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

På de laveste trinnene kan temaet kan virke matematisk krevende når en ser på det første gang. Derfor kan det kanskje være nyttig å først og fremst angripe det fra et programmeringsperspektiv, for koden i seg selv er ikke særlig komplisert. I neste omgang kan man da bruke det en har programmert for å forstå matematikken bedre.

Variasjoner

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

Eksterne ressurser

- [ ] Foreløpig ingen eksterne ressurser ...