Lærerveiledning - Diffie-Hellman nøkkelutveksling

TIL OPPGAVE | LAST NED PDF

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
- Primtall og effektivitet
- Tilfeldige tall

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

Oppgaven passer til:

Fag: Programmering, matematikk

Anbefalte trinn: 8. trinn--VG3

Tema: Kryptografi, primtall, 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
- ☐ **Matematikk X**: gjøre rede for praktiske anvendelser av kongruensregning i kryptering og feilrettingskoder
- ☐ **Matematikk X**: planlegge, utføre og presentere et selvstendig utforskende arbeid i et emne tilknyttet hovedområdet

Forslag til læringsmål

- ☐ Elevene behersker modulo-regning

- [ ] 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

Eksterne ressurser