H.C. Ørsted Gymnasiet

Opgaveformulering SOP 2021-22

Klasse:	3a1
Navn:	Philip Rying
Fødselsdato	

Fag:	Niveau:	Vejleder navn:	Vejleders mailadresse:
Matematik	A	Sara Hillerup Andersen	shan@tec.dk
Digital Design & Udvikling	A	Anders Juul Refslund Petersen	ajrp@tec.dk

Hvad er elliptisk kurvekryptografi og hvor sikkert er det?

Redegør kort for hvordan public-key kryptografi fungerer i forbindelse med elliptiske kurver.

Definer en gruppeoperator på en elliptisk kurve, og bevis at den overholder kriterierne for en gruppe.

Gør rede for den matematiske teori der ligger til grund for sikkerheden i elliptisk kurvekryptografi, kom herunder ind på det diskrete logaritme problem.

Design og implementer et elliptisk kurvekryptosystem og analyser sikkerheden i dette.

Vurder og diskuter hvor sikkert elliptisk kurvekryptografi er og sammenlign med RSA-kryptering.

Udleverede bilag	
Opgaven udleveres	**04. marts 2022 kl. 12:00**
Opgaven skal afleveres	**18. marts 2022 kl. 12:00**

H.C. Ørsted Gymnasiet

Besvarelsen skal indeholde:

3.1 Titelblad
Den opgaveformulering du har fået udleveret

3.2 Forside

3.3 Indholdsfortegnelsen
Efter forsiden placeres indholdsfortegnelsen inklusiv sidetal.

3.4 Resumé
Besvarelsen skal indledes med et resume på dansk. Det bør ikke fylde mere end 15-20 linjer.

3.5 Hoveddel
Opgavens omfang er 15-20 sider a' 2400 anslag (inkl. mellemrum), dog skal større mængder af symbolsprog opgøres ud fra deres omfang på siderne uden sammentælling af anslag. Dette er **eksklusive Titelblad, forside, indholdsfortegnelse, figurer, tabeller, kildefortegnelse, bilag og lign.** I hoveddelen indgår følgende afsnit:

Indledningen/problemformulering: Hvor du kan gøre rede for, hvordan du har besluttet dig at gå frem og hvorfor.
Opgavebesvarelsen: Her besvarer du opgaveformuleringen.
Konklusion

3.6 Litteraturliste/kildefortegnelser
Opgaven skal indeholde en samlet liste over det benyttede materiale i form af en litteraturliste. Henvisninger til benyttet kildemateriale skal være i teksten, angives ens i hele opgaven eventuelt ved citat, referat eller direkte omtale. Det er vigtigt, at du citerer korrekt. Tekstens stavemåde og retskrivning skal følges.

3.7 Evt. bilag

H.C. Ørsted Gymnasiet

Fra bekendtgørelsen:

Målet med studieretningsprojektet er, at eleverne skal kunne:

- undersøge og afgrænse en problemstilling ved at kombinere viden og metoder fra forskellige fag og udarbejde en problemformulering
- søge, vurdere og anvende fagligt relevant information
- kombinere viden og metoder fra fagene til indsamling og analyse af empiri og bearbejdning af problemstillingen
- perspektivere den behandlede problemstilling
- demonstrere evne til faglig formidling såvel mundtligt som skriftligt, herunder beherske forskellige genrer og fremstillingsformen i en skriftlig opgavebesvarelse
- vurdere forskellige fags og metoders muligheder og begrænsninger i arbejdet med problemstillingen
- kunne anvende relevante studiemetoder samt forholde sig refleksivt til egen læreproces og eget arbejde.

Den mundtlige prøve
Ved den mundtlige prøve er eksaminationstiden 30 minutter inklusive votering. Der gives ingen forberedelsestid. Eksaminationen tager udgangspunkt i eksaminandens præsentation af opgavens problemstillinger og konklusioner. Eksaminationen former sig herefter som en faglig samtale mellem eksaminand, eksaminator og evt. censor. Elevens fremlæggelse har en varighed på op til 10 minutter af eksaminationstiden. Ved den mundtlige prøve lægges der vægt på:

- den mundtlige præsentation af projektet og dets vigtigste konklusioner
- faglig dybde og selvstændighed i den faglige dialog om projektet
- forståelse af de indgående fags og faglige metoders muligheder og begrænsninger i forhold til arbejdet med den valgte problemstilling, og overvejelser om kvaliteten af den opnåede viden
- refleksion over de anvendte studiemetoder i forhold til gennemførelse af det konkrete projektforløb.

Der gives én karakter på baggrund af en helhedsvurdering af både den skriftlige opgavebesvarelse og den mundtlige eksamination.