

Lektionsplanering

Årskurs: Gymnasiet

Kurs: Matematik 3b

Tema: Talteori och kryptografi

Koppling till styrdokument

Centralt innehåll

Denna lektion syftar till att introducera begreppet talteori, med fokus på primtal och deras betydelse inom kryptografi. Eleverna kommer att lära sig om egenskaper hos primtal, hur de används inom säkerhetsprotokoll och grundläggande kryptografiska metoder, inklusive RSA-algoritmen.

Kunskapskrav

Eleven ska kunna redogöra för och tillämpa grundläggande begrepp inom talteori, inklusive primtal och deras egenskaper. Dessutom ska eleven kunna förklara hur dessa koncept används inom kryptografi.

Lärrarledda instruktioner

Introduktion till talteori (10 min)

- Definiera talteori och dess centrala frågor, som primtal och delbarhet.
- Diskutera primtalens definition och egenskaper (exempelvis endast delat med 1 och sig själv).
- Gå igenom några exempel på primtal och sammansatta tal.
- Klargöra vikten av primtal inom matematik och tillämpningar i kryptografi.

Egenskaper hos primtal (15 min)

- Diskutera primtalens fördelning och hur man kan identifiera primtal (exempelvis Sieve of Eratosthenes).
- Introducera Merlins och Fermats primtalstest.
- Låt eleverna arbeta tillsammans för att hitta primtal inom ett visst

intervall och diskutera metoderna de använde.

- Presentation av gruppernas resultat och strategier.

Kryptografi och dess grundprinciper (15 min)

- Introducera vad kryptografi är och dess historiska kontext.
- Diskutera hur primtal används i kryptografiska algoritmer, inklusive RSA.
- Förklara hur RSA-algoritmen fungerar, inklusive nyckelgenerering, kryptering och dekryptering.
- Ge exempel på hur kryptografi används i vardagen (exempelvis banktransaktioner, e-postsäkerhet).
- Låt eleverna diskutera sin förståelse av kryptografi och hur primtal bidrar till datasäkerhet.

Tillämpningar av talteori och kryptografi (10 min)

- Diskutera riktiga tillämpningar av talteori och kryptografi i samhället.
- Analysera hur dessa begrepp är viktiga för moderna kommunikationssystem och datasäkerhet.
- Låt eleverna arbeta i grupper för att lösa problem relaterade till kryptografi och presentation av sina fynd.

Diskussionsfrågor

- A. Hur kan talteori och primtal påverka cybersäkerheten? Ge exempel.
- B. Vilka begränsningar och utmaningar ser ni med att använda primtal i kryptografi? Diskutera.
- C. Hur kan kunskaperna om talteori tillämpas i andra områden av matematik eller datavetenskap?

Aktivitet

Eleverna delas in i grupper och får i uppdrag att utföra en djupgående analys av en specifik kryptografisk metod (exempelvis RSA). De ska formulera och beskriva hur metoden fungerar, vilket primtal och algoritm som används, och ge exempel på tillämpningar. Varje grupp presenterar sina fynd för klassen och diskuterar sina insikter om de matematiska koncepten.

Exit-ticket

- Vad är ett primtal och varför är det viktigt inom talteori?
- Svar: Ett primtal är ett tal som endast är delbart med 1 och sig självt; det är centralt i talteori och kryptografi.

