



KURSPLAN

Talteori och kryptografi G1N

4,5 högskolepoäng

Kurskod: MA191G

Revisionsnummer: 16

Gäller från: 2023-01-01

Beslutad av: Utbildningskommittén för ingenjörsvetenskap

Beslutsdatum: 2022-06-09

1. Allmänt om kursen

Kursen ges av Högskolan i Skövde och benämns Talteori och kryptografi G1N (Number Theory and Cryptography G1N). Omfattningen är 4,5 högskolepoäng (hp). Kursen är på grundnivå och har fördjupningsnivå G1N.

Kursen ingår i ämnet matematik/tillämpad matematik. Kursens utbildningsområde är naturvetenskap.

2. Behörighetskrav

Grundläggande behörighet.

Dessutom krävs: Matematik 2a eller 2b eller 2c (eller motsvarande kunskaper).

3. Innehåll

Kursen behandlar principerna bakom klassiska kryptografimetoder och kryptosystem med öppna nycklar samt matematiken bakom dessa.

4. Mål

Studenten skall efter avslutad kurs kunna:

- redogöra för begreppen delbarhet, primtal och modulär ekvivalens
- behärska moduloaritmetik samt algoritmer som divisionsalgoritmen och Euklides algoritmen
- visa kännedom om några klassiska kryptografimetoder
- redogöra för principerna bakom kryptosystem med öppna nycklar såsom RSA

5. Examination

Kursen bedöms med betygen VG (Väl godkänd), G (Godkänd) eller U (Underkänd).

Kursen har följande examinationsmoment:

- **Inlämningsuppgifter**
4,5 hp, betyg: VG/G/U

Studenter med varaktig funktionsnedsättning som har fått beslut om riktat pedagogiskt stöd kan erbjudas anpassad examination.

6. Undervisningsformer och undervisningsspråk

Undervisningen består av övningar och föreläsningar.

Undervisningen bedrivs på svenska. Viss undervisning på engelska kan förekomma.

7. Kurslitteratur och övriga läromedel

Sjögren, J. (2000) Talteori och kryptografi, Skövde: Högskolan i Skövde

Ytterligare material som tillgängliggörs via lärplattform.

8. Studentinflytande

Studentinflytande i kursen säkerställs genom kursvärdering. Studenterna informeras om resultatet av kursvärderingen och eventuella åtgärder som genomförts eller planeras, grundat på kursvärderingen.

9. Övrigt

Kursens innehåll överensstämmer helt eller delvis med följande kurs och kan därför inte ingå i examen med denna kurs:

- MA107G - Kryptografi och kodningsteori 7,5 hp

På Högskolan i Skövdes webbplats finns ytterligare information om kursen samt nationella och lokala styrdokument för högskoleutbildning.