Blekinge Tekniska Högskola
Institutionen för matematik och naturvetenskap

KURSPLAN

Kryptering 3

Cryptography 3

7,5 högskolepoäng (7,5 ECTS credit points)

Kurskod: MA2513
Nivå: Avancerad nivå
Fördjupning: A1N
Utbildningsområde: Naturvetenskap
Ämnesgrupp: Matematik

Huvudområde: Matematik
Version: 8
Gäller från: 2015-03-03
Fastställd: 2015-03-03

1. Kursens benämning och omfattning
Kursen benämns Kryptering 3 / Cryptography 3 och omfattar 7,5 högskolepoäng. En högskolepoäng motsvarar en poäng i European Credit Transfer System (ECTS).

2. Beslut om fastställande av kursplan
Denna kurs är inrättad av prefekten vid instituionen för matematik och naturvetenskap på delegation av dekanen vid fakulteten för teknikvetenskaper 2015-03-03. Kursplanen har reviderats av prefekten vid institutionen för matematik och naturvetenskap och gäller från 2015-03-03.
Kursen ersätter MA2510
BTH-4.1.1-0157-2015

3. Syfte
Kursens syfte är att ge fördjupad kunskap i kryptologi, det vill säga den matematiska grunden för kryptering och kryptoanalys.

4. Innehåll
• Informationsteori, perfekt sekretess och entropi.
• Algebra: polynomringar, gitter och Gröbnerbaser.
• Kort introduktion till kodningsteori, speciellt linjära koder.
• Kryptosystem: NTRU, GGH, Imai-Matsumoto och McEliece.
• Linjär kryptoanalys.
• Algoritmer: LLL, Buchberger och talkroppssållet.
• Matematisk programvara.

5. Mål
Kunskap och förståelse
Efter genomförd kurs ska studenten:
•kunna förklara principerna bakom olika moderna krypteringsmetoder och protokoll.
• kunna sammanfatta hur matematiken används inom kryptologin.
Färdigheter och förmåga
Efter genomförd kurs ska studenten:
•kunna beräkna och lösa problem av abstrakt algebraisk karaktär med hjälp av matematisk mjukvara.
• kunna implementera metoder och protokoll inom kryptologin.
• kunna skapa egna exempel vid implementation av kryptosystem, protokoll och matematiska algoritmer.
Värderingsförmåga och förhållningssätt
Efter genomförd kurs ska studenten:
•kunna jämföra olika kryptosystem med avseende på kända säkerhetsrisker och begränsningar vid implementation.

6. Lärande och undervisning
Undervisningen sker i form av föreläsningar. Teorin studeras i detalj genom laborationsövningar anpassade för matematisk mjukvara. Vidare ges handledning av en projektuppgift. Projektarbetet sker individuellt eller i grupp, och med en valfri inriktning inom kursen.
Svenska

7. Bedömning och examination
Examinationsmoment för kursen

Kod	Benämning	Omfattning	Betyg
1510	Laboration 1	2 hp	G-U
1520	Laboration 2	2 hp	G-U
1530	Projekt	3.5 hp	G-U

Kursen bedöms med betygen G Godkänd, UX Underkänd, något mer arbete krävs, U Underkänd. Vid betyget UX ges i samråd med kursansvarig/examinator möjlighet att inom 6 veckor komplettera betyget till G för det aktuella kursmomentet. Slutbetyg ges när samtliga moment är godkända.

8. Kursvärdering
Kursansvarig ansvarar för att studenternas synpunkter på kursen systematiskt och regelbundet

inhämtas och att resultaten av utvärderingar i olika former påverkar kursens utformning och utveckling.

9. Förkunskapskrav
Avklarade kurser: Kryptering 2, Linjär algebra, Analys 1 och Analys 2 samt Algoritmer och datastrukturer.

10. Utbildningsområde och huvudområde
Kursen tillhör utbildningsområdet Naturvetenskap och ingår i huvudområdet Matematik.

11. Begränsningar i examen
Kursen kan inte ingå i examen med annan kurs, vars innehåll helt eller delvis överensstämmer med innehållet i denna kurs.

12. Kurslitteratur och övriga lärresurser
Kurslitteratur:
Material som utdelas av institutionen.
Referenslitteratur:
Hoffstein, Jeffrey, Jill Pipher and Joseph. H. Silverman. (2014). An Introduction to Mathematical Cryptography, andra upplagan, New York: Springer-Verlag. ISBN: 9781493917105.
■