Fakulteten för hälsa, natur- och teknikvetenskap
Matematik

Kursplan

Algebraiska strukturer, koder och krypton

Kurskod:	MAGC15
Kursens benämning:	Algebraiska strukturer, koder och krypton *Algebraic structures, codes and cryptosystems*
Högskolepoäng:	7.5
Utbildningsnivå:	Grundnivå
Successiv fördjupning:	Grundnivå, har minst 60 hp kurs/er på grundnivå som förkunskapskrav (G2F)

Huvudområde:
MAA (Matematik/tillämpad matematik)

Beslut om fastställande
Kursplanen är fastställd av Fakulteten för hälsa, natur- och teknikvetenskap 2017-08-28 och gäller från vårterminen 2018 vid Karlstads universitet.

Behörighetskrav
Varit registrerad på kurser i matematik 60 hp, varav minst 45 hp godkända, inkl MAGA04 Linjär algebra, 7,5 hp. Motsvarandebedömning kan göras.

Lärandemål
Kursens mål är att de studerande efter avslutad kurs skall kunna:

- definiera och tillämpa de grundläggande begrepp och metoder som förekommer i teorierna för grupper, ringar och kroppar
- analysera ändliga gruppers egenskaper, bestämma delgrupper och kvotgrupper
- bestämma alla isomorfiklasser av ändliga grupper av låg ordning
- kryptera och dekryptera ett meddelande med RSA-kryptografi
- bestämma längd, dimension och kodavstånd för linjära, cykliska respektive BCH-koder
- formulera och tillämpa kursens satser
- bevisa ett givet urval av kursens satser
- visa förståelse genom att kombinera användningen av begrepp, satser och erfarenheter från exempel, se analogier och göra generaliseringar
- muntligt och skriftligt redogöra för självständigt lösta matematiska problem.

Innehåll
Teori för grupper: delgrupper, sidoklasser och Lagranges sats, kvotgrupper, isomorfier och homomorfier, struktursatsen för abelska grupper, klassifikation av isomorfiklasser av grupper av låg ordning, Sylows sats
Teori för ringar: karakteristik, integritetsområden, polynomringar, ideal och kvotringar, ringhomomorfier, isomorfisatserna, primideal och maximalideal, euklidiska områden, Gaussiska heltal

Teori för kroppar: kroppsutvidgningar, ändliga kroppar och talkroppar
Kryptografi: Symmetriska krypton (hemliga nycklar) och asymmetriska krypton (öppna nycklar), Revest-Shamir-Adelman (RSA)-krypto.
Kodning för felkontroll: Cykliska koder och BCH-koder, perfekta koder, kodning och avkodning.

Ett till omfattningen mindre projekt skall genomföras individuellt.

Kurslitteratur och övriga läromedel
Se separat dokument.

Examination
Examinationen sker i form av skriftlig tentamen samt muntlig och skriftlig presentation av projektet.

Antalet provtillfällen för att bli godkänd är begränsat till 3 per läsår.

Betyg
Kursen bedöms enligt betygsskalan U (Underkänd), G (Godkänd) eller VG (Väl godkänd).

Kvalitetsuppföljning
Under och efter kursen sker en uppföljning av måluppfyllelse och förutsättningar för lärande i kursen. Dess främsta syfte är att bidra till förbättringar. Studenternas erfarenheter och synpunkter är ett av underlagen för granskningen, och inhämtas i enlighet med gällande regelverk. Studenterna informeras om resultaten och eventuella beslut om åtgärder.

Kursbevis
Kursbevis utfärdas på begäran.

Övrigt
Regler för utbildning på grundnivå och avancerad nivå vid Karlstads universitet reglerar studenters och anställdas skyldigheter och rättigheter.