Blekinge Tekniska Högskola
Institutionen för matematik och naturvetenskap

Revision: 3,1
Dnr: BTH-4.1.14-0634-2020

KURSPLAN

Kryptering 2

Cryptography 2

6 högskolepoäng (6 credits)

Kurskod: MA1491
Huvudområde: Matematik
Utbildningsområde: Naturvetenskap
Utbildningsnivå: Grundnivå
Fördjupning: G1F - Grundnivå, har mindre än 60 hp kurs/er på grundnivå som förkunskapskrav

Ämnesgrupp: Matematik
Undervisningsspråk: Svenska men undervisning på engelska kan förekomma.
Gäller från: 2020-10-01
Fastställd: 2020-09-22

---

1. Beslut

Denna kurs är inrättad av dekan 2018-09-04. Kursplanen är fastställd av prefekten vid institutionen för matematik och naturvetenskap 2020-09-22 och gäller från 2020-10-01.

2. Förkunskapskrav

För tillträde till kursen krävs genomgången kurs Kryptering 1, 6 hp.

3. Syfte och innehåll

3.1 Syfte

Kursens syfte är att ge en fördjupad förståelse för de matematiska principerna bakom modern kryptering, säkerhetsprotokoll och forceringsmetoder.

3.2 Innehåll

- Algebraiska strukturer: grupper och kroppar
- Talteori: kvadratiska rester och Legendresymbolen
- Moderna kryptosystem: Advanced Encryption Standard (AES), Merkle-Hellmans ränselchiffer, Rabins krypto och Polly Cracker
- Elliptiska kurvor över ändliga kroppar: introduktion, som primitiv i en version av ElGamals kryptosystem och vid nyckelutväxling
- Heltalsfaktorisering: Pollards rho-metod, kvadratiska sållet och Lenstras metod baserad på elliptiska kurvor
- Introduktion till kryptografiska hackfunktioner: begrepp, Merkle-Damgårds konstruktion och kollisionsattacker
- Protokoll: noll koll-bevis och tröskelsystem
- Matematisk programvara och programmering

4. Lärandemål

Följande lärandemål examineras i kursen:

4.1 Kunskap och förståelse

Efter genomförd kurs ska studenten:
- kunna beskriva matematiken bakom kryptosystem och kryptologiska protokoll.

4.2 Färdighet och förmåga

Efter genomförd kurs ska studenten:
- kunna implementera moderna krypteringsmetoder och protokoll.
- kunna visa hur man utför beräkningar i algebraiska strukturer såsom grupper och kroppar.
- kunna använda moderna kryptoanalytiska metoder.

4.3 Värderingsförmåga och förhållningssätt

Efter genomförd kurs ska studenten:
- kunna väga olika kryptosystem mot varandra med avseende på deras säkerhet.

5. Läraktiviteter

Undervisningen ges i form av föreläsningar och övningar. Den obligatoriska projektuppgiften löses individuellt eller i grupp.

6. Bedömning och examination

Examinationsmoment för kursen

Kod	Benämning	Omfattning	Betyg
2005	Salstentamen	2 hp	GU
2015	Laboration	1 hp	GU
2025	Projektuppgift	3 hp	AF

Kursen bedöms med betygen A Utmärkt, B Mycket bra, C Bra, D Tillfredsställande, E Tillräckligt, FX Underkänd, något mer arbete krävs, F Underkänd.

I kurstillfällets kurs-PM framgår i vilka examinationsmoment som kursens lärandemål examineras samt gällande bedömningsgrunder.

Examinator kan, efter samråd med högskolans FUNKA-samordnare, fatta beslut om anpassad examinationsform för att en student med varaktig funktionsvariation ska ges en likvärdig examination jämfört med en student utan funktionsvariation.

7. Kursvärdering

Kursvärdering ska göras i enlighet med BTH:s beslut om frågeställning i kursvärderingar och beslut om process för hantering och uppföljning av kursvärderingar.

8. Begränsningar i examen

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

9. Kurslitteratur och övriga lärresurser

Material som utdelas av institutionen.

Referenslitteratur

Stanoyevitch, Alexander (2010). Introduction to Cryptography with Mathematical Foundations and Computer Implementations, Chapman & Hall/CRC. ISBN: 9781439817636.
Hoffstein, Jeffrey, Jill Pipher and Joseph. H. Silverman. (2014). An Introduction to Mathematical Cryptography, andra upplagan, New York: Springer-Verlag. ISBN: 9781493917105.

10. Övrigt

Denna kurs ersätter kursen MA1453