KURSPLAN

Kryptering I

Cryptography I

6 högskolepoäng (6 credits)

Kurskod: MA1490
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: 2019-08-01
Fastställd: 2019-03-01

1. Beslut

Denna kurs är inrättad av dekan 2018-08-24. Kursplanen är fastställd av prefekten vid institutionen för matematik och naturvetenskap 2019-03-01 och gäller från 2019-08-01.

2. Förkunskapskrav

För tillträde till kursen krävs genomgången kurs i Diskret matematik, 6 hp och genomgången kurs i Matematisk statistik, 6 hp.

3. Syfte och innehåll

3.1 Syfte

Kursens syfte är att ge studenten de grundläggande matematiska principerna för olika krypterings- och forceringsmetoder. Kursdeltagaren ska erhålla förståelse för hur man implementerar olika kryptosystem samt kända styrkor och svagheter hos dessa.

3.2 Innehåll

- Terminologi och problemställningar inom kryptologi.
- Elementär talteori: fördjupning i kongruensteori, modulär potensberäkning, Eulers fi-funktion, primitiva rötter och diskreta logaritmer.
- Modulär matrisaritmetik, determinant och matrisinvers.
- Primtalstester: Fermats metod och Miller-Rabins metod.
- Heltalsfaktorisering: Fermatfaktorisering och Pollards (p - 1)-metod.
- Olika typer av kryptosystem: symmetriska, asymmetriska, flödeskrypton och blockkrypton.
- Klassiska kryptosystem: substitution, affin, Vigenère, Hill, Enigma och engångschiffer.
- Moderna kryptosystem: Data Encryption Standard (DES), RSA och ElGamal.
- Kryptoanalys av klassiska kryptosystem samt differentiell kryptoanalys.
- Protokoll: nyckelutväxling och digitala signaturer.
- Matematisk programvara och matematisk programmering.

4. Lärandemål

Följande lärandemål examineras i kursen:

4.1 Kunskap och förståelse

Efter genomförd kurs ska studenten:

- kunna redogöra för övergripande terminologi och problemställningar inom kryptologin.
- kunna redogöra för grundläggande begrepp i elementär talteori
- kunna redogöra för grunderna för olika krypteringsmetoder och protokoll
- kunna redogöra för svagheter och styrkor hos olika krypteringsmetoder.

4.2 Färdighet och förmåga

Efter genomförd kurs ska studenten:

- kunna lösa linjära kongruenser och tillämpa kinesiska restsatsen
- kunna formulera och lösa problem inom modulär matrisaritmetik
- kunna beräkna funktionsvärden för Eulers fi-funktion

• kunna beräkna diskreta logaritmer
• kunna bevisa resultat av enklare karaktär i elementär talteori
• kunna använda algoritmer för primtalstest och heltalsfaktorisering
• kunna implementera klassiska och moderna kryptosystem samt protokoll
• kunna genomföra en forceringsattack på ett klassiskt kryptosystem.
• kunna söka och inhämta information inom kursens kunskapsområde samt sammanställa en kortare rapport enligt anvisade rapportform med korrekt referenshantering.

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. Laboration och inlämningsuppgift kan lösas individuellt eller i grupp.

6. Bedömning och examination

Examinationsmoment för kursen

Kod	Benämning	Omfattning	Betyg
1910	Salstentamen	3 hp	AF
1920	Laboration	1 hp	GU
1930	Inlämningsuppgift	2 hp	GU

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.

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.

Stanoyevitch, Alexander (2010). Introduction to Cryptography with Mathematical Foundations and Computer Implementations, Chapman & Hall/CRC. ISBN: 9781439817636.

Referenslitteratur

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 MA1474