Kursplan för:

Matematik GR (B), Kryptografi, 7,5 hp

Mathematics BA (B), Cryptography, 7.5 Credits

Allmänna data om kursen

Kurskod	MA080G
Ämne/huvudområde	Matematik
Nivå	Grundnivå
Progression	(B)
Inriktning (namn)	Kryptografi
Högskolepoäng	7.5
Fördjupning vs. Examen	G1F , Kursen ligger på grundnivå och fordrar mindre än 60 hp kurs(er) på grundnivå som förkunskapskrav.
Utbildningsområde	Naturvetenskap 100%
Ansvarig institution	Matematik och ämnesdidaktik
Inrättad	2007-08-15
Fastställd	2010-01-18
Senast reviderad	2020-11-30
Giltig fr.o.m	2021-01-01

Syfte

Studenterna ges en introduktion till kryptografi och kryptografiska metoder. Traditionella chiffreringsmetoder som t ex substitutionschiffer studeras, och några krypteringsmetoder med öppen nyckel behandlas.

Lärandemål

Efter avslutad kurs ska studenten
- visa förtrogenhet med kryptologisk terminologi för såväl klassiska symmetriska chiffersystem som kryptosystem med öppen nyckel, inkl. digitala signaturer
- ha någon insikt i hur monoalfabetiska och polyalfabetiska substitutionschiffer kan forceras med statistiska metoder
- kunna visa några djupare insikter om heltalen modulo n där n är ett primtal eller en produkt av två primtal, och i synnerhet visa någon förtrogenhet med Eulers fi-funktion, Carmichaels lambda-funktion, Eulers generalisering av Fermat lilla sats, kinesiska restsatsen, potensfunktioner modulo n och diskreta logaritmer
- ha någon insikt i vissa kryptografiska algoritmer och deras komplexitet; i synnerhet faktoriseringsalgoritmer, primtalstester, snabba algoritmer för exponentiering, samt några krypterings- och dekrypteringsalgoritmer från såväl klassisk kryptografi som kryptografi med öppen nyckel
- visa någon insikt i de respektive styrkorna och svagheterna för några kryptosystem med öppen nyckel.

Innehåll

- Kryptografins historia och grundläggande begrepp, såsom klartext, chiffertext, nycklar, substitutions- och andra klassiska chiffer.
- Chifferforcering med statistiska metoder.
- Introduktion till kryptografi med öppen nyckel, inkluderande digitala signaturer.
- Fortsatt modulär aritmetik.
- RSA, Elgamal, Diffie-Hellman nyckelutväxling och en grundläggande introduktion till kryptografi med elliptiska kurvor.

Behörighet

Matematik GR (A), Linjär algebra I, 6 hp, samt Diskret matematik A, 6 hp
eller
Matematik GR(A), Matematisk statistik och linjär algebra, 7,5 hp, samt Diskret matematik, 7,5 hp.

Urvalsregler

Urval sker i enlighet med Högskoleförordningen och den lokala antagningsordningen.

Undervisning

Självstudier och lärarledda sammankomster, eventuellt kombinerade med andra undervisningsformer.

Examination

S101: Gruppseminarier - , 1.5 hp

Betygsskala: U, G

T102: Skriftlig tentamen - , 6.0 hp

Betygsskala: 7-gradig betygskala. A-F o Fx.

Frivilliga aktiviteter i form av inlämningsuppgifter och kamratgranskning ingår. Dessa schemalagda aktiviteter kan generera bonuspoäng som läggs till poängen på tentamen (T102). Bonuspoängen gäller max ett år från kursstart på det kurstillfälle där de frivilliga aktiviteterna är schemalagda. Hur bonussystemet fungerar beskrivs utförligare i kursmiljön.

De examinerande momenten beskrivs tydligare i kursmiljön.

Slutbetyget baseras på en sammanvägd bedömning av hur väl de olika momenten klarats av.

Om en student har ett beslut från samordnaren vid Mittuniversitetet om pedagogiskt stöd vid funktionsnedsättning, har examinator rätt att ge anpassad examination för studenten.

Betygskriterier för ämnet finns på www.miun.se/betygskriterier.

Begränsning av examination

Studenter registrerade på denna version av kursplan har rätt att erbjudas 3 examinationstillfällen inom loppet av 1 år enligt angivna examinationsformer. Därefter gäller examinationsform enligt senast gällande version av kursplan.

Betygsskala

På kursen ges något av betygen A, B, C, D, E, Fx och F. A - E är Godkänt, Fx och F är underkänt.

Litteratur

Obligatorisk litteratur

Författare/red: Rubinstein-Salzedo, S
Titel: Cryptography
Upplaga: Senaste upplagan
Förlag: Springer
Kommentar: ISBN 978-3-319-94817-1

Referenslitteratur

Författare/red: Cameron P.J
Titel: Notes on Cryptography
Upplaga: Senaste upplagan
Webbadress: http://www.maths.qmul.ac.uk/%7Epjc/notes/crypt.pdf

Författare/red: Paar C, Pelzl J
Titel: Understanding Cryptography
Upplaga: Senaste upplagan
Förlag: Springer
Kommentar: ISBN 978-3-642-04100-6

Författare/red: Simon Singh
Titel: The Code Book: The Secret History of Codes and Code-breaking
Förlag: Fourth Estate Ltd