***Mal for Det matematisk-naturvitskaplege fakultet***

**Mal for emnebeskrivingar ved Universitetet i Bergen - Course Plan**

Eit studieprogram inneheld fleire emne. Ei emnebeskriving er ein detaljert plan for eitt av emna i eit studieprogram.

Krav til studiar går fram av *Forskrift for tilsyn med utdanningskvalitet i høyere utdanning**(studietilsynsforskriften),* NOKUT 2013, <http://link.uib.no/?21Vcl> . UiBs *Forskrift om opptak, studier, vurdering og grader ved Universitetet i Bergen* (Studieforskrifta) gir i kapittel 3 reglar for studiestruktur og studieplan: <http://link.uib.no/?YoXx>

UiB si *Handbok for kvalitetssikring av universitetsstudia* gir meir rettleiing om ansvar, prosedyrar og krav til oppretting av studieprogram og emne (pkt. 16.1 og 16.4). Sjå <http://www.uib.no/studiekvalitet> .

Studietilsynsforskrifta (NOKUT) seier i § 7-4 at «Delene studiet består av skal utgjøre en samlet helhet i samsvar med læringsutbyttet for studiet», og at de «skal tilfredsstille standarder og kriterier for akkreditering av studier i § 7-1 til § 7-3.»

I tillegg til kategoriane i tabellen nedanfor, skal emnebeskrivinga innehalde følgjande informasjon: dato for godkjenning, dato for eventuelle justeringar, namn på instans som har godkjent beskrivinga, dato for førre evaluering og neste planlagde evaluering av emnet. Denne informasjonen skal stå på forsida til planen. Forsidemal finn ein sist i dette dokumentet.

Eventuelt forslag til tekst står i kursiv i kolonnen «Tekst». Rettleiing og nokre døme finn ein i kolonnen til høgre. Den må fjernast før emnebeskrivinga vert send til programstyre, institutt og fakultet.

|  |  |
| --- | --- |
| **Kategori** |  |
| **Emnekode**  **Course Code** | INF240 |
| **Namn på emnet, nynorsk** | Grunnleggjande koder |
| **Namn på emnet, bokmål** | Grunnleggende koder |
| **Course Title, English** | Basic Codes |
| **Studiepoeng, omfang**  **ECTS Credits** | 10  10 |
| **Studienivå (studiesyklus)**  **Level of Study** | Master  Master |
| **Fulltid/deltid**  **Full-time/Part-time** | Fulltid  Full time |
| **Undervisningsspråk**  **Language of Instruction** | Norsk. Emnet undervisast på engelsk dersom engelskspråklege studentar meldar seg til emnet.  Norwegian. The course is taught in English if students speaking only English sign up for the course. |
| **Undervisningssemester**  **Semester of Instruction** | Haust  Autumn |
| **Undervisningsstad**  **Place of Instruction** | Institutt for informatikk, UiB  Department of Informatics, UoB |
| **Mål og innhald**  **Objectives and Content** | Mål:  INF240 gjev studentane ein introduksjon til kryptologi og kodeteori. Vanlege metodar for å bruke kryptografi til å sikre data mot uautorisert innsyn og manipulasjon vert gjevne. Studentane skal lære enkle metodar i kodeteori for sikring av feil i data som kan oppstå ved transmisjon og lagring.  Studentane skal etter kurset kunne forstå korleis ein brukar grunnleggjande metodar innan kryptologi og kodeteori.  Innhald:  Emnet tek opp ulike metodar for å konstruera kryptoalgoritmar og kryptografiske protokollar. Metodar for symmetrisk og asymmetrisk kryptografi inkludert RSA, AES, digitale signaturar, hashfunksjonar, autentisering av meldingar vert diskutert. Vidare gjev emnet ein elementær introduksjon til feilkorrigerande kodar. Noe bakgrunnsinformasjon om talteori og endelege kroppar vert presentert.  Objectives:  INF204 gives the students an introduction to cryptology and coding theory. Common methods to apply cryptography to secure data against unauthorized access and manipulation are explained. The students will learn simple methods in coding theory for correction of errors that may happen to data during transmission or storage.  After the course the students should be able to understand how to apply basic methods in cryptology and coding theory.  Content:  The course discusses different methods to construct crypto algorithms and crypto protocols. Methods for symmetric and asymmetric cryptography including RSA, AES, digital signatures, hash-functions, authentication of messages are explained. An introduction to error-correcting codes is given. Some background information on number theory and finite fields is provided. |
| **Læringsutbyte**  **Learning Outcomes** | *Studenten skal ved avslutta emne ha følgjande læringsutbyte definert i kunnskapar, ferdigheiter og generell kompetanse:*  Kunnskapar  Studenten kan   * forklare korleis dei mest vanlege kryptoalgoritmar fungerar * fortelje korleis kryptoprotokollar kan brukas til å sikre data mot uautorisert bruk * fortelje korleis teknikkar i kodeteori kan brukas til å retta feil i data   Ferdigheiter  Studenten skal kunne   * vurdere kva for metodar innan krypto som er mest effektive for å sikra data * forklare korleis enkle feilkorreksjons metodar kan brukas for å beskytte data mot feil   Generell kompetanse  Studenten kan diskutere kva for metodar i kryptografi og kodeteori som vil vere effektive å for å beskytte data.  On completion of the course the student should have the following learning outcomes defined in terms of knowledge, skills and general competence:  Knowledge  The student knows   * how the most common crypto algorithms work * how crypto protocols are used to protect data * how techniques in coding theory are applied to correct data against errors   Skills  The student is able to   * assess which crypto techniques that are most effective to secure data * explain how simple error correcting codes can be applied to protect data against errors   General competence  The student can discuss which methods in cryptography and coding theory that will be most effective to protect data |
| **Krav til forkunnskapar**  **Required Previous Knowledge** | Basic knowledge in discrete mathematics  None |
| **Tilrådde forkunnskapar**  **Recommended previous Knowledge** | INF142, MNF130  INF142, MNF130 |
| **Studiepoengsreduksjon**  **Credit Reduction due to Course Overlap** |  |
| **Krav til Studierett**  **Access to the Course** | For oppstart på emnet er det krav om ein studierett knytt til Det matematisk-naturvitskaplege fakultet <http://www.uib.no/matnat/52646/opptak-ved-mn-fakultetet>  Access to the course requires admission to a programme of study at The Faculty of Mathematics and Natural Sciences. |
| **Undervisningsformer og**  **omfang av organisert undervisning**  **Teaching Methods and Extent of Organized Teaching** | Undervisninga gis i form av førelesningar og gruppeøvingar  Førelesningar: 4 timar pr. veke i 11 veker  Gruppeøvingar: 2 timar pr. veke i 10 på veker  The teaching comprises of lectures and group exercises  Lectures: 4 hours pr. week for 11 weeks  Group exercises: 2 hours pr. week for 10 weeks |
|
| **Obligatorisk undervisningsaktivitet**  **Compulsory Assignments and Attendance** | Innlevering av obligatorisk oppgåve. Godkjend obligatorisk oppgåve er gyldig i eitt påfølgande semester etter godkjenninga.  Submission of compulsory exercise. Accepted compulory exercise is valid for one semester after acceptance. |
| **Vurderingsformer**  **Forms of Assessment** | I emnet nyttar ein følgjande vurderingsformer:   * obligatorisk oppgåve utgjer 20% av karakteren. * Skriftleg eksamen (3 timar), utgjør 80% av karakteren.   The forms of assessment are:   * compulsory exercise counts for 20% of total grade. * Written examination (3 hours) counts for 80% of total grade. |
| **Hjelpemiddel til eksamen**  **Examination Support Material** | Ingen  None |
| **Karakterskala**  **Grading Scale** | Ved sensur vert karakterskalaen A-F nytta.  The grading scale used is A to F. Grade A is the highest passing grade in the grading scale, grade F is a fail. |
| **Vurderingssemester**    **Assessment Semester** | Det er ordinær eksamen kvart semester. I semesteret utan undervisning er eksamen tidleg i semesteret.  Examination both spring semester and autumn semester. In semesters without teaching the examination will be arranged at the beginning of the semester. |
| **Litteraturliste**  **Reading List** | Litteraturlista vil vere klar innan 01.06. for haustsemesteret og 01.01. for vårsemesteret.  The reading list will be available within June 1st for the autumn semester and January 1st for the spring semester. |
| **Emneevaluering**  **Course Evaluation** | Studentane skal evaluere undervisninga i tråd med UiB og instituttet sitt kvalitetssikringssystem.  The course will be evaluated by the students in accordance with the quality assurance system at UiB and the department. |
| **Programansvarleg**  **Programme Committee** | Programstyret har ansvar for fagleg innhald og oppbygging av studiet og for kvaliteten på studieprogrammet og alle emna der.  The Programme Committee is responsible for the content, structure and quality of the study programme and courses. |
| **Emneansvarleg**  **Course Coordinator** | Emneansvarleg og administrativ kontaktperson finn du på Mitt UiB, kontakt eventuelt [studieveileder@ii.uib.no](mailto:studieveileder@ii.uib.no)  Course coordinator and administrative contact person is found on Mitt UiB. You may also contact studieveileder@ii.uib.no |
| **Administrativt ansvarleg**  **Course Administrator** | Det Matematisk-Naturvitenskapelege fakultet v/ Institutt for informatikk har det administrative ansvaret for emnet og studieprogrammet.  The Faculty of Mathematics and Natural Sciences by The Department of Informatics has the administrative responsibility for the course and the study program |
| **Kontaktinformasjon**  **Contact Information** | Studierettleiar kan kontaktast her: [studieveileder@ii.uib.no](mailto:studieveileder@ii.uib.no)  Tlf: 55 58 42 86 / 55 58 40 25  Study counselor can be contacted at: [studieveileder@ii.uib.no](mailto:studieveileder@ii.uib.no)  Phone: 55 58 42 86 / 55 58 40 25 |

Emnebeskriving for …………………………………………………………. *(Namn på emnet, nynorsk)*

………………………………………………………………. *(Navn på emnet, bokmål)*

………………………………………………………………. *(Name of the course, English)*

*Godkjenning:*

*Emnebeskrivinga er godkjend av (Fakultetet brukar nemningar for godkjenningsorgan i samsvar med eigen praksis.):*

*Programstyret: …………………………………….(dd.mm.år)*

*Institutt for …………….. : .………………………(dd.mm.år)*

*………… fakultet: …………………………………….(dd.mm.år)*

*Emnebeskrivinga vart justert: …………………………………….(dd.mm.år) av ……………………………………………………………….*

*Evaluering:*

*Emnet vart sist evaluert: …………………………………….(dd.mm.år)*

*Neste planlagde evaluering: …………………………………….(dd.mm.år)*