AALBORG UNIVERSITET

STUDIEORDNING FOR DIPLOMINGENIØRUDDANNELSEN I CYBERSIKKERHED, 2025, KØBENHAVN

DIPLOMINGENIØR
KØBENHAVN

MODULER SOM INDGÅR I STUDIEORDNINGEN

INDHOLDSFORTEGNELSE

INTRODUKTION TIL PROJEKTARBEJDE OM CYBERSIKKERHED

2025/2026

MODULETS INDHOLD, FORLØB OG PÆDAGOGIK

Den studerende skal gennem projektmodulet opnå viden om den problemorienterede læringsmetode (PBL). Dette projekt gennemføres i grupper, og de studerende sættes i stand til at løse en virklighedsnær problemstilling ved at identificere cybertrusler i det definerede use case.

LÆRINGSMÅL

VIDEN

- Overblik over projektbaseret problemløsning og forståelse for, hvordan man tilgår og strukturerer cybersikkerhedsprojekter
- Beskrive typiske faser i et problemorienteret projekt
- Forstå og forklare de teorier og metoder, der anvendes i projektet
- Forklare organiseringen af gruppearbejde og samarbejde med vejledere

FÆRDIGHEDER

- Samarbejde effektivt i en gruppesammenhæng
- Beskrive og definere et sikkeheds use case, der er relevant for professionen
- Formulere en problemstilling og beskrive problemet fra et holistisk perspektiv
- Identificere sikkerhedstrusler i det definerede use case
- Kommunikere og forsvare projektets overvejelser, arbejdsresultater og arbejdsprocesser skriftligt, visuelt og mundtligt
- Beskrive de erfaringer og indsigter, der er pnået gennem gruppens projektarbejde

KOMPETENCER

- Have opnået en forståelse for trusselsmodellering og cybersikkerheds use cases
- Reflektere over processen med at tilegne sig viden både som gruppe og individuelt

UNDERVISNINGSFORM

Jf. beskrivelsen i §18

EKSAMEN

PRØVER

Prøvens navn	Introduktion til projektarbejde om cybersikkerhed
Prøveform	Mundtlig pba. projekt
ECTS	5
Tilladte hjælpemidler	Alle skriftlige og alle elektroniske hjælpemidler
Bedømmelsesform	Bestået/ikke bestået
Censur	Intern prøve
Vurderingskriterier	Vurderingskriterierne er angivet i Universitetets eksamensordning

FAKTA OM MODULET

Engelsk titel	Introduction to Project Work about Cyber Security
Modulkode	ESNDCD1P1
Modultype	Projekt
Varighed	1 semester
Semester	Efterår
ECTS	5
Undervisningssprog	Dansk og engelsk
Undervisningssted	Campus København
Modulansvarlig	Tatiana Kozlova Madsen

ORGANISATION

Uddannelsesejer	Diplomingeniør i cybersikkerhed
Studienævn	Studienævn for Elektronik og IT
Institut	Institut for Elektroniske Systemer
Fakultet	Det Teknisk Fakultet for IT og Design

CYBERTRUSLER OG CYBERANGREB

2025/2026

MODULETS INDHOLD, FORLØB OG PÆDAGOGIK

I projektet skal de studerende tilegne sig viden inden for cybersikkerhed gennem teoretisk og praktisk arbejde. Der tages udgangspunkt i en samfunds- eller erhvervsrelevant problemstilling, der kan løses ved hjælp af teorier og metoder inden for feltet. I projektet arbejder de studerende med at designe og implementere en sikker applikation baseret på forskellige sikkerhedsprincipper.

LÆRINGSMÅL

VIDEN

- Have opnået teoretisk viden om centrale begreber inden for cybersikkerhed, trusler og modforanstaltninger
- Have erhvervet grundlæggende viden om cybersikkerhedsaspekter i applikationer og deres implementering
- Have en forståelse for, hvordan cybersikkerhedsproblemer påvirker industrier og samfund, og hvordan de kan adresseres gennem tekniske løsninger
- Have viden om teknologiske og samfundsmæssige problemstillinger, der er tilstrækkelig til at identificere relevante kontekstuelle perspektiver
- Have kendskab til arbejdsprocesserne i langsigtet problemorienteret projektarbejde
- Demonstrere viden om teori og metode, der er tilstrækkelig til at forklare det teoretiske og metodologiske grundlag for projektet

FÆRDIGHEDER

- Kunne anvende en relevant metode til struktureret projektarbejde, herunder analysere og formulere et problem samt opdele problemet i mindre dele
- Kunne implementere en valgt løsning på en passende platform
- Kunne vurdere egen anvendelse af de ovennævnte teorier og metoder
- Kunne formidle den ovenstående viden med korrekt brug af fagterminologi, både mundtligt og skriftligt, gennem en projektrapport
- Kunne analysere egen læringsproces ved brug af relevante analysestrategier
- Arbejde effektivt i et team for at levere løsninger på sociale eller forretningsrelevante problemer og planlægge langsigtet gruppearbejde eller samarbejde med en vejleder

KOMPETENCER

- Demonstrere evnen til at designe og implementere applikationer, der opfylder sikkerhedskrav
- Analysere cybersikkerhedsproblemer ved at kombinere teoretisk viden med praktiske færdigheder
- Demonstrere evnen til at samarbejde effektivt i et team for at opnå fælles mål og løse komplekse problemer
- Planlægge, strukturere, implementere og reflektere over et projekt baseret på et socialt eller professionelt relevant problem, hvor cybersikkerhed er et centralt element, både individuelt og i grupper
- Tage ansvar for egen læringsproces under et langsigtet projektforløb og generalisere samt perspektivere de opnåede erfaringer

UNDERVISNINGSFORM

Jf. beskrivelsen i §18

EKSAMEN

PRØVER

Prøvens navn	Cybertrusler og cyberangreb

Prøveform	Mundtlig pba. projekt
ECTS	10
Tilladte hjælpemidler	Alle skriftlige og alle elektroniske hjælpemidler
Bedømmelsesform	7-trins-skala
Censur	Intern prøve
Vurderingskriterier	Vurderingskriterierne er angivet i Universitetets eksamensordning

FAKTA OM MODULET

Engelsk titel	Cyber Threats and Attacks
Modulkode	ESNDCD1P2
Modultype	Projekt
Varighed	1 semester
Semester	Efterår
ECTS	10
Undervisningssprog	Dansk og engelsk
Undervisningssted	Campus København
Modulansvarlig	Tatiana Kozlova Madsen

ORGANISATION

Uddannelsesejer	Diplomingeniør i cybersikkerhed
Studienævn	Studienævn for Elektronik og IT
Institut	Institut for Elektroniske Systemer
Fakultet	Det Teknisk Fakultet for IT og Design

INTRODUKTION TIL CYBERSIKKERHED

2025/2026

MODULETS INDHOLD, FORLØB OG PÆDAGOGIK

Kursusmodulet giver et fundament i koncepter, terminologi og best practice for cybersikkerhed. De studerende udforsker cybertrusselslandskabet, angrebsmetoder, sårbarheder og sikkerhedsløsninger og udvikler færdigheder i kritisk tænkning og problemløsning for at kunne træffe informerede beslutninger i forbindelse med brancherelaterede scenarier.

LÆRINGSMÅL

VIDEN

- Have viden om centrale begreber, principper og terminologi inden for cybersikkerhed
- Genkende almindelige cybertrusler, sårbarheder og angrebsvektorer
- Forstå vigtigheden af cybersikkerhed i beskyttelsen af personlige, organisatoriske og samfundsmæssige aktiver
- Have kendskab til de vigtigste faser i et cyberangreb, herunder rekognoscering, scanning og opnåelse af adgang
- Have viden om sikkerhedsløsninger og bedste praksis til at beskytte systemer og data mod cyberangreb

FÆRDIGHEDER

- I stand til at analysere potentielle sårbarheder i systemer og genkende tegn på cyberangreb
- I stand til at simulere basale angreb eller forsvar i et kontrolleret miljø
- I stand til at anvende grundlæggende cybersikkerhedsværktøjer, såsom pakkesniffere
- I stand til at genkende almindelige cybertrusler som phishing, malware, ransomware og social engineering
- Identificere og beskrive centrale cybersikkerhedsrisici i forskellige kontekster

KOMPETENCER

- I stand til at analysere potentielle sårbarheder i systemer og genkende tegn på cyberangreb
- I stand til at simulere basale angreb eller forsvar i et kontrolleret miljø
- I stand til at anvende grundlæggende cybersikkerhedsværktøjer, såsom pakkesniffere
- I stand til at genkende almindelige cybertrusler som phishing, malware, ransomware og social engineering
- Identificere og beskrive centrale cybersikkerhedsrisici i forskellige kontekster

UNDERVISNINGSFORM

Jf. beskrivelse i §18

EKSAMEN

PRØVER

Prøvens navn	Introduktion til cybersikkerhed
Prøveform	Skriftlig eller mundtlig
ECTS	5
Tilladte hjælpemidler	Med visse hjælpemidler: Se eksamensspecifikation
Bedømmelsesform	7-trins-skala
Censur	Intern prøve
Vurderingskriterier	Vurderingskriterierne er angivet i Universitetets eksamensordning

FAKTA OM MODULET

Engelsk titel	Introduction to Cyber Security
Modulkode	ESNDCD1K1
Modultype	Kursus
Varighed	1 semester
Semester	Efterår
ECTS	5
Undervisningssprog	Dansk og engelsk
Tomplads	Ja
Undervisningssted	Campus København
Modulansvarlig	Tatiana Kozlova Madsen

ORGANISATION

Uddannelsesejer	Diplomingeniør i cybersikkerhed
Studienævn	Studienævn for Elektronik og IT
Institut	Institut for Elektroniske Systemer
Fakultet	Det Teknisk Fakultet for IT og Design

IMPERATIV PROGRAMMERING

2025/2026

MODULETS INDHOLD, FORLØB OG PÆDAGOGIK

FORMÅL
I dette kursus opnår den studerende indblik i grundlæggende begreber som algoritmer, datastrukturer og computerarkitekturer

BEGRUNDELSE
Computere er – uanset fagområde – et af de vigtigste værktøjer til problemløsning i dag. Den studerende skal derfor opnå et kendskab til datalogiske grundbegreber i så almen en form, at vedkommende bliver i stand til at løse problemer ved hjælp af imperative programmeringssprog.

LÆRINGSMÅL

VIDEN

- Udviklingsmiljø og kompilering
- Imperative principper
- Datatyper og variable
- Kontrolstrukturer
- Funktioner og procedurer
- Datastrukturer herunder arrays
- Input/output
- Sammensatte datastrukturer
- Simple algoritmer (f.eks. sortering og søgning)
- Basal test af programmer

FÆRDIGHEDER

- skrive, afvikle og teste programmer hvori de ovennævnte grundbegreber indgår i løsningen
- anvende korrekt fagterminologi

KOMPETENCER

- både selvstændigt og i samarbejde med andre implementere et imperativt program som løsning på en defineret opgave

UNDERVISNINGSFORM

Undervisningen tilrettelægges i henhold til de generelle undervisningsformer for uddannelsen, jf. § 17.

OMFANG OG FORVENTET ARBEJDSINDSATS

Det forventes at den studerende bruger 30 timer per ECTS, hvilket for denne aktivitet betyder 150 timer.

EKSAMEN

PRØVER

Prøvens navn	Imperativ programmering
Prøveform	Skriftlig eller mundtlig

ECTS	5
Tilladte hjælpemidler	Eventuelle tilladte hjælpemidler, vil fremgå af kursussiden i MOODLE
Bedømmelsesform	7-trins-skala
Censur	Intern prøve
Vurderingskriterier	Vurderingskriterierne er angivet i Universitetets eksamensordning

YDERLIGERE INFORMATIONER

Kontakt: Studienævn for datalogi via cs-sn@cs.aau.dk eller 9940 8854

FAKTA OM MODULET

Engelsk titel	Imperative Programming
Modulkode	DSNSWCB133
Modultype	Kursus
Varighed	1 semester
Semester	Efterår
ECTS	5
Undervisningssprog	Dansk
Tomplads	Ja
Undervisningssted	Campus København
Modulansvarlig	Lone Leth Thomsen

ORGANISATION

Uddannelsesejer	Bachelor (BSc) i teknisk videnskab (software)
Studienævn	Studienævn for Datalogi
Institut	Institut for Datalogi
Fakultet	Det Teknisk Fakultet for IT og Design

PROBLEMBASERET LÆRING

2025/2026

MODULETS INDHOLD, FORLØB OG PÆDAGOGIK

LÆRINGSMÅL

VIDEN

- centrale tilgange, begreber og teknikker i problembaseret læring
- forskellige problemtyper, projekttyper og deres indbyrdes relationer
- videnskabsteoretiske positioner i problembaseret projektarbejde

FÆRDIGHEDER

- definere problembaseret læring med udgangspunkt i teori og egne erfaringer
- planlægge og styre et problembaseret projektarbejde under hensynstagen til den givne problemtype, projektets længde og gruppens sammensætning
- identificere, analysere og formulere en åben og kompleks problemstilling under hensynstagen til de menneskelige og samfundsmæssige sammenhænge i hvilke problemet indgår
- udpege relevante fokusområder, begreber og metoder til åben og bæredygtig problemløsning af komplekse problemer
- diskutere metodiske konsekvenser af forskellige videnskabsteoretiske positioner
- analysere, sammenstille og vurdere processerne i arbejdet med forskellige problemtyper
- analysere og vurdere gruppeprocesserne i det problemorienterede projektarbejde, herunder gruppens planlægning, monitorering og udvikling af gruppearbejdet

KOMPETENCER

- udvikle en studiepraksis, der er tilpasset et problembaseret, projektorganiseret og digitaliseret læringsmiljø
- udpege, afprøve og evaluere relevante teknikker og tilgange til at forbedre et problembaseret projektarbejde
- overføre erfaringer fra problembaserede projekter til handlingsanvisninger for lignende projekter
- vurdere egen progression i PBL på et erfaringsbaseret og læringsteoretisk grundlag

UNDERVISNINGSFORM

Se § 17: Uddannelsens indhold og tilrettelæggelse

EKSAMEN

PRØVER

Prøvens navn	Problembaseret læring
Prøveform	Skriftlig eller mundtlig
ECTS	5
Tilladte hjælpemidler	Der henvises til den pågældende semesterbeskrivelse/modulbeskrivelse
Bedømmelsesform	Bestået/ikke bestået
Censur	Intern prøve
Vurderingskriterier	Vurderingskriterierne er angivet i Universitetets eksamensordning

FAKTA OM MODULET

Engelsk titel	Problem Based Learning
Modulkode	TECHENGPBL20
Modultype	Kursus
Varighed	1 semester
Semester	Efterår
ECTS	5
Undervisningssprog	Dansk
Tomplads	Ja
Undervisningssted	Campus Aalborg, Campus København, Campus Esbjerg
Modulansvarlig	Jette Egelund Holgaard

ORGANISATION

Uddannelsesejer	Bachelor (BSc) i teknisk videnskab (by-, energi- og miljøplanlægning)
Studienævn	Studienævn for Planlægning og Landinspektøruddannelsen
Institut	Institut for Bæredygtighed og Planlægning
Fakultet	Det Teknisk Fakultet for IT og Design

NETVÆRKSSIKKERHED

2025/2026

MODULETS INDHOLD, FORLØB OG PÆDAGOGIK

De studerende designer og implementerer en cybersikkerhedsløsning til at sikre datatransmission over et netværk og simulerer et scenarie i den virkelige verden, hvor sikkerheden er kritisk. Projektet involverer client-server kommunikation og overvejelser om sikker dataudveksling mellem klienter og servere

LÆRINGSMÅL

VIDEN

- Har en forståelse for nøgleprincipperne for sikker dataoverførsel, herunder kryptering, autentifikation og netværkssikkerhedsprotokoller
- Har en forståelse for klient-server-kommunikation og teknikker til sikker dataudveksling
- Har viden om kryptografiske teknikker såsom krypteringsalgoritmer og hash-metoder
- Forstår udfordringerne og løsningerne ved at sikre dataudveksling i kritiske, virkelige scenarier
- Har viden om almindelige trusler og sikkerhedsmekanismer til at afbøde dem

FÆRDIGHEDER

- I stand til at designe og implementere cybersikkerhedsløsninger til sikring af dataoverførsel over et netværk
- I stand til at implementere krypteringsmetoder for at sikre dataudveksling og garantere fortrolighed og integritet
- I stand til at anvende grundlæggende værktøjer til netværkstrafikovervågning for at identificere potentielle sårbarheder
- I stand til at dokumentere og præsentere tekniske løsninger effektivt for forskellige målgrupper

KOMPETENCER

- Anvende principper for netværkssikkerhed til at designe løsninger til kritiske, virkelige scenarier
- Integrere sikkerhedsovervejelser for klient-server i praktiske implementeringer
- Reflektere over effektiviteten og begrænsningerne ved cybersikkerhedsløsninger i en given kontekst
- Have opnået evnen til at evaluere potentielle sårbarheder og implementere passende modforanstaltninger for at sikre systemet

UNDERVISNINGSFORM

Jf. beskrivelsen i §18

EKSAMEN

PRØVER

Prøvens navn	Netværkssikkerhed
Prøveform	Mundtlig pba. projekt
ECTS	15
Tilladte hjælpemidler	Alle skriftlige og alle elektroniske hjælpemidler
Bedømmelsesform	7-trins-skala
Censur	Ekstern prøve
Vurderingskriterier	Vurderingskriterierne er angivet i Universitetets eksamensordning

FAKTA OM MODULET

Engelsk titel	Network Security
Modulkode	ESNDCD2P1
Modultype	Projekt
Varighed	1 semester
Semester	Forår
ECTS	15
Undervisningssprog	Dansk og engelsk
Undervisningssted	Campus København
Modulansvarlig	Tatiana Kozlova Madsen

ORGANISATION

Uddannelsesejer	Diplomingeniør i cybersikkerhed
Studienævn	Studienævn for Elektronik og IT
Institut	Institut for Elektroniske Systemer
Fakultet	Det Teknisk Fakultet for IT og Design

MATEMATIK FOR CYBERSIKKERHED

2025/2026

MODULETS INDHOLD, FORLØB OG PÆDAGOGIK

Dette kursus handler om det matematiske grundlag, der er afgørende for cybersikkerhed. De studerende får viden om mængdeteori, algoritmer, kompleksitetsanalyse, logaritmer, kombinatorik, lineær algebra og vektorrum.

LÆRINGSMÅL

VIDEN

- Viden om mængdelære: mængder, relationer, funktioner og kardinalitet
- Viden om grundlæggende talteori, modulær aritmetik, Euklids algoritme, den kinesiske restklasseteori, Fermats lille sætning og primtalsfaktorisering
- Viden om rekursive og iterative algoritmer
- Viden om tidskompleksitet
- Viden om logaritmer og eksponentielle funktioner
- Viden om metoder til løsning af lineære ligningssystemer

FÆRDIGHEDER

- Færdigheder i at bevise korrektheden og kompleksiteten af en given algoritme
- Færdigheder i at diskutere den optimale datastruktur til løsning af et givet problem
- Færdigheder i at løse lineære ligningssystemer
- Færdigheder i matrixoperationer (f.eks. multiplikation, inverse matricer)

KOMPETENCER

- Har opnået færdigheder i at anvende begreber inden for diskrete strukturer til at udvikle avancerede algoritmer, der bruges i kurser og projekter på uddannelsen
- Har opnået færdigheder i at anvende lineær algebra i kryptografiske algoritmer

UNDERVISNINGSFORM

Jf. beskrivelsen i §18

EKSAMEN

PRØVER

Prøvens navn	Matematik for cybersikkerhed
Prøveform	Skriftlig eller mundtlig
ECTS	5
Tilladte hjælpemidler	Med visse hjælpemidler: Se eksamensspecifikation
Bedømmelsesform	7-trins-skala
Censur	Intern prøve
Vurderingskriterier	Vurderingskriterierne er angivet i Universitetets eksamensordning

FAKTA OM MODULET

Engelsk titel	Mathematics for Cyber Security
Modulkode	ESNDCD2K1
Modultype	Kursus
Varighed	1 semester
Semester	Forår
ECTS	5
Undervisningssprog	Dansk og engelsk
Tomplads	Ja
Undervisningssted	Campus København
Modulansvarlig	Tatiana Kozlova Madsen

ORGANISATION

Uddannelsesejer	Diplomingeniør i cybersikkerhed
Studienævn	Studienævn for Elektronik og IT
Institut	Institut for Elektroniske Systemer
Fakultet	Det Teknisk Fakultet for IT og Design

SIKKERHED I COMPUTERSYSTEMER

2025/2026

MODULETS INDHOLD, FORLØB OG PÆDAGOGIK

Grundlæggende forståelse af computersystemers sikkerhed

LÆRINGSMÅL

VIDEN

- har viden om begreber og fagtermer inden for cybersikkerhed
- har forståelse af teorier og metoder for forebyggelse, detektion og håndtering af cyberangreb
- har indgående kendskab til moderne projektstyringsværktøjer

FÆRDIGHEDER

- kan anvende teorier og metoder omkring analyse af sikkerhedstrusler
- kan benytte sikkehedsprotokoller og "security-by-design" til løsning af givet problem
- kan foretage analyse af netværkstrafik med henblik på detektion af anomalier
- kan anvende udvalgte metoder og værktøjer til at angribe og forsvare IT-infrastruktur
- kan benytte tidssvarende udviklingsværktøjer til implementering af løsninger
- kan reflektere over egne erfaringer med projektarbejde ved hjælp af relevante analyseværktøjer
- er i stand til at arbejde på et projekt baseret på valg af projektstyringsværktøjer
- er i stand til at identificere afhængighed mellem projektets forskellige opgaver

KOMPETENCER

- kan gennemføre og reflektere over udviklingsforløb, som omfatter et sikkerhedsaspekt i et computersystem
- kan dokumentere projektresultater, så udenforstående kan foretage en faglig vurdering
- kan erkende behov for og tilvejebringe viden
- kan formidle projektets resultater under anvendelse af korrekt fagterminologi
- kan reflektere over egen brug af PBL-værktøjer i undersøgelserne, og hvordan disse kan bruges aktivt i fremtiden
- er i stand til at udføre en kritisk evaluering af relevansen af indsamlet viden i relation til projektarbejdet, herunder vurdering af egnetheden af valgte modeller, teorier og metoder

UNDERVISNINGSFORM

Jf. beskrivelsen i § 17

EKSAMEN

PRØVER

Prøvens navn	Sikkerhed i computersystemer
Prøveform	Skriftlig eller mundtlig
ECTS	5
Bedømmelsesform	7-trins-skala
Censur	Intern prøve
Vurderingskriterier	Vurderingskriterierne er angivet i Universitetets eksamensordning

FAKTA OM MODULET

Engelsk titel	Computer Systems Security
Modulkode	ESNCCEB4K2
Modultype	Kursus
Varighed	1 semester
Semester	Forår
ECTS	5
Undervisningssprog	Dansk og engelsk
Tomplads	Ja
Undervisningssted	Campus København
Modulansvarlig	Tatiana Kozlova Madsen

ORGANISATION

Uddannelsesejer	Bachelor (BSc) i teknisk videnskab (cyber- og computerteknologi)
Studienævn	Studienævn for Elektronik og IT
Institut	Institut for Elektroniske Systemer
Fakultet	Det Teknisk Fakultet for IT og Design

COMPUTERNETVÆRK

2025/2026

MODULETS INDHOLD, FORLØB OG PÆDAGOGIK

Den studerende skal gennem dette kursus opnå en bred viden om relevante dataprotokoller på tværs af OSI-modellen. Derudover skal den studerende opnå færdigheder i at kunne udvikle, arbejde med og analysere protokoller. Endelig skal den studerende opnå kompetencer inden for datanetværk og opnå en forståelse af sammenspil mellem datanetværk og dataprotokoller.

LÆRINGSMÅL

VIDEN

- redegøre for og anvende korrekt fagterminologi
- redegøre for væsentlige ydelsesmetrikker inden for netværk og kommunikation
- redegøre for problematikker, der adresseres i forskellige lag i OSI-modellen
- forstå mekanismerne bag mest anvendte protokoller sam f.eks. IP, TCP og UDP
- beskrive Quality of Service koncepter
- forstå og beskrive problematikker omkring tidssynkronisering

FÆRDIGHEDER

- analysere og forstå dataprotokoller ved brug af netværksanalyseværktøjer
- gennemskue datanetværk og deres konfigurering
- gennemskue og konfigurere væsentlige netværkskomponenter
- kunne implementere egne dataprotokoller på transportlags niveau, f.eks. TCP sockets
- kunne måle og vurdere ydelse af datanetværk

KOMPETENCER

- kunne designe egen dataprotokol, der lever op til fastlagte krav
- kunne opsætte og konfigurere simple datanetværk

UNDERVISNINGSFORM

Jf. beskrivelsen i § 17

EKSAMEN

PRØVER

Prøvens navn	Computernetværk
Prøveform	Skriftlig eller mundtlig
ECTS	5
Tilladte hjælpemidler	Med visse hjælpemidler: Se eksamensspecifikation
Bedømmelsesform	7-trins-skala
Censur	Intern prøve
Vurderingskriterier	Vurderingskriterierne er angivet i Universitetets eksamensordning

FAKTA OM MODULET

Engelsk titel	Computer Networks
Modulkode	ESNCCEB2K2
Modultype	Kursus
Varighed	1 semester
Semester	Forår
ECTS	5
Undervisningssprog	Dansk og engelsk
Tomplads	Ja
Undervisningssted	Campus København
Modulansvarlig	Tatiana Kozlova Madsen

ORGANISATION

Uddannelsesejer	Bachelor (BSc) i teknisk videnskab (cyber- og computerteknologi)
Studienævn	Studienævn for Elektronik og IT
Institut	Institut for Elektroniske Systemer
Fakultet	Det Teknisk Fakultet for IT og Design

SIKKERHED I APPLIKATIONSUDVIKLING

2025/2026

MODULETS INDHOLD, FORLØB OG PÆDAGOGIK

I projektmodulet får de studerende kompetencer i udvikling af en sikkerhedsløsning til en applikation, et netværk eller et indlejret system (eller en kombination af disse) ud fra de nyest tilgængelige teknologier.

LÆRINGSMÅL

VIDEN

- Forståelse for sikkerhedsprincipper og metodologier, der er relevante for udvikling af applikationer, netværk og indlejrede systemer
- Viden om de nyeste teknologier og værktøjer, der bruges til at designe og implementere sikkerhedsløsninger
- Bevidsthed om almindelige sårbarheder og trusselsmodeller, der er specifikke for applikationer, netværk og indlejrede systemer
- Forståelse for livscyklussen for sikker udvikling, herunder design, implementering, testning og implementering
- Viden om, hvordan data kan overføres sikkert mellem maskiner til fjernbehandling eller kommunikation
- Forståelse af principperne for "security by design" og "privacy by design" i udviklingen af sikre løsninger

FÆRDIGHEDER

- Designe og implementere en sikkerhedsløsning, der er skræddersyet til en applikation, et netværk eller et indlejret system, eller en kombination af disse
- Anvende moderne sikkerhedsteknologier og værktøjer til at afbøde specifikke sårbarheder og sikre sikker dataoverførsel mellem maskiner
- Integrere principperne for "security by design" og "privacy by design" i arkitekturen af applikationer og systemer
- Udføre sikkerhedsvurderinger og test for at validere effektiviteten af sikre designs og datahåndteringspraksisser
- Integrere sikkerhedsforanstaltninger i systemarkitekturen uden at gå på kompromis med brugervenlighed og ydeevne
- Samarbejde i et team om at håndtere komplekse sikkerhedskrav gennem hele projektets livscyklus

KOMPETENCER

- Analysere og håndtere virkelige sikkerhedsudfordringer i udvikling af applikationer, netværk eller indlejrede systemer med fokus på sikker dataoverførsel og designprincipper
- Arbejde selvstændigt eller i samarbejde for at udvikle innovative, praktiske og privatlivsbevidste sikkerhedsløsninger ved hjælp af avancerede teknologier
- Evaluere og forbedre sikkerhedsløsninger baseret på testresultater, feedback og skiftende sikkerhedsbehov
- Kommunikere projektresultater, løsninger og anvendelsen af principperne for "security by design" og "privacy by design" til både tekniske og ikke-tekniske målgrupper
- Demonstrere evnen til at tilgå sikkerhed holistisk og sikre, at løsninger er robuste, skalerbare og i overensstemmelse med krav til privatliv

UNDERVISNINGSFORM

Jf. beskrivelsen i §18

EKSAMEN

PRØVER

Prøvens navn	Sikkerhed i applikationsudvikling
Prøveform	Mundtlig pba. projekt

ECTS	15
Tilladte hjælpemidler	Alle skriftlige og alle elektroniske hjælpemidler
Bedømmelsesform	7-trins-skala
Censur	Ekstern prøve
Vurderingskriterier	Vurderingskriterierne er angivet i Universitetets eksamensordning

FAKTA OM MODULET

Engelsk titel	Security in Application Development
Modulkode	ESNDCD3P1
Modultype	Projekt
Varighed	1 semester
Semester	Efterår
ECTS	15
Undervisningssprog	Dansk og engelsk
Tomplads	Ja
Undervisningssted	Campus København
Modulansvarlig	Tatiana Kozlova Madsen

ORGANISATION

Uddannelsesejer	Diplomingeniør i cybersikkerhed
Studienævn	Studienævn for Elektronik og IT
Institut	Institut for Elektroniske Systemer
Fakultet	Det Teknisk Fakultet for IT og Design

ETISK HACKING

2025/2026

MODULETS INDHOLD, FORLØB OG PÆDAGOGIK

Dette kursus handler om metoder til penetrationstest, herunder rekognoscering, sårbarhedsanalyse og teknikker til at identificere og adressere sikkerhedssvagheder i systemer før og efter et sikkerhedsbrud. Gennem praktiske øvelser vil de studerende lære om etisk udnyttelse af systemer, at opdage sårbarheder, og at udvikle strategier til at sikre netværk.

LÆRINGSMÅL

VIDEN

- Forstå principperne og metodologierne for penetrationstest, herunder de etiske og juridiske implikationer
- Viden om rekognosceringsteknikker og deres anvendelse til indsamling af information om systemer og netværk
- Viden om almindelige sikkerhedssårbarheder i systemer, netværk og applikationer samt deres potentielle konsekvenser
- Viden om penetrationstestværktøjer (f.eks. Nmap, Metasploit) og rammer (f.eks. MITRE ATT&CK)
- Forståelse for de etiske og juridiske overvejelser ved udførelse af penetrationstest og sårbarhedsvurderinger

FÆRDIGHEDER

- Udføre rekognoscering for at indsamle information om systemer og netværk
- Identificere og analysere sikkerhedssårbarheder ved hjælp af penetrationstestværktøjer og -teknikker
- Udføre kontrolleret og etisk udnyttelse af systemer for at afdække svagheder
- Udvikle og implementere strategier til at forbedre sikkerheden i netværk og systemer baseret på identificerede sårbarheder
- Dokumentere resultater og udarbejde omfattende rapporter, der beskriver sårbarheder og anbefalede afhjælpninger

KOMPETENCER

- Anvende metodologier for penetrationstest til at vurdere sikkerheden i systemer og netværk på en etisk og ansvarlig måde
- Arbejde selvstændigt eller i samarbejde for at identificere og håndtere sikkerhedssvagheder i forskellige miljøer
- Kommunikere tekniske resultater effektivt til både tekniske og ikke-tekniske interessenter
- Opbygge et fundament for at udvikle færdigheder inden for cybersikkerhed og bidrage til udviklingen af sikre systemer

UNDERVISNINGSFORM

Jf. beskrivelsen i §18

EKSAMEN

PRØVER

Prøvens navn	Etisk hacking
Prøveform	Skriftlig eller mundtlig
ECTS	5
Tilladte hjælpemidler	Med visse hjælpemidler: Se eksamensspecifikation
Bedømmelsesform	Bestået/ikke bestået

Censur	Intern prøve
Vurderingskriterier	Vurderingskriterierne er angivet i Universitetets eksamensordning

FAKTA OM MODULET

Engelsk titel	Ethical Hacking
Modulkode	ESNDCD3K1
Modultype	Kursus
Varighed	1 semester
Semester	Efterår
ECTS	5
Undervisningssprog	Dansk og engelsk
Tomplads	Ja
Undervisningssted	Campus København
Modulansvarlig	Tatiana Kozlova Madsen

ORGANISATION

Uddannelsesejer	Diplomingeniør i cybersikkerhed
Studienævn	Studienævn for Elektronik og IT
Institut	Institut for Elektroniske Systemer
Fakultet	Det Teknisk Fakultet for IT og Design

PROGRAMMERING OG DATABASER FOR CYBERSIKKERHED

2025/2026

MODULETS INDHOLD, FORLØB OG PÆDAGOGIK

Dette kursus introducerer bachelorstuderende til grundlæggende færdigheder inden for programmering og databaser med et fokus på cybersikkerhed. Med udgangspunkt i deres viden om imperativ programmering lærer de studerende at udvikle enkle applikationer, opbygge og arbejde med databaser samt forstå, hvordan man beskytter data mod grundlæggende sikkerhedstrusler. Gennem praktiske øvelser og teori opnår de indsigt i, hvordan programmering og databasedesign anvendes til at analysere og forebygge sikkerhedsmæssige udfordringer i små systemer. Kurset er designet til at bygge videre på deres programmeringserfaring og introducere dem til sikkerhedskoncepter i en tilgængelig kontekst.

LÆRINGSMÅL

VIDEN

- Forståelse af grundlæggende programmeringsprincipper og deres anvendelse i udviklingen af funktionelle applikationer
- Viden om databasedesign, herunder oprettelse af tabeller, relationer og forespørgsler
- Grundlæggende forståelse af datahåndtering og lagring i databaser og filer
- Bevidsthed om enkle metoder til at identificere og afbøde sårbarheder i programmer og databaser
- Anvendelse af programmering til at analysere cybersikkerhedsrelaterede data som netværkstrafik osv.

FÆRDIGHEDER

- Udvikle funktionelle programmer ved hjælp af grundlæggende programmeringsprincipper, herunder fil- og datahåndtering
- Designe og implementere strukturerede databaser, herunder oprettelse af tabeller, definition af relationer og udarbejdelse af forespørgsler
- Analysere og fejlfinde simple programmer og databaser for at sikre korrekthed og effektivitet
- Anvende grundlæggende metoder til at identificere og afbøde sårbarheder i programmer og databaser
- Bruge programmering til at analysere cybersikkerhedsrelaterede data, såsom netværkstrafik, logfiler eller andre datasæt

KOMPETENCER

- Anvende programmerings- og databaseviden til at designe, udvikle og administrere små applikationer, der involverer struktureret datahåndtering
- Arbejde selvstændigt eller i teams for at løse praktiske udfordringer inden for programmering, databaser eller grundlæggende cybersikkerhedsrelateret dataanalyse
- Vurdere og forbedre funktionalitet, sikkerhed og effektivitet i applikationer og databaser
- Opbygge et fundament for anvendelse af programmerings- og databasefærdigheder i tværfaglige områder, herunder cybersikkerhed

UNDERVISNINGSFORM

Jf. beskrivelsen i §18

EKSAMEN

PRØVER

Prøvens navn	Programmering og databaser for cybersikkerhed

Prøveform	Skriftlig eller mundtlig
ECTS	5
Tilladte hjælpemidler	Med visse hjælpemidler: Se eksamensspecifikation
Bedømmelsesform	7-trins-skala
Censur	Intern prøve
Vurderingskriterier	Vurderingskriterierne er angivet i Universitetets eksamensordning

FAKTA OM MODULET

Engelsk titel	Programming and Databases for Cyber Security
Modulkode	ESNDCD3K4
Modultype	Kursus
Varighed	1 semester
Semester	Efterår
ECTS	5
Undervisningssprog	Dansk og engelsk
Tomplads	Ja
Undervisningssted	Campus København
Modulansvarlig	Tatiana Kozlova Madsen

ORGANISATION

Uddannelsesejer	Diplomingeniør i cybersikkerhed
Studienævn	Studienævn for Elektronik og IT
Institut	Institut for Elektroniske Systemer
Fakultet	Det Teknisk Fakultet for IT og Design

PROGRAMMERING AF INDLEJREDE SYSTEMER

2025/2026

MODULETS INDHOLD, FORLØB OG PÆDAGOGIK

Studerende på dette kursus opnår teoretisk og praktisk viden om avancerede koncepter af computerarkitekturer og grundlæggende elementer af indlejrede systemer. Studerende vil lære om principper for multiheading, synkronisering og interproces-kommunikation og de udfordringer synkroniseringstråde og processer har, når de tilgår delte ressourcer. Studerende vil få et overblik over de nyeste enheder med indlejrede systemer og lære om deres begrænsninger og muligheder gennem programmering.

LÆRINGSMÅL

VIDEN

- har viden om de vigtigste komponenter af et operativsystem (OS), og hvorledes man kommunikerer om struktur og virkemåde af OS-komponenter.
- har viden om forskellige operativsystemer og computerarkitekturer med fokus på indlejrede systemer.
- har viden om komponenter i en typisk computer eller micro-controller, og hvordan operativsystemer anvender disse komponenter.
- har viden om de vigtigste udfordringer, som et givet OS-løser, såsom hukommelseshåndtering, interproces-kommunikation, synkronisering osv., og kan diskutere mulige løsninger til disse.
- har viden om de nyeste micro-controllers, deres begrænsninger, og hvordan de kan anvendes i IoT-enheder.
- har viden om programmering af indlejrede systemer og hvordan det kan anvendes i indlejrede enheder.

FÆRDIGHEDER

- kan oprette tråde og processer og afvikle dem i et program.
- kan skrive simple programmer for indlejrede enheder og i mikrokontrollere.
- kan anvende programmering til at adressere udfordringer relateret il tråde, proces-synkronisering og hukommelseshåndtering.
- har færdigheder i design og implementering af datastrukturer for indlejrede enheder.
- kan anvende kommandolinjer for at afvikle en simple kommando.

KOMPETENCER

- kan anvende sin viden inden for computerarkitekturer og indlejrede systemer i forhold til udviklingsprojekter på flere abstraktionsniveauer.
- har forståelse af arkitekturen for en given enhed samt egenskaberne for det tilhørende operativsystem,
- kan skrive optimerede programmer, som er tilpasset en bestemt computerarkitektur.

UNDERVISNINGSFORM

Jf. beskrivelsen i §17

EKSAMEN

PRØVER

Prøvens navn	Programmering af indlejrede systemer
Prøveform	Skriftlig eller mundtlig
ECTS	5
Bedømmelsesform	7-trins-skala

Censur	Intern prøve
Vurderingskriterier	Vurderingskriterierne er angivet i Universitetets eksamensordning

FAKTA OM MODULET

Engelsk titel	Programming of embedded systems
Modulkode	ESNCCTB3K1
Modultype	Kursus
Varighed	1 semester
Semester	Efterår
ECTS	5
Undervisningssprog	Dansk og engelsk
Tomplads	Ja
Undervisningssted	Campus København
Modulansvarlig	Tatiana Kozlova Madsen

ORGANISATION

Uddannelsesejer	Bachelor (BSc) i teknisk videnskab (cyber- og computerteknologi)
Studienævn	Studienævn for Elektronik og IT
Institut	Institut for Elektroniske Systemer
Fakultet	Det Teknisk Fakultet for IT og Design

CYBERANGREB OG -FORSVAR

2025/2026

MODULETS INDHOLD, FORLØB OG PÆDAGOGIK

I dette projektmodul arbejder de studerende med et konkret system og lærer, hvordan det kan angribes og/eller forsvares. Ved at lære at "tænke som en angriber" får de studerende en bedre forståelse af, hvordan systemer kan sikres mod angreb, og hvordan angreb opdages.

LÆRINGSMÅL

VIDEN

- Har viden om angrebsmetoder og forsvarsstrategier
- Forstår begreberne red team- og blue team-øvelser, inklusive deres roller, mål og metoder i cybersikkerhedsvurderinger
- Har viden om teknikker til at opdage, afbøde og reagere på sikkerhedshændelser i realtid
- Forstår integrationen af risikostyringsprincipper i angrebs- og forsvarsscenarier, herunder risikovurdering og prioritering af modforanstaltninger
- Har viden om statistiske metoders rolle i at analysere angrebsmønstre og evaluere effektiviteten af forsvarsmekanismer

FÆRDIGHEDER

- Kunne simulere og udføre realistiske angrebsscenarier og forsvare systemer mod dem ved hjælp af branche-standardværktøjer og -teknikker
- Kunne vurdere og kortlægge sårbarheder i et givet system for at identificere potentielle angrebsvektorer og prioritere forsvar
- Kunne anvende datasikkerheds- og privatlivsprincipper til at designe og teste robuste forsvarsmekanismer, der overholder juridiske og etiske standarder
- Kunne analysere og fortolke risikofaktorer ved hjælp af statistiske metoder for at understøtte informerede beslutninger under øvelser
- Kunne dokumentere og kommunikere resultater fra simulerede øvelser, herunder hændelsesrapporter, risikovurderinger og foreslåede forbedringer

KOMPETENCER

- Have kompetence til at designe og udføre omfattende angrebs- og forsvarsøvelser i organisatoriske sammenhænge, med fokus på tilpasning til realistiske scenarier
- Have kompetence til at integrere viden om risikostyring, datasikkerhed og privatliv i planlægning og udførelse af angrebs- og forsvarssimulationer
- Have kompetence til at tilpasse og anvende lærte strategier til nye eller fremvoksende trusler, med fokus på kontinuerlig forbedring af forsvarsmekanismer og strategier for hændelsesrespons
- Have kompetence til at præsentere resultaterne af øvelserne

UNDERVISNINGSFORM

Jf. beskrivelsen i §18

EKSAMEN

PRØVER

Prøvens navn	Cyberangreb og -forsvar
Prøveform	Mundtlig pba. projekt

ECTS	15
Tilladte hjælpemidler	Alle skriftlige og alle elektroniske hjælpemidler
Bedømmelsesform	7-trins-skala
Censur	Intern prøve
Vurderingskriterier	Vurderingskriterierne er angivet i Universitetets eksamensordning

FAKTA OM MODULET

Engelsk titel	Cyber Attacks and Defense
Modulkode	ESNDCD4P1
Modultype	Projekt
Varighed	1 semester
Semester	Forår
ECTS	15
Undervisningssprog	Dansk og engelsk
Undervisningssted	Campus København
Modulansvarlig	Tatiana Kozlova Madsen

ORGANISATION

Uddannelsesejer	Diplomingeniør i cybersikkerhed
Studienævn	Studienævn for Elektronik og IT
Institut	Institut for Elektroniske Systemer
Fakultet	Det Teknisk Fakultet for IT og Design

RISIKOHÅNDTERING

2025/2026

MODULETS INDHOLD, FORLØB OG PÆDAGOGIK

Dette kursus handler om metoder til at identificere, analysere og prioritere cybersikkerhedstrusler i samspil med risikohåndtering, business continuity-planer og omkostningseffektive sikkerhedsløsninger

LÆRINGSMÅL

VIDEN

- Have viden om metoder til at identificere, analysere og prioritere cybersikkerhedsrisici i forskellige organisatoriske kontekster
- Forstå strategier for risikoreduktion og kontrol, herunder implementering af tekniske, organisatoriske og proceduremæssige kontroller
- Have viden om forretningskontinuitet, katastrofehåndtering og beredskabsplaner, herunder strategier til at opretholde og genoprette operationer efter hændelser
- Have viden om risikovurderingsmetoder og målinger, herunder deres anvendelse til at kvantificere og evaluere risici

FÆRDIGHEDER

- Kunne identificere, analysere og prioritere cybersikkerhedstrusler ved hjælp af strukturerede risikovurderingsteknikker
- Kunne udvikle og foreslå planer for risikoreduktion, der integrerer tekniske og organisatoriske kontroller
- Kunne designe og implementere forretningskontinuitet, katastrofehåndtering og beredskabsplaner, der sikrer operationel modstandsdygtighed
- Kunne kommunikere risikovurderinger, strategier for risikoreduktion og beredskabsplaner effektivt til forskellige interessenter

KOMPETENCER

- Have kompetence til at evaluere og tilpasse risikovurderingsmetoder til at håndtere nye cybersikkerhedstrusler
- Have kompetence til at integrere beredskabsplanlægning med forretningskontinuitets- og katastrofehåndteringsstrategier for at sikre hurtig genopretning efter sikkerhedshændelser

UNDERVISNINGSFORM

Jf. beskrivelsen i §18

EKSAMEN

PRØVER

Prøvens navn	Risikohåndtering
Prøveform	Skriftlig eller mundtlig
ECTS	5
Tilladte hjælpemidler	Med visse hjælpemidler: Se eksamensspecifikation
Bedømmelsesform	7-trins-skala
Censur	Intern prøve

Vurderingskriterier	Vurderingskriterierne er angivet i Universitetets eksamensordning

FAKTA OM MODULET

Engelsk titel	Risk Management
Modulkode	ESNDCD4K1
Modultype	Kursus
Varighed	1 semester
Semester	Forår
ECTS	5
Undervisningssprog	Dansk og engelsk
Tomplads	Ja
Undervisningssted	Campus København
Modulansvarlig	Tatiana Kozlova Madsen

ORGANISATION

Uddannelsesejer	Diplomingeniør i cybersikkerhed
Studienævn	Studienævn for Elektronik og IT
Institut	Institut for Elektroniske Systemer
Fakultet	Det Teknisk Fakultet for IT og Design

DATASIKKERHED OG PRIVATLIVSBESKYTTELSE

2025/2026

MODULETS INDHOLD, FORLØB OG PÆDAGOGIK

Dette kursus dækker teknikker til at beskytte dataintegritet, fortrolighed og tilgængelighed. De studerende udforsker kryptering, adgangskontrol og sikre kommunikationsmetoder for at beskytte følsomme oplysninger mod cybertrusler.

LÆRINGSMÅL

VIDEN

- Have viden om teknikker og bedste praksis til at sikre dataintegritet, fortrolighed og tilgængelighed inden for cybersikkerhed
- Have viden om begrebet "privatliv" i databeskyttelse
- Forstå krypteringsmetoder, herunder symmetrisk og asymmetrisk kryptering, hashing og digitale signaturer, samt deres anvendelser i beskyttelse af følsomme oplysninger
- Have viden om adgangskontrolmodeller og sikre kommunikationsprotokoller samt deres betydning for datasikkerhed
- Have viden om juridiske, etiske og regulatoriske rammer for databeskyttelse

FÆRDIGHEDER

- Kunne anvende krypteringsteknikker til at beskytte følsomme data, både i hvile og under transmission, ved hjælp af branche-standardprotokoller
- Kunne implementere teknologier til forbedring af privatliv og udføre risikovurderinger af privatliv, samtidig med at overholdelse af regler for databeskyttelse sikres
- Kunne vurdere krav til databeskyttelse og designe systemer, der integrerer privatlivsbeskyttelse såsom "privacy by design" og "privacy by default" i udviklingsprocessen

KOMPETENCER

- Have kompetence til at designe sikre datastyringssystemer, der balancerer krav til sikkerhed, privatliv og brugervenlighed
- Have kompetence til kritisk at analysere risici for privatliv og anvende de mest effektive teknologier til forbedring af privatliv for at beskytte følsomme oplysninger i komplekse systemer

UNDERVISNINGSFORM

Jf. beskrivelsen i §18

EKSAMEN

PRØVER

Prøvens navn	Datasikkerhed og privatlivsbeskyttelse
Prøveform	Skriftlig eller mundtlig
ECTS	5
Tilladte hjælpemidler	Med visse hjælpemidler: Se eksamensspecifikation
Bedømmelsesform	7-trins-skala
Censur	Intern prøve

Vurderingskriterier	Vurderingskriterierne er angivet i Universitetets eksamensordning

FAKTA OM MODULET

Engelsk titel	Data Security and Privacy Protection
Modulkode	ESNDCD4K2
Modultype	Kursus
Varighed	1 semester
Semester	Forår
ECTS	5
Undervisningssprog	Dansk og engelsk
Tomplads	Ja
Undervisningssted	Campus København
Modulansvarlig	Tatiana Kozlova Madsen

ORGANISATION

Uddannelsesejer	Diplomingeniør i cybersikkerhed
Studienævn	Studienævn for Elektronik og IT
Institut	Institut for Elektroniske Systemer
Fakultet	Det Teknisk Fakultet for IT og Design

SANDSYNLIGHEDSREGNING OG STATISTIK

2025/2026

MODULETS INDHOLD, FORLØB OG PÆDAGOGIK

Kurset har til formål at introducere studerende til grundlæggende koncepter inden for sandsynlighed, statistik og stokastiske processer. Studerende skal opnå færdigheder, så de kan modellere og løse simple ingeniørmæssige problemstillinger, der involverer tilfældighed.

LÆRINGSMÅL

VIDEN

- har viden om koncepter inden for sandsynlighedsrum
- har viden om konceptuelle modeller til estimering og hypoteseafprøvning
- forstår grundlæggende koncepter inden for sandsynlighedsteori, såsom sandsynlighedsteori af en begivenhed og tilfældige variable
- forstår grundlæggende koncepter inden for statistik, bl.a. binær hypoteseafprøvning

FÆRDIGHEDER

- har færdigheder til at anvende og forstå:
  - bayers rule i simple situationer
  - sandsynligheden for, at tilfældige variable med binomial-, poisson- eller normalfordeling antager værdier i et givet interval
  - forventningsværdi og standardafvigelse for tilfældige variable med binomial-, poisson- eller normalfordeling
  - marginalfordelingen af en normalfordeling med flere variable
- har færdigheder til at kunne anvende og forstå maximum Likelihood (ML) estimering og binære hypoteseafprøvning i simple situationer, som involverer binomial-, Poisson- eller normalfordeling

KOMPETENCER

- Skal kunne anvende generelle koncepter fra sandsynlighedsteori og statistik inden for forskellige områder. Dette indebærer at kunne vælge egnet metode, evaluere resultat og konkludere ud for forståelsen af resultaterne

UNDERVISNINGSFORM

Jf. beskrivelsen i § 17

EKSAMEN

PRØVER

Prøvens navn	Sandsynlighedsregning og statistik
Prøveform	Skriftlig eller mundtlig
ECTS	5
Tilladte hjælpemidler	Med visse hjælpemidler: Se eksamensspecifikation
Bedømmelsesform	7-trins-skala
Censur	Intern prøve
Vurderingskriterier	Vurderingskriterierne er angivet i Universitetets eksamensordning

FAKTA OM MODULET

Engelsk titel	Probability Theory and Statistics
Modulkode	ESNCCEB4K3
Modultype	Kursus
Varighed	1 semester
Semester	Forår
ECTS	5
Undervisningssprog	Dansk og engelsk
Tomplads	Ja
Undervisningssted	Campus København
Modulansvarlig	Tatiana Kozlova Madsen

ORGANISATION

Uddannelsesejer	Bachelor (BSc) i teknisk videnskab (cyber- og computerteknologi)
Studienævn	Studienævn for Elektronik og IT
Institut	Institut for Elektroniske Systemer
Fakultet	Det Teknisk Fakultet for IT og Design

CLOUD SIKKERHED

2025/2026

MODULETS INDHOLD, FORLØB OG PÆDAGOGIK

Dette kursus udstyrer de studerende med viden og kompetencer til at bygge sikre distribuerede systemer i skyen, udforske cloud-implementering og cloud-servicemodeller sammen med aktuelle trends og sikkerhedsovervejelser for cloud, virtualisering og edge computing.

LÆRINGSMÅL

VIDEN

- Have viden om de grundlæggende begreber inden for cloud computing, aktuelle tendenser, rammer og bedste praksis inden for cloud computing
- Forstå de forskellige modeller for cloud-implementering (offentlig, privat og hybrid) og servicemodeller (IaaS, PaaS, SaaS), inklusive deres sikkerhedsmæssige implikationer og anvendelsesområder
- Forstå principperne for virtualisering og deres sikkerhedsaspekter
- Have viden om tredjeparts intelligens og sikkerhedsværktøjer, der er tilgængelige i cloudmiljøer

FÆRDIGHEDER

- Kunne evaluere og vælge passende cloud-implementeringsmodeller (offentlig, privat, hybrid) og servicemodeller (IaaS, PaaS, SaaS) baseret på organisatoriske behov, samtidig med at relaterede sikkerhedsrisici adresseres
- Kunne implementere og administrere sikkerhedsforanstaltninger i virtualiserede miljøer, herunder sikring af virtuelle maskiner, containere og cloud-native applikationer
- Kunne anvende tredjeparts intelligensværktøjer og platforme i cloud-miljøer til at overvåge trusler, styrke sikkerhedsniveauet og automatisere trusselsdetektion og -respons

KOMPETENCER

- Have kompetence til at vurdere og afbøde sikkerhedsrisici i forskellige cloud-implementeringsmodeller og servicemodeller, samtidig med at overholdelse af relevante standarder og regler sikres
- Have kompetence til at administrere og optimere sikkerheden i virtuelle miljøer

UNDERVISNINGSFORM

Jf. beskrivelsen i §18

EKSAMEN

PRØVER

Prøvens navn	Cloud sikkerhed
Prøveform	Skriftlig eller mundtlig
ECTS	5
Tilladte hjælpemidler	Med visse hjælpemidler: Se eksamensspecifikation
Bedømmelsesform	7-trins-skala
Censur	Ekstern prøve
Vurderingskriterier	Vurderingskriterierne er angivet i Universitetets eksamensordning

FAKTA OM MODULET

Engelsk titel	Cloud Security
Modulkode	ESNDCD5K1
Modultype	Kursus
Varighed	1 semester
Semester	Efterår
ECTS	5
Undervisningssprog	Dansk og engelsk
Tomplads	Ja
Undervisningssted	Campus København
Modulansvarlig	Tatiana Kozlova Madsen

ORGANISATION

Uddannelsesejer	Diplomingeniør i cybersikkerhed
Studienævn	Studienævn for Elektronik og IT
Institut	Institut for Elektroniske Systemer
Fakultet	Det Teknisk Fakultet for IT og Design

SIKKERHED I IOT- OG OT-MILJØER

2025/2026

MODULETS INDHOLD, FORLØB OG PÆDAGOGIK

Dette kursus gør de studerende i stand til at navigere i sikkerhedsudfordringerne ved sammenkoblede IoT- og OT-miljøer. Ved at udforske nye teknologier og forskellige IoT- og OT-enheder vil deltagerne få grundlæggende viden om sikkerhedskoncepter og best practice for sikring af disse komplekse systemer.

LÆRINGSMÅL

VIDEN

- Har viden om, hvordan IoT påvirker samfundet, og fremtidige udviklingstendenser for IoT og OT-enheder
- Forstå mangfoldigheden af IoT- og OT-enheder, herunder deres karakteristika, begrænsninger og de unikke sikkerhedsudfordringer, de udgør i komplekse systemer
- Have viden og forståelse for sikkerhedskoncepter relateret til IoT- og OT-enheder
- Give den studerende viden om nye teknologier i konteksten af IoT- og OT-systemer
- Forstå truslerne og sårbarhederne, der er specifikke for IoT- og OT-miljøer

FÆRDIGHEDER

- Kunne designe og implementere løsninger, hvor IoT- og OT-enheder sikkert leverer data til et system, der sikrer både funktionalitet og databeskyttelse
- Kunne anvende IoT-netværksprotokoller til sikkert at overføre data fra IoT-enheder til centrale servere eller edge-systemer
- Kunne integrere sikkerhedsforanstaltninger i forskellige lag af arkitekturen, herunder enhedsniveau-sikkerhed, kommunikationsprotokoller og central systeminfrastruktur
- Kunne anvende de nyeste udviklingsværktøjer og rammer til at integrere IoT- og OT-løsninger med cloud-tjenester

KOMPETENCER

- Have kompetence til at udvikle en omfattende IoT- og OT-løsning, der inkluderer aspekter af IoT- og OT-programmering, netværksprotokoller, sikkerhedsforanstaltninger og integration med cloud computing

UNDERVISNINGSFORM

Jf. beskrivelsen i §18

EKSAMEN

PRØVER

Prøvens navn	Sikkerhed i IoT- og OT-miljøer
Prøveform	Skriftlig eller mundtlig
ECTS	5
Tilladte hjælpemidler	Med visse hjælpemidler: Se eksamensspecifikation
Bedømmelsesform	7-trins-skala
Censur	Intern prøve
Vurderingskriterier	Vurderingskriterierne er angivet i Universitetets eksamensordning

FAKTA OM MODULET

Engelsk titel	Security in IoT and OT Environments
Modulkode	ESNDCD5K3
Modultype	Kursus
Varighed	1 semester
Semester	Efterår
ECTS	5
Undervisningssprog	Dansk og engelsk
Tomplads	Ja
Undervisningssted	Campus København
Modulansvarlig	Tatiana Kozlova Madsen

ORGANISATION

Uddannelsesejer	Diplomingeniør i cybersikkerhed
Studienævn	Studienævn for Elektronik og IT
Institut	Institut for Elektroniske Systemer
Fakultet	Det Teknisk Fakultet for IT og Design

DIPLOMINGENIØRPRAKTIK

2025/2026

MODULETS INDHOLD, FORLØB OG PÆDAGOGIK

Praktikforløbet giver de studerende mulighed for at anvende deres akademiske viden på cybersikkerhedsudfordringer i den virkelige verden, samtidig med at de udvikler værdifulde professionelle kompetencer. Ved at integrere praktikanter i igangværende projekter kan virksomheder styrke deres rekrutteringsmuligheder og få adgang til nye perspektiver og potentielt samarbejde om den studerendes afsluttende projekt. Til gengæld for deres bidrag opnår praktikanterne et godt fundament for en fremtidig karriere inden for cybersikkerhed.

Studerende er ansvarlige for selv at finde en praktikplads. Praktikforløbet skal være relevant for området cybersikkerhed og kræver normalt, at virksomheden betaler den studerende en løn. I særlige tilfælde kan praktikkoordinatoren, som er udpeget af studienævnet, hjælpe med at etablere nødvendige virksomhedskontakter.

Universitetet skal godkende praktikpladsen, hvorefter der udarbejdes en praktikaftale mellem den studerende og virksomheden. Virksomheden udpeger en praktikvejleder, som vil fungere som primær kontaktperson for den studerende under praktikforløbet. Praktikaftalen fastlægger læringsmål, arbejdsopgaver, praktikperiode, arbejdstid, praktikkoordinator, praktikvejleder og andre relevante detaljer. Aftalen skal underskrives af praktikvejlederen/virksomheden, den studerende (praktikant), praktikkoordinatoren og studienævnet inden praktikstart.

Hvis der under praktikforløbet opstår ændringer, der nødvendiggør justeringer af den godkendte praktikaftale, skal disse godkendes af praktikkoordinatoren og studienævnet.

Under praktikken skal den studerende føre en dagbog, som er en daglig rapport over begivenheder, der finder sted i løbet af dagen, primært om det udførte arbejde.

Praktikrapporten skal udarbejdes i overensstemmelse med de generelle retningslinjer, der tidligere har været gældende for udarbejdelse af projektrapporter i programmets tidligere semestre.

Praktikrapporten skal dog også indeholde:

- Beskrivelse af virksomheden – herunder organisationen
- Beskrivelse af virksomhedens arbejdsområder
- Oversigt over de arbejdsområder, som den studerende har været involveret i
- Gennemgang af mindst ét fagligt emne, der er relevant for uddannelsen, som de studerende har arbejdet med under praktikken. Gennemgangen skal – i det omfang det er relevant – omfatte problemanalyse, teori, metoder, modeller, løsningsforslag, implementering, test, konklusion mv.
- Dagbog
- Analyse af de faglige, arbejdsrelaterede og sociale udbytter af praktikken
- Erfaringer fra praktikken og refleksion over processen

Behandlingen af det/de faglige emner skal være på et niveau svarende til 6. semester.

LÆRINGSMÅL

VIDEN

- Have viden om en virksomheds organisation og arbejde fra et ingeniørperspektiv, herunder dens cybersikkerhedspraksis
- Kunne forklare de emner, der er relevante for uddannelsen, som er blevet arbejdet med under praktikopholdet, herunder hvilke teorier og metoder der er blevet anvendt, og hvilke resultater der er opnået
- Kunne forstå og forklare sammenhængen mellem teori i uddannelsen og praksis
- Udvikle bevidsthed om branchetrends, udfordringer og muligheder inden for cybersikkerhed

FÆRDIGHEDER

- Anvende cybersikkerhedsteorier, metoder og værktøjer til at løse praktiske problemer i et professionelt miljø
- Kunne vurdere de anvendte teorier og metoder i forhold til de teoretiske og/eller empiriske principper og metoder, der er brugt i studiets tidligere kurser og projektarbejde
- Analysere organisatoriske cybersikkerhedsproblemer og foreslå løsninger baseret på akademisk og praktisk viden
- Kommunikere effektivt med teammedlemmer, vejledere og interessenter i virksomheden
- Kunne analysere, om professionen har nye faglige behov, der bør/kan imødekommes af uddannelsen
- Dokumentere og rapportere arbejdsprocesser og resultater gennem dagbøger og strukturerede rapporter

KOMPETENCER

- Kunne dokumentere praktikopholdet i en praktikrapport, så opfyldelsen af praktikopholdets læringsmål kan evalueres
- Kunne analysere og reflektere over de faglige, arbejdsrelaterede og sociale fordele ved praktikopholdet
- Kunne håndtere udviklingsorienterede situationer i studie- og arbejdskontekster
- Tilpasse sig organisatoriske kulturer og arbejdsmiljøer, mens der opretholdes fokus på cybersikkerhedsmål
- Udvikle et fundament for en fremtidig karriere inden for cybersikkerhed gennem praktisk erfaring og netværksmuligheder

UNDERVISNINGSFORM

Jf. beskrivelsen i §18

EKSAMEN

FORUDSÆTNING FOR INDSTILLING TIL PRØVEN

- Udtalelse fra praktikvejlederen/virksomheden, som dokumenterer praktikkens gennemførelse

PRØVER

Prøvens navn	Diplomingeniørpraktik
Prøveform	Mundtlig pba. projekt Praktikopholdet evalueres på grundlag af: - Praktikrapporten - Mundtlig præstation Evalueringen foretages af den studerendes AAU-vejleder (eksaminator) og en censor samt om muligt med deltagelse af praktikvejlederen fra virksomheden. Selve bedømmelsen foregår dog alene mellem eksaminator og censor.
ECTS	30

Tilladte hjælpemidler	Alle skriftlige og alle elektroniske hjælpemidler
Bedømmelsesform	Bestået/ikke bestået
Censur	Intern prøve
Vurderingskriterier	Vurderingskriterierne er angivet i Universitetets eksamensordning

FAKTA OM MODULET

Engelsk titel	Internship
Modulkode	ESNDCD6P1
Modultype	Projekt
Varighed	1 semester
Semester	Forår
ECTS	30
Undervisningssprog	Dansk og engelsk
Undervisningssted	Campus København
Modulansvarlig	Tatiana Kozlova Madsen

ORGANISATION

Uddannelsesejer	Diplomingeniør i cybersikkerhed
Studienævn	Studienævn for Elektronik og IT
Institut	Institut for Elektroniske Systemer
Fakultet	Det Teknisk Fakultet for IT og Design

BACHELORPROJEKT

2025/2026

MODULETS INDHOLD, FORLØB OG PÆDAGOGIK

I det sidste semester arbejder de studerende på færdiggørelsen af bacheloropgaven, som giver dem mulighed for at anvende teoretisk viden og praktiske færdigheder, som de har lært under deres studie. Projektet skal desuden demonstrere deres generelle færdigheder inden for problemanalyse og ingeniørvidenskab.

LÆRINGSMÅL

VIDEN

- Have viden om de teoretiske og praktiske fundamenter for cybersikkerhedsteknik, herunder avancerede teknikker til sikring af systemer, netværk og data
- Forstå metoder til at udføre omfattende problemanalyser og designe tekniske løsninger inden for cybersikkerhed
- Opnå dybdegående viden om det valgte emne og dets relevans for ingeniørarbejde og problemløsning
- Have viden om nøglemetoder til relevante analyser relateret til sikkerhedsudfordringer i computersystemer
- Have viden og forståelse for forhold og afhængigheder mellem systemkomponenter samt deres inflydelse på systemarkitekturer og betydning for cybersikkerhed
- Forstå de etiske, samfundsmæssige og juridiske overvejelser relateret til cybersikkerhedsløsninger i virkelige kontekster

FÆRDIGHEDER

- Anvende teoretisk viden og praktiske færdigheder til at definere, analysere og løse komplekse ingeniørmæssige problemer
- Udføre systematisk forskning og analyse for at understøtte udviklingen af innovative løsninger
- Kunne designe, implementere og evaluere en løsning eller prototype, der adresserer et specifikt cybersikkerhedsproblem ved hjælp af forskellige cybersikkerhedsværktøjer, rammer og metoder
- Kunne anvende avancerede analytiske og kritiske tænkningsfærdigheder til at vurdere effektiviteten, skalerbarheden og sikkerheden af foreslåede løsninger
- Forberede strukturerede projektrapporter, der præsenterer resultater og anbefalinger på en klar og professionel måde

KOMPETENCER

- Have opnået kompetencer til at demonstrere en sammenhængende forståelse af projektets relation til cybersikkerhedsområdet
- Have opnået kompetencer til at planlægge, strukturere og gennemføre et større projekt inden for cybersikkerhed
- Have opnået kompetencer til at reflektere over projektets betydning fra et teknisk og samfundsmæssigt perspektiv, især i forhold til sikkerhed
- Kan identificere deres egne læringsbehov og strukturere deres egen læring i forskellige læringsmiljøer
- Kan kommunikere problemer, metoder og resultater inden for det videnskabelige felt, skriftligt, mundtligt og ved brug af forskellige digitale medier, samt diskutere faglige og videnskabelige problemer med projektkolleger og vejleder(e)

UNDERVISNINGSFORM

Jf. beskrivelsen i §18

EKSAMEN

PRØVER

Prøvens navn	Bachelorprojekt

Prøveform	Speciale/afgangsprojekt
ECTS	20
Tilladte hjælpemidler	Alle skriftlige og alle elektroniske hjælpemidler
Bedømmelsesform	7-trins-skala
Censur	Ekstern prøve
Vurderingskriterier	Vurderingskriterierne er angivet i Universitetets eksamensordning

FAKTA OM MODULET

Engelsk titel	Bachelor's Project
Modulkode	ESNDCD7P1
Modultype	Projekt
Varighed	1 semester
Semester	Efterår
ECTS	20
Undervisningssprog	Dansk og engelsk
Undervisningssted	Campus København
Modulansvarlig	Tatiana Kozlova Madsen

ORGANISATION

Uddannelsesejer	Diplomingeniør i cybersikkerhed
Studienævn	Studienævn for Elektronik og IT
Institut	Institut for Elektroniske Systemer
Fakultet	Det Teknisk Fakultet for IT og Design

PROJEKTLEDELSE OG FORRETNINGSFORSTÅELSE

2025/2026

MODULETS INDHOLD, FORLØB OG PÆDAGOGIK

Dette kursus udstyrer de studerende med væsentlige færdigheder i at planlægge, udføre og styre ingeniørprojekter effektivt. De studerende lærer om projekters livscyklus, risikostyring og ledelsesteknikker, der kan sikre en succesfuld projektgennemførelse i tekniske miljøer, og de får indsigt i projekternes forretningsmæssige kontekst.

LÆRINGSMÅL

VIDEN

- Have viden om projektlivscyklusser og deres anvendelse i styring af tekniske og ingeniørprojekter i cybersikkerhedskontekster
- Have viden om risikostyringsteknikker og deres rolle i at sikre vellykket gennemførelse af tekniske projekter
- Forstå begreberne teknologiledelse og entreprenørskab og deres relevans for styring af ingeniørprojekter
- Forstå forretningsbegreber som omkostningsstrukturer, markedsanalyse og oprettelse af forretningsmodeller i forbindelse med cybersikkerhedsprojekter

FÆRDIGHEDER

- Planlægge, organisere og styre ingeniørprojekter effektivt for at sikre succesfulde resultater
- Kunne udføre risikovurderinger for ingeniørprojekter og udvikle strategier til risikoreduktion
- Kunne udføre en markedsanalyse for at identificere muligheder og udfordringer for teknologibaserede løsninger
- Kunne udvikle en forretningsmodel og tilpasse projektresultater til forretningsmål
- Kunne anvende værktøjer og teknikker til effektivt at håndtere tid, ressourcer og budgetter i tekniske projektmiljøer

KOMPETENCER

- Demonstrere evnen til selvstændigt at styre tekniske projekter fra start til afslutning
- Have kompetence til at lede komplekse tekniske projekter inden for cybersikkerhed og sikre, at de er i overensstemmelse med forretningsmål og markedsbehov
- Have kompetence til at integrere risikostyring og markedsindsigter i projektplanlægning og - gennemførelse
- Samarbejde effektivt med forskellige teams for at opnå projektmål i tekniske miljøer
- Kommunikere projektmål, fremskridt og resultater effektivt til både tekniske og ikke-tekniske interessenter

UNDERVISNINGSFORM

Jf. beskrivelsen i §18

EKSAMEN

PRØVER

Prøvens navn	Projektledelse og forretningsforståelse
Prøveform	Skriftlig eller mundtlig
ECTS	5
Tilladte hjælpemidler	Med visse hjælpemidler: Se eksamensspecifikation
Bedømmelsesform	7-trins-skala
Censur	Intern prøve

Vurderingskriterier	Vurderingskriterierne er angivet i Universitetets eksamensordning

FAKTA OM MODULET

Engelsk titel	Project Management and Business Understanding
Modulkode	ESNDCD7K1
Modultype	Kursus
Varighed	1 semester
Semester	Efterår
ECTS	5
Undervisningssprog	Dansk og engelsk
Tomplads	Ja
Undervisningssted	Campus København
Modulansvarlig	Tatiana Kozlova Madsen

ORGANISATION

Uddannelsesejer	Diplomingeniør i cybersikkerhed
Studienævn	Studienævn for Elektronik og IT
Institut	Institut for Elektroniske Systemer
Fakultet	Det Teknisk Fakultet for IT og Design

CYBERSIKKERHED I DISTRIBUEREDE SYSTEMER

2025/2026

MODULETS INDHOLD, FORLØB OG PÆDAGOGIK

I dette projekt designer og implementerer de studerende et sikkert distribueret system. Systemet kan inkludere IoT-, OT- og edge-enheder og en cloud-server. Studerende kan bruge machine learning og AI til at sikre deres system.

LÆRINGSMÅL

VIDEN

- Have viden om principperne og teknologierne bag sikre distribuerede systemer, herunder kommunikationsprotokoller, dataintegritet og sikkerhedsmekanismer i IoT-, OT- og cloud-miljøer
- Forstå sikkerhedsudfordringerne og risiciene, der er specifikke for IoT- og OT-enheder, herunder sårbarheder, autentifikation, datakryptering og netværkssikkerhed i disse miljøer
- Have viden om cloud-sikkerhedens rolle i distribuerede systemer, med fokus på sikker lagring, adgangskontrol, databeskyttelse og overholdelse af regler i cloud computing
- Forstå anvendelsen af maskinlæring og AI inden for cybersikkerhed, især i detektering af unormale mønstre, automatisering af trusselsdetektion og styrkelse af sikkerheden gennem adaptive systemer

FÆRDIGHEDER

- Kunne designe og implementere sikre distribuerede systemer, der integrerer IoT-, OT-, edgeenheder og cloud-servere, samt inkludere strategier for sikker kommunikation, autentifikation og enhedshåndtering
- Kunne implementere sikkerhedsteknikker til at beskytte data under transmission og i hvile i distribuerede systemer
- Kunne anvende maskinlæringsalgoritmer til detektion af unormale mønstre, trusselsdetektion og forudsigende sikkerhed for at styrke den samlede beskyttelse af et distribueret system

KOMPETENCER

- Have kompetence til at anvende sikkerhedsprincipper for at sikre sikkerheden og privatlivet for IoT- og OT-enheder, og beskytte dem mod trusler som uautoriseret adgang, databrud og netværksangreb
- Have kompetence til at vurdere og afbøde sikkerhedsrisici i komplekse, distribuerede systemer ved hjælp af en omfattende forståelse af cloud-sikkerhed, IoT/OT-sårbarheder og anvendelsen af maskinlæring

UNDERVISNINGSFORM

Jf. beskrivelsen i §18

EKSAMEN

PRØVER

Prøvens navn	Cybersikkerhed i distribuerede systemer
Prøveform	Mundtlig pba. projekt
ECTS	15
Tilladte hjælpemidler	Alle skriftlige og alle elektroniske hjælpemidler
Bedømmelsesform	7-trins-skala
Censur	Ekstern prøve
Vurderingskriterier	Vurderingskriterierne er angivet i Universitetets eksamensordning

FAKTA OM MODULET

Engelsk titel	Cyber Security in Distributed Systems
Modulkode	ESNDCD5P1
Modultype	Projekt
Varighed	1 semester
Semester	Efterår
ECTS	15
Undervisningssprog	Dansk og engelsk
Undervisningssted	Campus København
Modulansvarlig	Tatiana Kozlova Madsen

ORGANISATION

Uddannelsesejer	Diplomingeniør i cybersikkerhed
Studienævn	Studienævn for Elektronik og IT
Institut	Institut for Elektroniske Systemer
Fakultet	Det Teknisk Fakultet for IT og Design

CYBERSIKKERHED OG GOVERNANCE

2025/2026

MODULETS INDHOLD, FORLØB OG PÆDAGOGIK

Dette projekt handler om at designe ”security awareness” kampagner, udføre risikovurderinger og foreslå afværgestrategier for cybersikkerhedstrusler. Derudover vil de studerende udforske de juridiske og regulatoriske rammer for cybersikkerhed og governance i Europa.

LÆRINGSMÅL

VIDEN

- Have viden om principperne og metoderne til at designe effektive kampagner for sikkerhedsbevidsthed, med fokus på at fremme bedste praksis inden for cybersikkerhed i organisationer
- Forstå processen med at udføre omfattende risikovurderinger for at identificere cybersikkerhedstrusler og foreslå passende strategier til afbødning af organisatoriske sårbarheder
- Forstå cybersikkerhedens styringsstruktur i organisationer, med fokus på politikker, roller og ansvar for implementering af sikkerhedsforanstaltninger og reaktion på trusler
- Have viden om integrationen af cloud-sikkerhed, IoT- og OT-sikkerhedshensyn i bredere organisatoriske styrings- og risikostyringsrammer

FÆRDIGHEDER

- Kunne udføre risikovurderinger for specifikke cybersikkerhedstrusler i en organisation og foreslå målrettede strategier til at reducere risici
- Kunne analysere relevante juridiske og regulatoriske krav vedrørende cybersikkerhedsstyring i Europa og anvende disse regler på organisatoriske politikker og praksis
- Kunne integrere de specifikke cybersikkerhedsudfordringer, som cloud-miljøer, IoT- og OT-systemer udgør, i en organisations bredere styrings- og risikostyringsstrategier

KOMPETENCER

- Have kompetence til at udføre detaljerede risikovurderinger, evaluere komplekse cybersikkerhedstrusler og implementere strategiske afbødningsforanstaltninger for at styrke en organisations cybersikkerhedsposition
- Have kompetence til at håndtere de unikke sikkerhedsudfordringer, som cloud-, IoT- og OT-miljøer udgør, i organisatoriske cybersikkerhedsstyringsrammer og sikre, at disse teknologier integreres og administreres sikkert

UNDERVISNINGSFORM

Jf. beskrivelse i §18

EKSAMEN

PRØVER

Prøvens navn	Cybersikkerhed og governance
Prøveform	Mundtlig pba. projekt
ECTS	15
Tilladte hjælpemidler	Alle skriftlige og alle elektroniske hjælpemidler
Bedømmelsesform	7-trins-skala
Censur	Ekstern prøve

Vurderingskriterier	Vurderingskriterierne er angivet i Universitetets eksamensordning

FAKTA OM MODULET

Engelsk titel	Cyber Security and Governance
Modulkode	ESNDCD5P2
Modultype	Projekt
Varighed	1 semester
Semester	Efterår
ECTS	15
Undervisningssprog	Dansk og engelsk
Undervisningssted	Campus København
Modulansvarlig	Tatiana Kozlova Madsen

ORGANISATION

Uddannelsesejer	Diplomingeniør i cybersikkerhed
Studienævn	Studienævn for Elektronik og IT
Institut	Institut for Elektroniske Systemer
Fakultet	Det Teknisk Fakultet for IT og Design

MACHINE LEARNING OG AI I CYBERSIKKERHED

2025/2026

MODULETS INDHOLD, FORLØB OG PÆDAGOGIK

Kursusmodulet introducerer koncepter som statistisk interferens og data mining-algoritmer og beskriver, hvordan machine learning og kunstig intelligens anvender disse algoritmer til forbedring og løsning af problemstillinger inden for cybersikkerhed.

LÆRINGSMÅL

VIDEN

- Have viden og forståelse for grundlæggende begreber og metoder inden for superviseret og ikke-superviseret læring, herunder regression, klassifikation, klyngedannelse, repræsentationslæring og tæthedsestimering
- Have viden og forståelse for deep learning-algoritmer
- Have viden og forståelse for AI og forbindelsen mellem AI og maskinlæring
- Have viden om grundlæggende begreber som statistisk inferens, både model- og databaseret

FÆRDIGHEDER

- Have færdigheder til at træffe informerede valg vedrørende metoder til superviseret og ikkesuperviseret læring
- Have færdigheder i at evaluere valg af forskellige typer neurale netværk og vurdere deres kompleksitet og ydeevneafvejninger
- Have færdigheder i at anvende og evaluere metoder til statistisk inferens
- Have færdigheder i at anvende AI til at forbedre og løse cybersikkerhedsproblemer
- Kunne bruge værktøjer og ML-biblioteker som fx Python, scikit-learn og et deep learningbibliotek (f.eks. TensorFlow eller PyTorch) til at implementere maskinlæringsalgoritmer

KOMPETENCER

- Have kompetence til at anvende algoritmer til superviseret og ikke-superviseret læring på cybersikkerhedsudfordringer og evaluere resultaterne
- Have kompetence til at bruge forskellige typer neurale netværk og datamining-algoritmer til at håndtere forskellige cybersikkerhedsscenarier

UNDERVISNINGSFORM

Jf. beskrivelsen i §18

EKSAMEN

PRØVER

Prøvens navn	Machine Learning og AI i cybersikkerhed
Prøveform	Skriftlig eller mundtlig
ECTS	5
Tilladte hjælpemidler	Med visse hjælpemidler: Se eksamensspecifikation
Bedømmelsesform	7-trins-skala
Censur	Intern prøve
Vurderingskriterier	Vurderingskriterierne er angivet i Universitetets eksamensordning

FAKTA OM MODULET

Engelsk titel	Machine Learning and AI in Cyber Sercurity
Modulkode	ESNDCD5K4
Modultype	Kursus
Varighed	1 semester
Semester	Efterår
ECTS	5
Undervisningssprog	Dansk og engelsk
Tomplads	Ja
Undervisningssted	Campus København
Modulansvarlig	Tatiana Kozlova Madsen

ORGANISATION

Uddannelsesejer	Diplomingeniør i cybersikkerhed
Studienævn	Studienævn for Elektronik og IT
Institut	Institut for Elektroniske Systemer
Fakultet	Det Teknisk Fakultet for IT og Design

SIKKERHED I ORGANISATIONER

2025/2026

MODULETS INDHOLD, FORLØB OG PÆDAGOGIK

Dette kursus giver de studerende viden og færdigheder til at sikre virksomhedens data, aktiver og infrastruktur. Ved at udforske sikkerhedspolitikker, procedurer, incident response og nye trusler lærer deltagerne at udvikle og implementere effektive sikkerhedsstrategier. Dette kursus dækker også forståelse af menneskelige faktorer, der påvirker onlineadfærd og cybersikkerhed i organisationer.

LÆRINGSMÅL

VIDEN

- Have viden om sikkerhedspolitikker, procedurer og rammer til beskyttelse af organisatoriske data, aktiver og infrastruktur
- Forstå de menneskelige faktorer, der påvirker onlineadfærd, og deres indvirkning på cybersikkerhed i organisationer
- Have viden om de lovgivningsmæssige og overholdelsesmæssige krav, der påvirker organisatoriske cybersikkerhedspraksisser
- Have viden om strategier for hændelsesrespons

FÆRDIGHEDER

- Kunne identificere og håndtere risici i kombination med sikkerhedskrav
- Kunne designe, implementere og verificere virksomhedssikkerhedsløsninger
- Kunne analysere menneskelig adfærd for at identificere sårbarheder forårsaget af social engineering og foreslå effektive oplysnings- og træningsprogrammer

KOMPETENCER

- Have kompetence til at designe og administrere sikkerhedsstrategier, der stemmer overens med organisatoriske mål og overholdelseskrav
- Have kompetence til at diskutere menneskecentrerede cybersikkerhedsudfordringer

UNDERVISNINGSFORM

Jf. beskrivelsen i §18

EKSAMEN

PRØVER

Prøvens navn	Sikkerhed i organisationer
Prøveform	Skriftlig eller mundtlig
ECTS	5
Tilladte hjælpemidler	Med visse hjælpemidler: Se eksamensspecifikation
Bedømmelsesform	7-trins-skala
Censur	Intern prøve
Vurderingskriterier	Vurderingskriterierne er angivet i Universitetets eksamensordning

FAKTA OM MODULET

Engelsk titel	Security in Organisations
Modulkode	ESNDCD5K2
Modultype	Kursus
Varighed	1 semester
Semester	Efterår
ECTS	5
Undervisningssprog	Dansk og engelsk
Tomplads	Ja
Undervisningssted	Campus København
Modulansvarlig	Tatiana Kozlova Madsen

ORGANISATION

Uddannelsesejer	Diplomingeniør i cybersikkerhed
Studienævn	Studienævn for Elektronik og IT
Institut	Institut for Elektroniske Systemer
Fakultet	Det Teknisk Fakultet for IT og Design

MALWARE ANALYSE

2025/2026

MODULETS INDHOLD, FORLØB OG PÆDAGOGIK

Dette kursus dækker teknikker til at identificere, dissekere og eliminere skadelig software. Det inkluderer avancerede reverse engineering-teknikker og software security practices, der giver de studerende ekspertise i at analysere og beskytte systemer mod cybertrusler.

LÆRINGSMÅL

VIDEN

- Have viden om typer og funktionaliteter af ondsindet software, herunder vira, orme, trojanere, ransomware og spyware
- Forstå principperne og metodologierne for malwareanalyse, herunder statiske og dynamiske analyseteknikker
- Have viden om værktøjer og teknologier, der bruges til reverse engineering af malware, såsom disassemblere, debuggere og sandbox-miljøer
- Forstå, hvordan malware udnytter software-sårbarheder og sikkerhedssvagheder til at kompromittere systemer
- Have viden om bedste praksis og strategier til at beskytte systemer mod malware, herunder detektion, forebyggelse og fjernelsesteknikker

FÆRDIGHEDER

- Kunne udføre statisk analyse for at inspicere malwarekode og identificere dens karakteristika og adfærd
- Kunne bruge dynamiske analyseværktøjer til at udføre malware i kontrollerede miljøer og overvåge dens handlinger
- Kunne anvende reverse engineering-teknikker til at forstå komplekse malwarestrukturer og funktioner
- Kunne udvikle afbødningsstrategier og implementere værktøjer til at forsvare systemer mod malwaretrusler

KOMPETENCER

- Have kompetence til at analysere komplekse malwaresamples ved hjælp af avancerede værktøjer og metoder
- Have kompetence til at designe og implementere omfattende malwareforsvarsstrategier for organisatoriske netværk og systemer
- Have kompetence til at evaluere effektiviteten af forskellige teknikker til detektion og fjernelse af malware i forskellige scenarier
- Have kompetence til at kommunikere resultater fra malwareanalyse til interessenter, herunder både tekniske og ikke-tekniske målgrupper

UNDERVISNINGSFORM

Jf. beskrivelsen i §18

EKSAMEN

PRØVER

Prøvens navn	Malware analyse
Prøveform	Skriftlig eller mundtlig
ECTS	5
Tilladte hjælpemidler	Med visse hjælpemidler: Se eksamensspecifikation

Bedømmelsesform	7-trins-skala
Censur	Intern prøve
Vurderingskriterier	Vurderingskriterierne er angivet i Universitetets eksamensordning

FAKTA OM MODULET

Engelsk titel	Malware Analysis
Modulkode	ESNDCD7K2
Modultype	Kursus
Varighed	1 semester
Semester	Efterår
ECTS	5
Undervisningssprog	Dansk og engelsk
Tomplads	Ja
Undervisningssted	Campus København
Modulansvarlig	Tatiana Kozlova Madsen

ORGANISATION

Uddannelsesejer	Diplomingeniør i cybersikkerhed
Studienævn	Studienævn for Elektronik og IT
Institut	Institut for Elektroniske Systemer
Fakultet	Det Teknisk Fakultet for IT og Design

CYBERSIKKERHEDSLOVGIVNING

2025/2026

MODULETS INDHOLD, FORLØB OG PÆDAGOGIK

Dette kursus handler om global cybersikkerhedslovgivning med fokus på EU-direktiver og forordninger. Studerende lærer, hvordan disse regler påvirker organisationer og vigtigheden af compliance for opretholdelse af sikre digitale miljøer

LÆRINGSMÅL

VIDEN

- Have viden om globale cybersikkerhedslove, herunder EU-direktiver og -forordninger (såsom GDPR, NIS-direktivet) samt fremtrædende lovgivning fra regioner som USA og Asien
- Forstå de juridiske principper og rammer, der regulerer cybersikkerhed på tværs af forskellige jurisdiktioner, herunder databeskyttelseslove, krav til hændelsesrespons og nationale cybersikkerhedsstrategier
- Have viden om internationale aftalers og traktaters rolle i styring af cybersikkerhed
- Forstå vigtigheden af overholdelse af cybersikkerhedsregler for organisationer, herunder de juridiske konsekvenser af sikkerhedsbrud, databeskyttelse og beskyttelse af intellektuelle rettigheder
- Have viden om håndhævelsesmekanismer, sanktioner og juridiske konsekvenser af manglende overholdelse af cybersikkerhedslove i forskellige regioner

FÆRDIGHEDER

- Kunne fortolke og analysere globale cybersikkerhedslove og -regler og forstå, hvordan de gælder for specifikke organisatoriske kontekster
- Kunne vurdere en organisations overholdelse af internationale, regionale og nationale cybersikkerhedsregler samt identificere risici og mangler
- Kunne udføre revisioner og vurderinger for at evaluere cybersikkerhedspraksis og overholdelse af love som GDPR

KOMPETENCER

- Have kompetence til at vurdere påvirkningen af global cybersikkerhedslovgivning på organisatoriske strategier, især med hensyn til databeskyttelse, brudnotifikation og risikostyring
- Have kompetence til at reflektere over de bredere implikationer af global cybersikkerhedslovgivning og dens rolle i at forme fremtidige politikker, internationalt samarbejde og virksomheders ansvar inden for cybersikkerhed

UNDERVISNINGSFORM

Jf. beskrivelsen i §18

EKSAMEN

PRØVER

Prøvens navn	Cybersikkerhedslovgivning
Prøveform	Skriftlig eller mundtlig
ECTS	5
Tilladte hjælpemidler	Med visse hjælpemidler: Se eksamensspecifikation
Bedømmelsesform	7-trins-skala
Censur	Intern prøve

Vurderingskriterier	Vurderingskriterierne er angivet i Universitetets eksamensordning

FAKTA OM MODULET

Engelsk titel	Cyber Security Legislation
Modulkode	ESNDCD7K3
Modultype	Kursus
Varighed	1 semester
Semester	Efterår
ECTS	5
Undervisningssprog	Dansk og engelsk
Tomplads	Ja
Undervisningssted	Campus København
Modulansvarlig	Tatiana Kozlova Madsen

ORGANISATION

Uddannelsesejer	Diplomingeniør i cybersikkerhed
Studienævn	Studienævn for Elektronik og IT
Institut	Institut for Elektroniske Systemer
Fakultet	Det Teknisk Fakultet for IT og Design