



Fakulteten för hälsa, natur- och teknikvetenskap  
Datavetenskap

# Kursplan

## Säkerhet och integritet på internet

**Kurskod:** DVAD23  
**Kursens benämning:** Säkerhet och integritet på internet  
*Internet Security and Privacy*  
**Högskolepoäng:** 7.5  
**Utbildningsnivå:** Avancerad nivå  
**Successiv fördjupning:** Avancerad nivå, har endast kurs/er på grundnivå som förkunskapskrav (A1N)

**Huvudområde:**  
DVA (Datavetenskap)

### Beslut om fastställande

Kursplanen är fastställd av Fakulteten för hälsa, natur- och teknikvetenskap 2022-02-24 och gäller från höstterminen 2022 vid Karlstads universitet.

### Behörighetskrav

7.5 hp vardera inom säkerhet, datakommunikation, operativsystem och programmering. Gymnasiets Engelska kurs 6. Motsvarandebedömning kan göras.

### Lärandemål

Efter avslutad kurs ska studenten kunna:

1. förklara grundläggande kryptografiska primitiver som används i vanligt förekommande kommunikationsprotokoll på internet,
2. kategorisera kommunikationsprotokoll baserat på den högsta möjliga säkerhetsnivå som kan uppnås utifrån använda kryptografiska primitiver och gällande rekommendationer,
3. tillämpa moderna kryptografiska programbibliotek på ett korrekt och säkert sätt,
4. tillämpa moderna teknologier för säker och integritetsskyddande kommunikation,
5. jämföra olika teknologier för säker och integritetsskyddande kommunikation utifrån användares olika hotbilder och

6. beskriva etiska aspekter och samhälliga intressen som driver utvecklingen samt användandet av säkerhets- och integritetsskyddande teknologier på internet.

### **Innehåll**

Kursen fokuserar på hur kommunikation på internet görs säker och integritetsskyddande med hjälp av kryptografi och god ingenjörskonst.

Den första halvan av kursen består av tillämpad kryptografi med fokus på kryptografiska primitiver, säkerhetsdefinitioner och gällande rekommendationer kring val av primitiver och parametrar. Målet är att bygga upp en verktygslåda med förståelse kring primitiver, deras styrkor och begränsningar, samt förståelse för hur dessa används i praktiken i mjukvara.

Den andra halvan av kursen tillämpar verktygslådan från den första halvan. Kommunikationsprotokoll och andra teknologier för säker och integritetsskyddande kommunikation som är vanligt förekommande på internet studeras i detalj. Fokus ligger på teknikens konstruktion för att uppnå olika nivåer och typer av skydd utifrån olika hotbilder. Exempel är Transport Layer Security, WireGuard och anonymitetsnätverket Tor.

Under kursens gång genomförs laborationer och inlämningsuppgifter med muntlig och skriftlig redovisning. Kursen avslutas med muntlig redovisning av ett mindre projekt där studenterna i mindre grupp får analysera ett protokoll eller en teknik på egen hand. Analysen består av tekniska, etiska och samhälliga aspekter kring teknikens användningsområde, målgrupp, utvecklare och andra drivkrafter.

### **Kurslitteratur och övriga läromedel**

Se separat dokument.

### **Examination**

Examination sker i form av:

- individuell skriftlig tentamen,
- muntlig samt skriftlig redovisning av inlämningsuppgifter både individuellt och i grupp,
- laborationsredovisningar både individuellt och i grupp.

Om studenten har ett beslut från Karlstads universitet om riktat pedagogiskt stöd på grund av dokumenterad funktionsnedsättning har examinator rätt att ge studenten en anpassad examination eller att låta studenten genomföra examinationen på ett alternativt sätt.

### **Betyg**

Kursen bedöms enligt betygsskalan Med beröm godkänd (5), Icke utan beröm godkänd (4), Godkänd (3) eller Underkänd (U).

### **Kvalitetsuppföljning**

Under och efter kursen sker en uppföljning av måluppfyllelse och förutsättningar för lärande i kursen. Dess främsta syfte är att bidra till förbättringar. Studenternas erfarenheter och synpunkter är ett av underlagen för granskningen, och inhämtas i enlighet med gällande regelverk. Studenterna informeras om resultaten och eventuella beslut om åtgärder.

### **Kursbevis**

Kursbevis utfärdas på begäran.

### **Övrigt**

Gällande regler för utbildning på grundnivå och avancerad nivå vid Karlstads universitet reglerar studenters och anställds skyldigheter och rättigheter.