# Forside H2025

**UNIVERSITETET I OSLO**

**Det matematisk-naturvitenskapelige fakultet**

**Skriftlig eksamen i IN1020**
**2025 HØST**

**Varighet: 8. desember kl. 15:00-19:00**
**Tillatte hjelpemidler: Ingen hjelpemidler er tillatt.**

**En kalkulator er tilgjengelig i Inspera (se nederst på siden).**
**Det er viktig at du leser hele forsiden før du begynner å besvare eksamensoppgavene.**

**Om du ønsker å zoome i oppgavesettet, hold ctrl nede og trykk + eller - på numerisk tastatur.**

Faglærere vil gå en runde fra ca kl. 16:00.

## Oppgavesettet

Eksamenssettet består av 4 seksjoner, hvor de er poenggivende med 25 poeng hver - totalt 100 poeng.

Seksjon 1 er Digital representasjon og assemblerkode.
Seksjon 2 er Maskinvare og arkitektur.
Seksjon 3 er Datasikkerhet.
Seksjon 4 er Datanettverk.

Merk at hver seksjonen må være bestått for at eksamen skal kunne bestås.

## Oppgavene

Noen oppgaver kan ha flere riktige svar, mens andre bare har ett. Alle vil ha minst ett korrekt svar. Man får poeng for å velge et korrekt alternativ og man kan miste poeng ved å velge et galt, men man vil aldri få mindre enn 0 poeng på en oppgave.

## Tillatte hjelpemidler

Ingen hjelpemidler er tillatt.

## Tilgjengelige ressurser i Inspera

- Enkel kalkulator
- Ascii-tabellen

# IN1020 H25 Seksjon Digital representasjon og assemblerprogrammering

**Du er nå i seksjon 1: Digital representasjon og assemblerprogrammering**

Oppgave nr 1.1 - 1.8 er en del av seksjon 1.

## 1.1 IN1020 H25 bit-representasjon

En byte inneholder følgende bit:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 |

Hvilke(n) verdi(er) i 10-tallssystemet kan representeres av disse bit-ene?

**Velg ett eller flere alternativer:**

- [ ] -42
- [ ] 99
- [ ] -85 ✔
- [ ] 171 ✔

Maks poeng: 2

## 1.2 IN1020 H25 Tallsystemer og 10

Velg det som er sant om tallet representert som **10** i forskjellige tallsystem - flere valg kan være riktig.

**Velg ett eller flere alternativer:**

- [ ] $10_2 = 2_{10}$ ✔
- [ ] $10_{15} = 15_{10}$ ✔
- [ ] $10_3 = 3_{10}$ ✔
- [ ] $10_{23} = 23_{10}$ ✔

Maks poeng: 2.5

## 1.3 IN1020 H25 Tallsystemer representasjon

Du får oppgitt en del tall, men dessverre har notasjonen som skal fortelle oss hvilket tallsystem de er skrevet i, blitt borte. Hva slags tallsystemer kan disse verdiene være skrevet i? Det kan være flere riktige alternativer per bolk.

**0f0cdb0d**

- [ ] Heksadesimale tall ✔
- [ ] Titallsystemet
- [ ] Binære tall
- [ ] Base 64 (64-tallsystemet) ✔

**MTIz**

- [ ] Titallsystemet
- [ ] Base 64 (64-tallsystemet) ✔
- [ ] Heksadesimale tall
- [ ] Binære tall

**10111010**

- [ ] Heksadesimale tall ✔
- [ ] Binære tall ✔
- [ ] Base 64 (64-tallsystemet) ✔
- [ ] Titallsystemet ✔

---

Maks poeng: 3.5

## 1.4 IN1020 H25 Enkoding

Kryss av for sanne utsagn i oppgaven under. Det kan være mer enn ett riktig svar.

**Velg ett eller flere alternativer:**

- [ ] Vi bruker en enkoding, som UTF-8 eller ASCII, fordi vi ønsker å komprimere teksten
- [ ] UTF-8 er en enkoding som lar oss representere alle tegn i Unicode ved bruk av mellom 1 og 4 byte per tegn ✔
- [ ] Unicode har plass til alle tegn i verden ✔
- [ ] ASCII er alltid bedre enn UTF-8 fordi ASCII bruker mindre plass
- [ ] Det er vanlig å bruke kompresjon med tap for å spare plass når man lagrer tekst

---

Maks poeng: 2

## 1.5 IN1020 H25 Lyd og bilde

Velg sanne utsagn om representasjon av lyd og bilde:

**Velg ett eller flere alternativer:**

- [ ] Vektorgrafikk egner seg godt for lagring av fotografier
- [ ] Kompresjon med tap er ofte brukt for å spare plass når man overfører eller lagrer l ✔ er
- [ ] Kompresjon med tap er ofte brukt for å spare plass når man overfører eller lagrer l ✔
- [ ] Bitdybden på et lydopptak angis i Hz
- [ ] Hz angir antall målinger per sekund når vi konverterer fra analog til digital lyd ✔
- [ ] Bildefiler lagres ofte med UTF-8-enkoding

---

Maks poeng: 3

## 1.6 IN1020 H25 LMC instruksjonsplassering

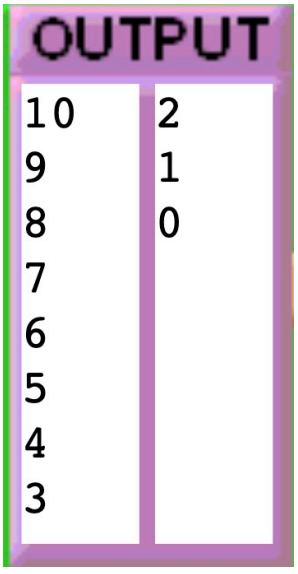
Dette programmet skal telle ned fra 10 til 0, og skrive ut alle tallene, som vist på bildet under. Men, det mangler en instruksjon, og dens argument. Fyll de ledige lukene ved å dra inn fra alternativene listet opp øverst.

Hjelp

BRP | BRZ | LDA | LOOP | v10 | STA | v1 | START

```
START   LDA  v10
LOOP    OUT
        SUB  v1
        [BRP ✔]  [LOO ✔]
        HLT

v1      DAT  1
v10     DAT  10
```




Maks poeng: 4

## 1.7 IN1020 H25 LMC Maskinkode

Du får oppgitt følgende LMC-program som maskinkode.

```
507
922
508
922
509
922
000
073
102
105
```

Du kan anta at programmet er lagret fra minneposisjon 0 i minnet til LMC.

Hva gjør dette programmet?

Du kan støtte deg på følgende mapping mellom maskinkode og assemblerkode:
0xx: HLT
1xx: ADD
2xx: SUB
3xx: STA
5xx: LDA
6xx: BRA
7xx: BRZ
8xx: BRP
922: OTC

**Velg ett eller flere alternativer:**

- [ ] Det er kodet feil, og vil ikke kunne kjøre
- [ ] Det teller opp 7, 8, 9 og skriver ut dette på skjermen
- [ ] Det skriver ut følgende tekst: Hei
- [ ] Det skriver ut følgende tekst: Ifi ✔
- [ ] Det legger sammen tre tall, og skriver ut summen av disse

---

Maks poeng: 2

## 1.8 IN1020 H25 LMC feil i programmet

Dette programmet har vi sett på forelesning, og det skal skrive ut teksten "Velkommen!". Imidlertid har det sneket seg inn en liten feil, som gjør at programmet ikke fungerer helt som det skal. Velg riktig(e) utsagn under som beskriver noe sant om programmet.

```
Skriv   LDA txt
        BRZ Ferdig
        OTC
        LDA Skriv
        ADD 1
        STA Skriv
        BRA Skriv
Ferdig  HLT
v1      DAT 1 // Konstant 1
txt     DAT 86 // 'V'
        DAT 101 // 'e'
        DAT 108 // 'l'
        DAT 107 // 'k'
        DAT 111 // 'o'
        DAT 109 // 'm'
        DAT 109 // 'm'
        DAT 101 // 'e'
        DAT 110 // 'n'
        DAT 33 // '!'
        DAT 0 // Slutt
```

**Velg ett eller flere alternativer:**

- [ ] Instruksjonen "STA Skriv" er feil siden den overskriver en eksisterende instruksjon i programmet
- [ ] Programmet skriver ut "Velkommen", men klarer ikke skrive ut utropstegnet til slutt
- [ ] Programmet vil få en aritmetisk overflyt, og forsøke å utføre en instruksjon som har en negativ tallverdi i minnet ✔
- [ ] Programmet skriver ut "V" før det stopper ✔
- [ ] Instruksjonen "ADD 1" er feil siden den leser instruksjon fra minnecelle 1 i stedet for konstantverdien 1 ✔

---

Maks poeng: 6

# H25 - Seksjon Maskinvare

**Du er nå i seksjon - Maskinvare og arkitektur.**

Oppgave nr 2.1- 2.10 er en del av seksjon 2.

Noen av oppgavene er slik at du skal angi din konfidens på svarene.

**Slik svarer du på oppgaver med konfidensvurdering:**

- Les hvert spørsmål nøye før du svarer
- Du skal fordele totalt **100 % konfidens** på de ulike svaralternativene
- Hvis du er helt sikker på ett svar: gi det 100 % og resten 0 %
- Hvis du er usikker: fordel prosentene på flere alternativer basert på hvor sannsynlig du mener hvert alternativ er riktig
- Eksempel: Hvis du tror B er mest sannsynlig riktig, men er litt usikker, kan du for eksempel fordele slik: 75 % på den ene og 25 % på andre, og resten på 0 %.
- **Viktig:** Summen av alle prosentene må alltid bli nøyaktig 100 %
- **Strategi:** Vær ærlig om din faktiske usikkerhet – poengsystemet belønner realistisk selvvurdering. Hvis du gjetter blindt, risikerer du å tape poeng.

## 2.1 H25 - CBA - Cache-miss

Hva betyr det når CPU-en opplever en cache-miss?

**Fordel din konfidens på de ulike svaralternativene**

| | 0 % | 25 % | 50 % | 75 % | 100 % |
|---|---|---|---|---|---|
| Data finnes ikke i cache og må hentes fra et høyere minnehierarkinivå | ○ | ○ | ○ | ○ | ○ ✔ |
| Data finnes i cache og kan leses raskt | ○ ✔ | ○ | ○ | ○ | ○ |
| Cache-minnet er fullt og må tømmes | ○ ✔ | ○ | ○ | ○ | ○ |
| To prosessorkjerner prøver å aksessere samme cache-linje samtidig | ○ ✔ | ○ | ○ | ○ | ○ |
| Cache-koherens protokollen feiler | ○ ✔ | ○ | ○ | ○ | ○ |

Maks poeng: 2

## 2.2 H25 - CBA - Adder

Hvorfor kalles en halv-adder for "halv"?

**Fordel din konfidens på de ulike svaralternativene**

| | 0 % | 25 % | 50 % | 75 % | 100 % |
|---|---|---|---|---|---|
| Den mangler "mente inn" (Carry in) som inngang | ○ | ○ | ○ | ○ | ○ ✔ |
| Den gir bare ut halve resultatet | ○ ✔ | ○ | ○ | ○ | ○ |
| Den kan bare addere halve tall | ○ ✔ | ○ | ○ | ○ | ○ |
| Den bruker bare halvparten så mange logiske porter | ○ ✔ | ○ | ○ | ○ | ○ |
| Den kan bare håndtere 4-bits tall | ○ ✔ | ○ | ○ | ○ | ○ |

Maks poeng: 2

## 2.3 H25 - CBA - ALU

Hva bestemmer styresignalet i en ALU?

**Fordel din konfidens på de ulike svaralternativene**

| | 0 % | 25 % | 50 % | 75 % | 100 % |
|---|---|---|---|---|---|
| Hvilken operasjon ALU-en skal utføre | ○ | ○ | ○ | ○ | ○ ✔ |
| Hvilken adresse i minnet som skal brukes | ○ ✔ | ○ | ○ | ○ | ○ |
| Hvor raskt operasjonen skal utføres | ○ ✔ | ○ | ○ | ○ | ○ |
| Hvilken type beregning som skal gjøres | ○ ✔ | ○ | ○ | ○ | ○ |
| Hvor mange bits ALU-en skal behandle | ○ ✔ | ○ | ○ | ○ | ○ |

Maks poeng: 2

## 2.4 H25 - CBA - PC

Hva er hovedfunksjonen til Program Counter (PC) i en CPU?

**Fordel din konfidens på de ulike svaralternativene**

| | 0 % | 25 % | 50 % | 75 % | 100 % |
|---|---|---|---|---|---|
| Lagrer resultatet av beregninger | ✔ | | | | |
| Teller antall instruksjoner som er utført | ✔ | | | | |
| Holder adressen til gjeldende instruksjon | ✔ | | | | |
| Styrer hastigheten på prosessoren | ✔ | | | | |
| Holder adressen til neste instruksjon som skal hentes fra minnet | | | | | ✔ |

Maks poeng: 2

## 2.5 H25 - CBA - Universell porter

Hvorfor kalles NAND og NOR for "universelle porter"?

**Fordel din konfidens på de ulike svaralternativene**

| | 0 % | 25 % | 50 % | 75 % | 100 % |
|---|---|---|---|---|---|
| Alle andre logiske porter kan bygges ved å bruke bare NAND eller bare NOR | ○ | ○ | ○ | ○ | ○ ✔ |
| De er de eneste portene som kan lagre data | ○ ✔ | ○ | ○ | ○ | ○ |
| De kan operere på alle datatyper | ○ ✔ | ○ | ○ | ○ | ○ |
| De fungerer med både AC og DC strøm | ○ ✔ | ○ | ○ | ○ | ○ |
| De brukes overalt i moderne datamaskiner | ○ ✔ | ○ | ○ | ○ | ○ |

Maks poeng: 2

## 2.6 H25 - CBA - Pipeline ytelse

Hva setter begrensningen på maksimal hastighet i en pipeline?

**Fordel din konfidens på de ulike svaralternativene**

| | 0 % | 25 % | 50 % | 75 % | 100 % |
|---|---|---|---|---|---|
| Den raskeste komponenten i pipelinen | ✔ | | | | |
| Størrelsen på cache-minnet | ✔ | | | | |
| Antall instruksjoner som utføres samtidig | ✔ | | | | |
| Den tregeste komponenten/fasen i pipelinen | | | | | ✔ |
| Det totale antallet pipeline-trinn | ✔ | | | | |

Maks poeng: 2

## 2.7 H25 - CBA - Seriell Adder

Hva er hovedproblemet med en Ripple Carry Adder (seriell adder) når antall bits øker?

**Fordel din konfidens på de ulike svaralternativene**

| | 0 % | 25 % | 50 % | 75 % | 100 % |
|---|---|---|---|---|---|
| Den kan bare addere tall av samme størrelse | ✔ | | | | |
| Mente-biten må propagere gjennom alle full-addere | | | | | ✔ |
| Den bruker for mye strøm | ✔ | | | | |
| Den kan ikke håndtere negative tall | ✔ | | | | |
| Den krever for mange transistorer | ✔ | | | | |

Maks poeng: 2

## 2.8 H25 - Minne/Cache

Ta utgangspunkt i at det gjenstår 100 instruksjoner å gjennomføre, basert på historikken kan vi forvente at det vil bli 60 % L1-cache-hit, 20 % L1-cache-miss, 10 % L2-cache-miss, 10 % RAM-miss.

**Hvor mange klokkesykler vil det gå for å gjennomføre de 100 instruksjonene?**

Minnehierarkien er som følger:

3 nivåer med cache, hvor hvert nivå gir total forsinkelse på 10 klokkesykler for hver instruksjon.

RAM gir en total forsinkelse på 1000 klokkesykler for hver instruksjon.

De instruksjonene som ikke trenger minneaksess bruker 1 klokkesykel for hver instruksjon.

**Velg ett alternativ:**

- 400
- 3060
- 10400
- 10360
- 10460 ✔

---

Maks poeng: 3

## 2.9 H25 - Instruksjonsflyt

Mellom hver pipeline-fase lagres data i Velg alternativ (RAM, cache, register) , og

Velg alternativ (IR, PC, ALU, RAM) holder styr på neste instruksjon.

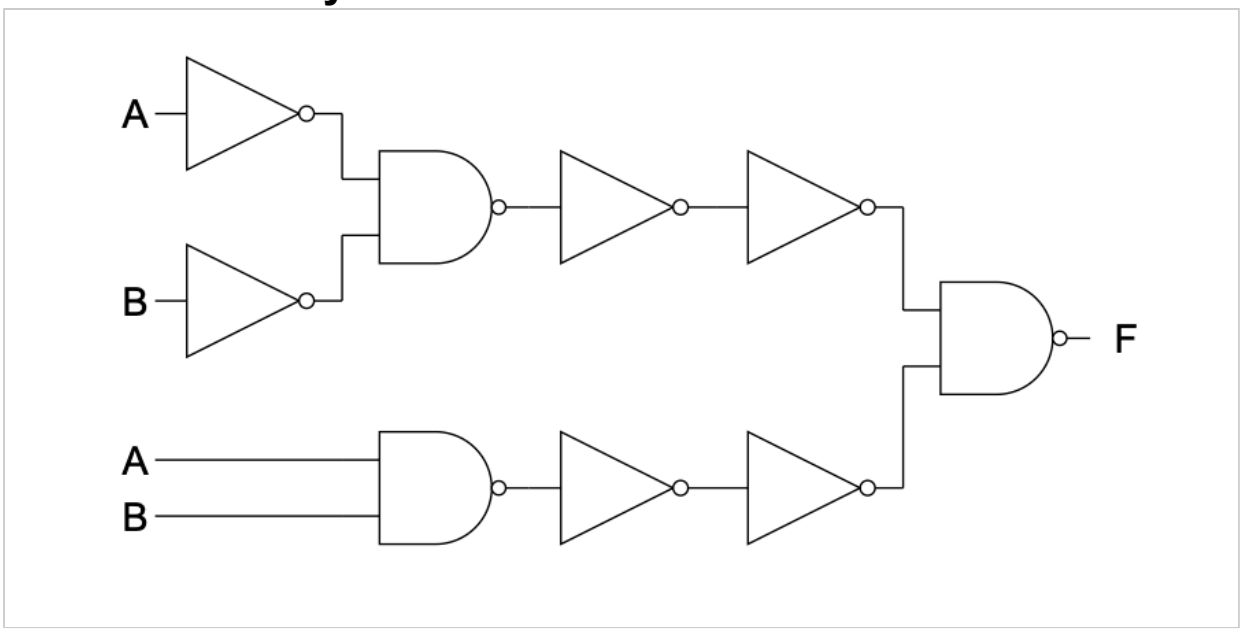
I Velg alternativ (EX, DE, IF) -fasen dekoder Control Unit instruksjonen og bestemmer hvilken operasjon som skal utføres.

En data hazard oppstår når en instruksjon trenger Velg alternativ (en adresse, et resultat, en instruksjon) fra en tidligere instruksjon. For å løse dette kan prosessoren Velg alternativ (stoppe, ignorere, slette, hoppe) pipelinen.

---

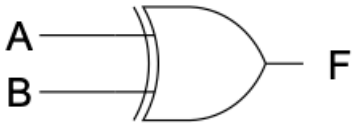
Maks poeng: 3

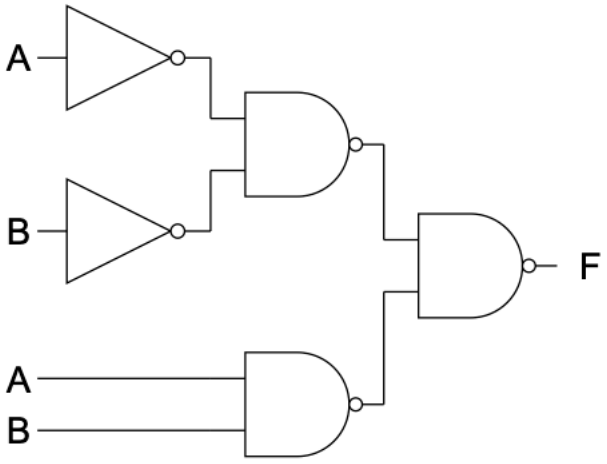
## 2.10 H25 - Kretsanalyse

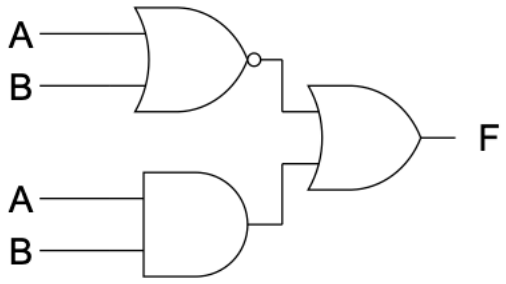


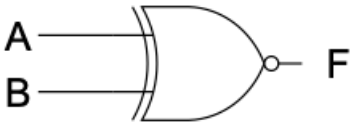
**Hvilket krets realiserer denne funksjonen F med færrest antall porter?**






Maks poeng: 5

# Seksjon 3

**Du er nå i seksjon 3 - datasikkerhet.**

Oppgave nr 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7 og 3.8 er en del av seksjon 3.

## 3.1 Sikkerhetsmål

I IN1020 definerer vi en rekke sikkerhetsmål, som er egenskaper man vil ivareta i de aller fleste IT-systemer. Plasser riktig sikkerhetsmål til riktig definisjon i teksten nedenfor.

Hjelp

| | | |
|---|---|---|
| Integritet | Tilgjengelighet | Personopplysningsvern |
| Uavviselighet | Autentisitet | Konfidensialitet |

- Tilgjengelighet ✔ er egenskapen at data og tjenester er anvendbare ved forespørsel fra en autorisert entitet.
- Konfidensialitet ✔ er egenskapen at data ikke blir gjort tilgjengelig for uautoriserte entiteter.
- Autentisitet ✔ er tillitt til at en entitet er ekte og som påstått.
- Integritet ✔ er egenskapen at data ikke er blitt endre eller slettet på en uautorisert måte.
- Uavviselighet ✔ er at en entitet ikke kan benekte å ha utført en handling.
- Personopplysningsve ✔ er beskyttelse av personopplysninger mot ulovlig innsamling og behandling.

Maks poeng: 2

## 3.2 Brudd på sikkerhetsmål

Angi hvilket sikkerhetsmål som <u>først og fremst</u> brytes som resultat av hvert av følgende angrep:

**Finn de som passer sammen:**

| | Konfidensialitet | Integritet | Tilgjengelighet | Autentisitet |
|---|---|---|---|---|
| Endring av nettverkstrafikk | ○ | ○ ✔ | ○ | ○ |
| Tjenestenektangrep | ○ | ○ | ○ ✔ | ○ |
| Avlytting nettverkstrafikk | ○ ✔ | ○ | ○ | ○ |
| Løsepengevirus | ○ | ○ | ○ ✔ | ○ |
| Spionprogramvare | ○ ✔ | ○ | ○ | ○ |
| Falsk digital ID | ○ | ○ | ○ | ○ ✔ |

Maks poeng: 3

## 3.3 Begrepsforståelse

Plasser begrepene under sammen med riktig tekst. Merk: Noen av begrepene vil være til overs.

Hjelp

| | | |
|---|---|---|
| Sårbarhet | Hash-funksjoner | Digitale sertifikater |
| Phishing | SQL-injisering | Formålsbegrensning |
| Dataminimering | Angrepsvektor | Autentiseringsfaktor |
| Symmetrisk nøkkel | Autentisering | Cross site scripting (XSS) |
| Autorisering | PKI | |

Formålsbegrensning ✔ som prinsipp i GDPR legger føringer for hva innsamlede personopplysninger kan brukes til.

Autentisering ✔ er mekanismen for å bekrefte en hevdet identitet.

Phishing ✔ er navnet på en framgangsmåte for å lure fra deg hemmelige opplysninger.

Hash-funksjoner ✔ brukes ved behov for sjekk av en meldings integritet.

Autentiseringsfaktor ✔ er et bevismateriale for å bekrefte identitet.

SQL-injisering ✔ kan brukes til å få tak i data direkte fra en database.

PKI ✔ er et rammeverk for å sikre ekteheten av offentlige nøkler.

Angrepsvektor ✔ er et annet ord for metodene som brukes for å angripe en datamaskin.

---

Maks poeng: 4

## 3.4 Tilgangskontroll

**a)** Hva er de to grunnleggende elementene i et system for tilgangskontroll?
**Velg ett alternativ**

- ○ Multifaktor-autentisering og biometri
- ○ Autorisering og brukeridentitet
- ○ Passord og privat nøkkel
- ○ Autentisering og autorisasjon ✔

**b)** Hvilken av følgende er korrekt definisjon av tilgangskontroll?
**Velg ett alternativ**

- ○ Tilgangskontroll er å håndheve definerte tilgangsrettigheter i et datasystem. ✔
- ○ Tilgangskontroll er å spesifisere tilgangsrettigheter til dataressurser.
- ○ Tilgangskontroll er å definere et regelsett for passordhåndtering.
- ○ Tilgangskontroll er å lage regler for identifisering av brukere.

**c)** Tilgangskontroll er først og fremst et [Velg alternativ] (forebyggende, korrigerende, detekterende) sikkerhetstiltak.

**d)** Feil i et systemet som håndterer tilgangskontroll kan føre til brudd på hvilke sikkerhetsmål?
**Velg ett eller flere alternativer**

- ☐ Integritet ✔
- ☐ Tilgjengelighet ✔
- ☐ Konfidensialitet ✔

Maks poeng: 3

## 3.5 Anvendelse av kryptografi 1

**a)** Alice og Bob skal utveksle hemmelige meldinger, og bestemmer seg for å bruke kryptering med én hemmelig delt nøkkel de begge - men ingen andre - kjenner.

Alice krypterer en melding med den hemmelige nøkkelen, og sender kryptert melding til Bob.

**Hvilke(t) av følgende utsagn stemmer?**

- [ ] Bob forsøker å overbevise Eve (en tredjepart) om at meldingen kommer fra Alice. Eve kan være sikker på at Alice er opphavet.
- [ ] Alice kan være sikker på at meldingen kun kan leses av Bob. ✔
- [ ] Bob kan være sikker på at meldingen kommer fra Alice. ✔

**Denne måten å sende meldinger på sikrer konfidensialitet for meldingen.**

- ○ Usant
- ○ Sant ✔

**b)** Alice og Bob syns det er vanskelig å utveksle en delt hemmelig nøkkel trygt, og tar i bruk offentlig nøkkel-kryptering isteden. Alice oppretter et nøkkelpar der hun holder den private nøkkelen hemmelig mens den tilhørende offentlige nøkkelen deles med blant annet Bob og Eve.

Alice krypterer en melding med sin private nøkkel, og sender den krypterte meldingen til Bob som dekrypterer med den tilhørende offentlige nøkkelen.

**Hvilke(t) av følgende utsagn stemmer?**

- [ ] Bob forsøker å overbevise Eve (en tredjepart) om at meldingen kommer fra Alice. Eve kan være sikker på at Alice er opphavet. ✔
- [ ] Alice kan være sikker på at meldingen kun kan leses av Bob.
- [ ] Bob kan være sikker på at meldingen kommer fra Alice. ✔

**Denne måten å sende meldinger på sikrer konfidensialitet for meldingen.**

- ○ Sant
- ○ Usant ✔

---

Maks poeng: 3

## 3.6 Anvendelse av kryptografi 2

Alice og Bob benytter asymmetrisk kryptering for meldingsutveksling og signering, og har fått utdelt hvert sitt nøkkelpar bestående av en privat og en offentlig nøkkel.

**a)** For å signere et dokument D må Alice bruke Velg alternativ (Bob sin private, Alice sin offentlige, Alice sin private, Bob sin offentlige) nøkkel. For å verifisere at det er Alice som har signert dokument D må Bob bruke Velg alternativ (Alice sin private, Alice sin offentlige, Bob sin private, Bob sin offentlige) nøkkel.

**b)** For å kryptere og sende en hemmelig (konfidensiell) melding M til Bob må Alice bruke Velg alternativ (Bob sin private, Bob sin offentlige, Alice sin offentlige, Alice sin private) nøkkel. For å dekryptere og lese meldingen M må Bob bruke Velg alternativ (Alice sin private, Bob sin offentlige, Bob sin private, Alice sin offentlige) nøkkel.

---

Maks poeng: 2

## 3.7 Personopplysningsvern

En arbeidsgiver ønsker å registrere en del tilleggsopplysninger om sine ansatte. De vil registrere følgende data:

- Informasjon om en ansatts barn.
- Kontaktinformasjon til partner/ektefelle.
- Hvilken fagforening den ansatte er medlem i.
- Opplysninger om helse som kan påvirke den ansatte negativt i arbeidshverdagen.
- Religiøs overbevisning for å kunne feire ulike høytidsdager.

**a)** Har arbeidsgiveren uten videre lov til å registrere disse opplysningene om en ansatt?
**Velg ett alternativ**

- [ ] Ja
- [ ] Nei ✔

**b)** Lov om behandling av personopplysninger definerer det som kalles *særlige kategorier av personopplysninger*. Hvilke av følgende er definert i denne kategorien?
**Velg ett eller flere alternativer**

- [ ] Etnisk opprinnelse ✔
- [ ] Religiøs overbevisning ✔
- [ ] Eksamensresultat
- [ ] Epost-adresse
- [ ] Personnummer
- [ ] Politisk oppfatning ✔

**c)** Hvilke krav må oppfylles for å lovlig kunne registrere og behandle personopplysninger om fysiske personer?
**Velg ett eller flere alternativer**

- [ ] Krav om at informasjonssikkerhet ivaretas i behandlingen. ✔
- [ ] Ingen spesielle krav så lenge den registrerte har samtykket til behandlingen.
- [ ] Krav om at opplysninger arkiveres i fall det dukker opp nye behandlingsbehov.
- [ ] Krav om at det ikke registreres flere personopplysningen enn nødvendig for behar ✔ igen.
- [ ] Krav til at personopplysninger som hovedregel ikke benyttes til andre formål enn d[illegible]e er samlet inn for. ✔

Maks poeng: 4

## 3.8 Trusselmodellering og risiko

Du er konsulent i et IT-selskap som skal bidra til trusselvurdering av informasjonssikkerhet hos en bedrift. Bedriften behandler data om sine kunder, som er både privatpersoner og andre bedrifter. I tillegg lagrer de en rekke data/opplysninger om sin egen virksomhet, som de ønsker å holde hemmelig.

**a)** Selskapet er svært opptatt av å unngå datalekkasjer. Hva kan være trusler mot *konfidensialitet* til data firmaet behandler?

**Velg ett eller flere alternativer**

- [ ] Passordlekkasje. ✔
- [ ] Angrep med løsepengevirus.
- [ ] Sårbarhet i programvare via leverandørkjeden. ✔
- [ ] Phishingangrep mot ansatte. ✔
- [ ] Tjenestenektangrep fra utenforstående.

**b)** Hvilke sikkerhetstiltak vil du anbefale for å minske sannsynligheten for og konsekvensen av brudd på *konfidensialitet*?

**Velg ett eller flere alternativer**

- [ ] Sørge for at alle ansatte har tilgang til alle bedriftshemmeligheter.
- [ ] Innføre tofaktorautentisering for ansattes innlogging. ✔
- [ ] Bruke sjekksumalgoritmer for alle data som lagres.
- [ ] Gjennomføre regelmessige sikkerhetsøvelser. ✔
- [ ] Kryptere alle data som lagres. ✔

**c)** Hva er direkte trusler mot *tilgjengelighet* til data firmaet behandler og IT-tjenester de tilbyr?

**Velg ett eller flere alternativer**

- [ ] Spionprogramvare på en ansatts datamaskin.
- [ ] Avlytting av nettverkstrafikk internt i bedriften.
- [ ] Avlytting av nettverkstrafikk mellom kunde og bedrift.
- [ ] Tjenestenektangrep fra utenforstående. ✔
- [ ] Angrep med løsepengevirus. ✔

**d)** Hvilke sikkerhetstiltak vil du anbefale for å minske konsekvensen av brudd på *tilgjengelighet*?
**Velg ett eller flere alternativer**

- [ ] Gjennomføre regelmessige sikkerhetsøvelser. ✔
- [ ] Kryptere alle data som lagres.
- [ ] Ha gode rutiner for sikkerhetskopiering av lagrede data. ✔
- [ ] Innføre tofaktorautentisering for ansattes innlogging.
- [ ] Bruke sjekksumalgoritmer for alle data som lagres.

---

Maks poeng: 4

# Seksjon 4

**Du er nå i seksjon 4 - Operativsystemer og Datakommunikasjon.**

Oppgave nr 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7 og 4.8 er en del av seksjon 4.

## 4.1 Operativsystemer

**Hvilke påstander om operativsystemer er sanne og hvilke er usanne?**

| | Sann | Usann |
|---|---|---|
| Operativsystemet sørger for at flere brukere kan dele en datamaskin | ✔ | |
| Det er operativsystemet sin oppgave å fordele resurser på programmene som skal kjøre. | ✔ | |
| Mobiltelefoner kjører kun ett program om gangen, og trenger derfor ikke et operativsystem. | | ✔ |
| Et operativsystem tilbyr APIer for at programmer skal kunne bruke tjenester som lagring og nettverk. | ✔ | |
| Operativsystemet skjuler kompliserte maskinvare detaljer for å gjøre det enklere å utvikle programvare. | ✔ | |
| Vanlige programmer kjørere i kjernemodus fordi dette er mer effektivt. | | ✔ |

Maks poeng: 3

## 4.2 Pakkeswitching

Hva er sant for et pakkeswitchet nettverk?

**Velg ett eller flere alternativer**

- [ ] Det settes opp en dedikert forbindelse mellom sender og mottaker.
- [ ] Data for sending deles opp i mindre deler som sendes uavhengig på nettet. ✔
- [ ] Det må alltid reserveres kapasitet langs hele stien.
- [ ] Forskjellige pakker kan ta forskjellige stier fra avsender til mottaker. ✔

Maks poeng: 2

## 4.3 Antall IP-adresser

Du skal bestille Internett fra en ny leverandør til leiligheten din, og du leser på leverandøren sin nettside at den nye DHCP-tjenern er konfigurert med et 25-nettverk (CIDR-notasjon: /25).

Hvor mange IP-adresser kan deles ut av DHCP-tjeneren i dette nettverket? [ ] (126)

---

Maks poeng: 2

## 4.4 CIDR til punktnotasjon

Når du kobler en maskin til nettverket, får du følgende IP-adresse: *10.10.100.15*

Som nevnt i forrige oppgave har du fått vite fra leverandøren av nettverket at det er reservert et 25-nettverk. Din IP i CIDR-notasjon er da: *10.10.100.15/25*.

Hva er nettverksmasken til din maskin i punktnotasjon? [ ]

(255.255.255.128)

---

Maks poeng: 3

## 4.5 Nettverk + Broadcast

Som nevnt i forrige oppgave så har du koblet en datamaskin til nettverket, og du har fått IP-adressen: *10.10.100*.15

Nettverket er fremdeles et 25-nettverk, og IP-adressen i CIDR-notasjon er: *10.10.100*.15*/25*.

Hva er subnettadressen til nettverket? [ ] (10.10.100.0)

Hva er kringkastningsadressen til nettverket? [ ] (10.10.100.127)

---

Maks poeng: 6

## 4.6 TCP og UDP

Hvilke av disse tjenestene tilbys av både TCP og UDP

**Velg ett eller flere alternativer**

- [x] Multipleksing over en IP-adresse (porter) ✔
- [ ] Pålitelighet
- [ ] Metningskontoll
- [ ] Flytkontroll
- [x] Sjekksum (dataintegritet) ✔

Maks poeng: 2

## 4.7 Metningskontroll

Oppgaven til metningskontroll er å...

**Velg ett eller flere alternativer**

- [x] ...sikre at ressursene over en flaskehals i nettverket blir delt likt mellom datastrømı ✔ ıe
- [ ] ...hindre at mottakeren får mere data enn den kan ta imot
- [ ] ...telle antall datastrømmer over et nettverksinterface
- [x] ...hindre at nettet stopper opp på grunn av overbelastning (congestion collapse) ✔
- [ ] ...sende datapakker ut av riktig port i en router

Maks poeng: 4

## 4.8 Diverse fra applikasjonslaget

**Hvilke påstander fra applikasjonslaget er sanne og hvilke er usanne?**

| | Usann | Sann |
|---|---|---|
| Peer-to-peer (P2P) nettverk er den mest vanlige aksessmodellen som brukes. | ✔ | |
| Domain Name System (DNS) bruker kun TCP som transportprotokoll. | ✔ | |
| Pull er den vanligste forbindelsesstrategien i klient-tjener modellen. | | ✔ |
| Domain Name System (DNS) har en hierarkisk struktur. | | ✔ |
| Et content delivery nettverk (CDN) brukes for å gjøre distribusjonen av innhold som for eksempel video mer effektivt. | | ✔ |
| HTTPS bruker en offentlig-nøkkel infrastruktur (PKI) for å utveksle krypteringsnøkler. | | ✔ |

Maks poeng: 3