# Forside

**UNIVERSITETET I OSLO**
**Det matematisk-naturvitenskapelige fakultet**
**Skriftlig eksamen i IN1020**
**2024 HØST**
**Varighet: 11.desember kl. 15:00-19:00**
**Tillatte hjelpemidler: Alle trykte og skrevne hjelpemidler.**
**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.**

Faglærerne 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 Sikkerhet.
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

Alle trykte og skrevne hjelpemidler.

## Tilgjengelige ressurser i Inspera

- Enkel kalkulator
- Ascii-tabellen

# Seksjon 1

**Du er nå i seksjon 1  - Digital representasjon og assemblerkode.**

Oppgave nr 1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.7 og 1.8 er en del av seksjon 1.

## 1.1 Tallsystemer

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

**0f00d00d**

- [ ] Binære tall
- [ ] Titallsystemet
- [ ] Heksadesimale tall ✔
- [ ] Oktale tall

**7777**

- [ ] Oktale tall ✔
- [ ] Titallsystemet ✔
- [ ] Binære tall
- [ ] Heksadesimale tall ✔

**10101010**

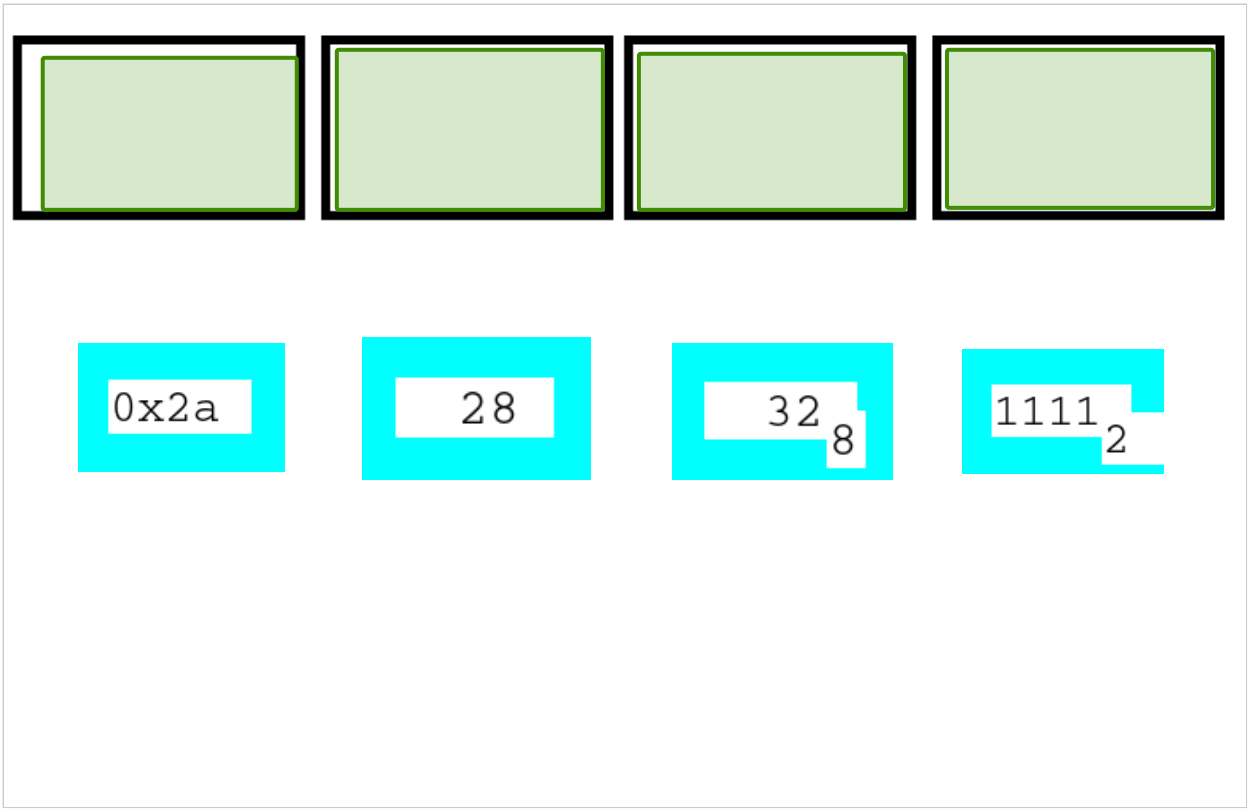
- [ ] Heksadesimale tall ✔
- [ ] Binære tall ✔
- [ ] Titallsystemet ✔
- [ ] Oktale tall ✔

---

Maks poeng: 2.4

## 1.2 Tallsortering

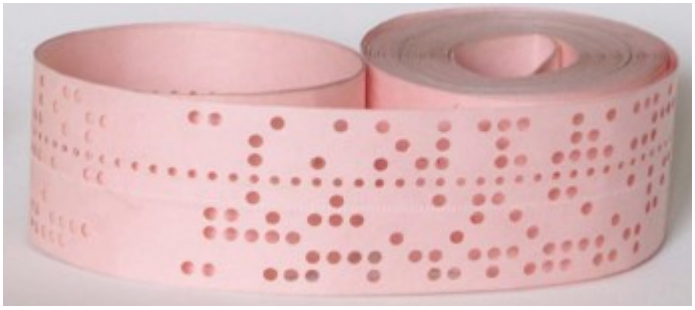
Sortèr tallene i stigende rekkefølge (fra venstre til høyre).



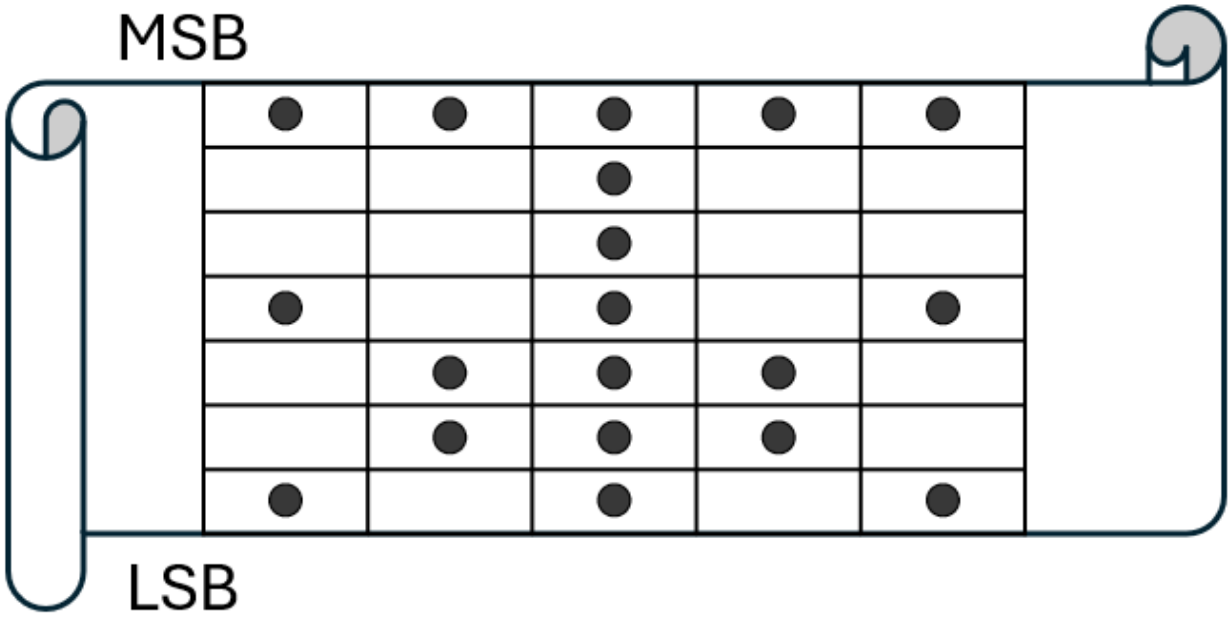

Maks poeng: 3

## 1.3 ASCII - Hullbånd

Tidlige datamaskiner brukte hullbånd for å representere informasjon:



Forestill deg at du har følgende utsnitt av et slikt hullbånd, der hver celle inneholder en "1" dersom det er hull (svart sirkel), og "0" ellers:




Hva står det her når du vet at data er representert med ASCII?

[ ] (IFFI)

---

Maks poeng: 3.8

## 1.4 Minnebruk

Du har skrevet et program for LMC (brukt i forelesning) hvor matvarer skal være representert digitalt på denne måten:

| Hva | Antall celler |
|---|---|
| PLU kode | 1 |
| Navn på varen | 4 |
| Pris | 1 |

Programkoden din bruker 43 celler. Hvor mange matvarer kan du representere?

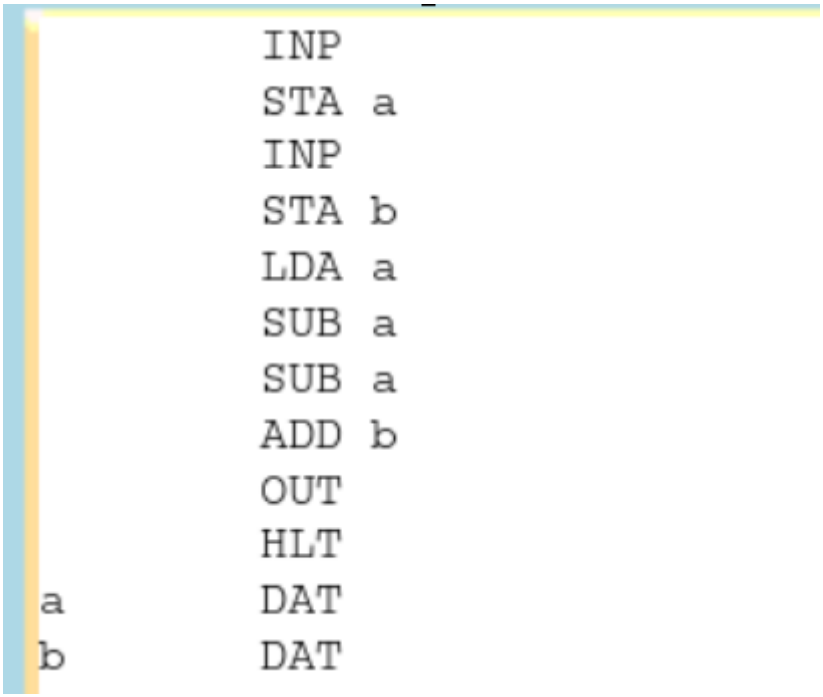
(9)

---

Maks poeng: 3

## 1.5 LMC - Aritmetikk

Du får oppgitt følgende program for LMC:



```
        INP
        STA a
        INP
        STA b
        LDA a
        SUB a
        SUB a
        ADD b
        OUT
        HLT
a       DAT
b       DAT
```

Hvilken funksjon beregner programmet?

**Velg ett alternativ:**

- a - b
- 2a + b
- -a + b ✔
- 2a - b

---

Maks poeng: 3

## 1.6 LMC - Maskinkode

Du får oppgitt følgende LMC kode, som skal lese inn to tall **a** og så **b**. Koden skal så beregne **a + b** og skrive ut svaret. Virker koden?

```
          INP
          STA a
          INP
          STA b
          DAT 508
          ADD b
          OUT
          HLT
a         DAT
b         DAT
```

**Velg ett alternativ:**

- Ja ✔
- Nei

Maks poeng: 3

## 1.7 LMC - Programflyt

Du får oppgitt følgende program i LMC:

```
        INP
        STA a
        INP
        STA b
        SUB a
        STA a
        LDA b
        ADD a
        OUT
        HLT
a       DAT
b       DAT
```

Hva skrives ut når bruker gir som input **2** og så **-1**?

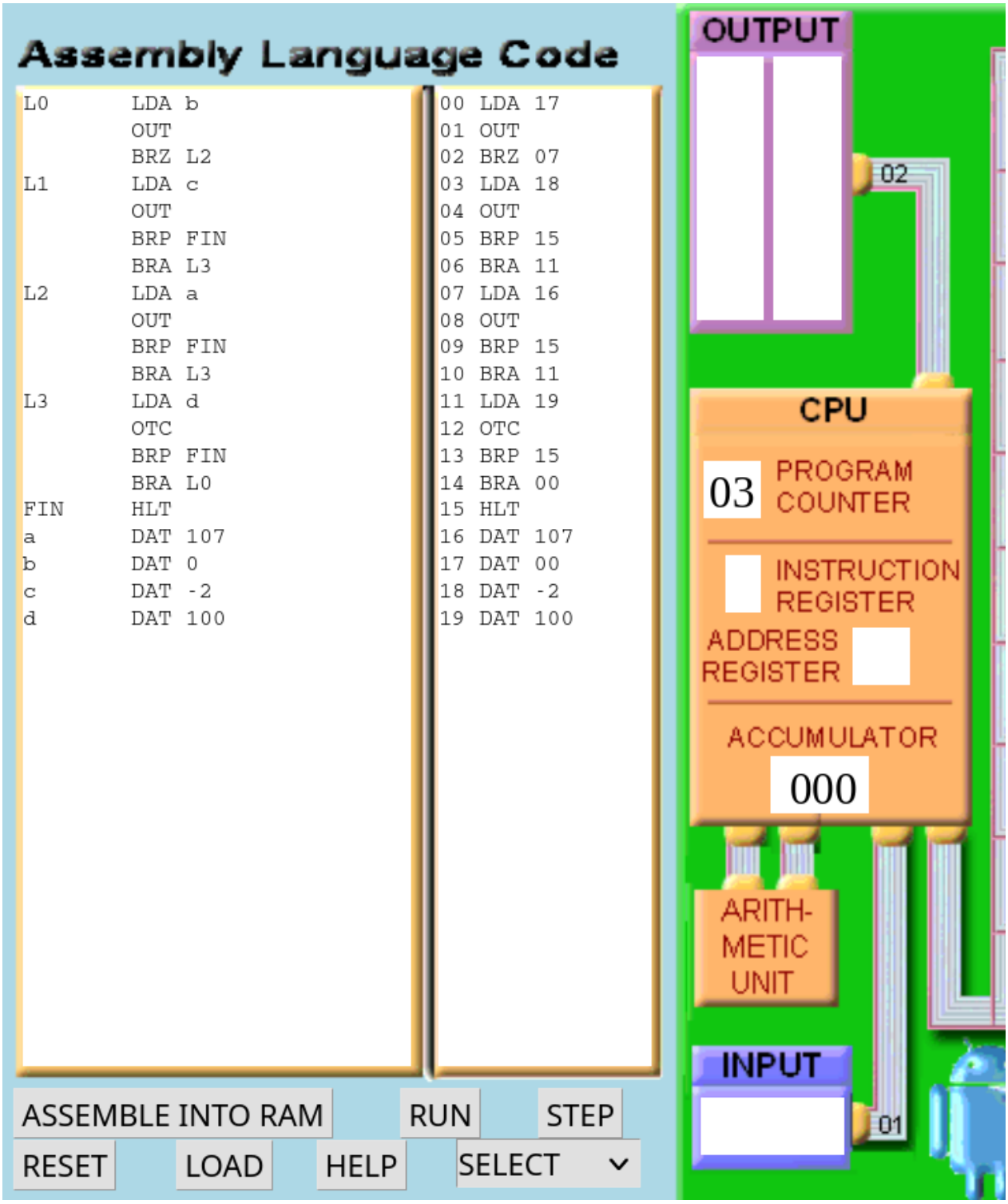
(-4)

---

Maks poeng: 3

## 1.8 LMC - Hopping

Du har programmert og satt opp LMC slik:




Hva skriver LMC ut når du trykker "run"?

Første utskrift:

(-2)

Andre utskrift:

(d)

Maks poeng: 3.8

# 24-seksjon 2

**Du er nå i seksjon 2 - Maskinvare og arkitektur.**

Oppgave nr 2.1, 2.2, 2.3, 2.4, 2.5 og 2.6 er en del av seksjon 2.

## 2.1 24-Minne/Cache

Et cachehierarki med to-nivås cache har følgende egenskaper:
30% av instruksjonene krever tilgang til Cache L1. 10% av instruksjonene krever tilgang til Cache L2. 4% av instruksjonene krever tilgang til RAM. Resten av instruksjonene krever ingen minneaksess.

Hver instruksjon tar: 1 klokkesykler uten minneaksess.20 klokkesykler for hvert cache-nivå. 400 klokkesykler for RAM.

Hvor mangeklokkesykler tar det å utføre 100 instruksjoner?
**Velg ett alternativ:**

- 3056
- 2600
- 2656 ✔
- 2456
- 3456
- 2256

Maks poeng: 5

## 2.2 24-datapath

**Velg de riktige alternativene for hvordan en prosessor håndterer instruksjoner.**
HINT! husker du forelesningen "Pipeline" og "kretser som driver koden"?

Instruksjonsformatet bestemmes av Velg alternativ (Operativ systemet, Minnet, Prosessorarkitekturen, Kompilatoren).

Resultatet av en beregning lagres midlertidig i Velg alternativ (Register, Klokke, Harddisk, Cache).

Dekoding av instruksjoner gjøres av Velg alternativ (ALU, Memory Controller, Instruction Decoder, DMA) i Velg alternativ (EX-fasen, DE-fasen, WB-fasen, IF-fasen).

Styresignaler fra dekodingen sendes til Velg alternativ (Minnet, Harddisk, ALU, PC) for å bestemme Velg alternativ (Synkronisering, Operasjon, Adresse, Spenning).

---

Maks poeng: 6

## 2.3 24-Godt og blandet

**Hvilke av disse utsagnene er sanne?**

- [ ] En NAND-port kan brukes til å lage alle andre logiske porter ✔
- [ ] En synkron krets trenger alltid en klokkepuls ✔
- [ ] Alle logiske porter må ha minst to innganger
- [ ] En CPU kan bare utføre instruksjoner som er lagret i RAM
- [ ] I en pipeline må alle trinn ta like lang tid ✔
- [ ] En halv-adder kan ikke håndtere mente-in ✔
- [ ] En pipeline med 5 trinn utfører alltid 5 instruksjoner samtidig
- [ ] Cache-minne er tregere enn hovedminnet (RAM)

---

Maks poeng: 4

## 2.4 24-Abstraksjonnivå

Ranger disse 5 i henhold til abstraksjonivåene de tilhører relativ til hverandre.

| | |
|---|---|
| Høyeste | Velg alternativ (ALU, Inverter, Transistor, Register, CPU) |
| | Velg alternativ (ALU, Transistor, Register, Inverter, CPU) |
| | Velg alternativ (Transistor, CPU, Register, Inverter, ALU) |
| | Velg alternativ (Register, Transistor, ALU, CPU, Inverter) |
| Laveste | Velg alternativ (ALU, Transistor, CPU, Inverter, Register) |

Maks poeng: 3

## 2.5 24-Kretsanalyse

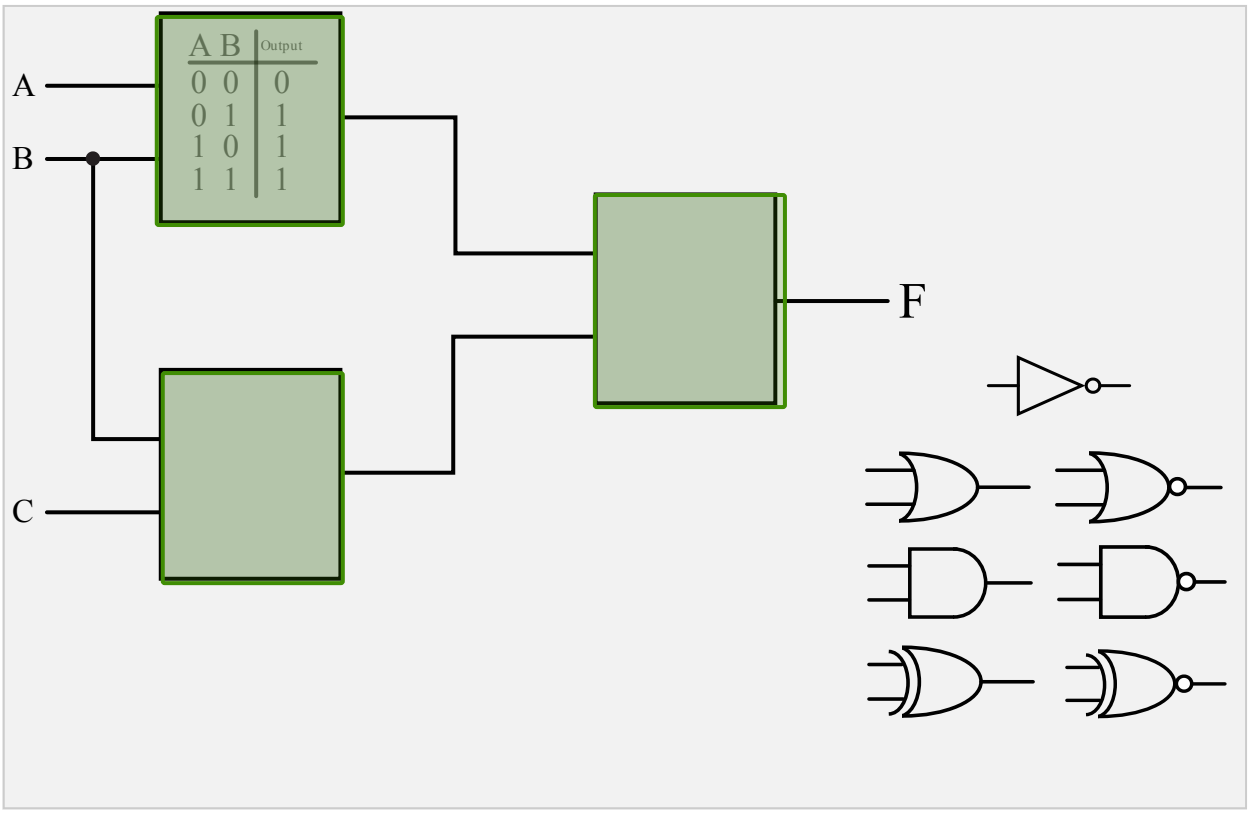
Kretsen har funksjonen

$$F = \overline{A'C' + B + AC + A}$$

Bruk figuren under til å dra de riktige portene inn på de grå boksene.

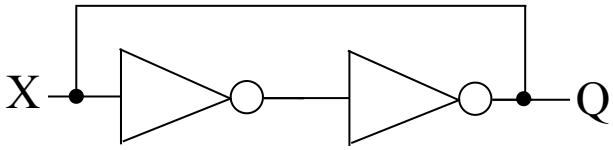
Hint! IKKE forenkle funksjonsuttrykket. Bruk funksjonsuttrykket slik det står.
Hint! Husker du de ulike symbolene for et funksjonsuttrykk som er invertert?
Hint! I den ene gråboksen er sannhetsverditabellen til porten oppgitt.

**Dra og slipp riktig port til riktig grå felt.**




Maks poeng: 5

## 2.6 24-Undring




**Slik skal du svare på oppgaven:**
For hvert alternativ skal du angi hvor sannsynlig det er at alternativet er riktig, uttrykt i prosent (%).
Eksempler:

- Hvis du er helt sikker på at alternativ 1 er riktig og alle andre er feil:
  - Alternativ 1: 100%
  - Alle andre alternativer: 0%
- Hvis du tror både alternativ 1 og 2 kan være riktige, men er mer sikker på alternativ 1:
  - Alternativ 1: 75%
  - Alternativ 2: 25%
  - Alle andre alternativer: 0%
- Hvis du er usikker mellom tre alternativer:
  - Alternativ 1: 50%
  - Alternativ 2: 25%
  - Alternativ 3: 25%
  - Andre alternativer: 0%

Summen av alle prosentene skal bli 100%.

**Hva gjør/hvilke funksjon har kretsen over?**

| | 0 % | 25 % | 50 % | 75 % | 100 % |
|---|---|---|---|---|---|
| Minne | ○ | ○ | ○ | ○ | ○ ✔ |
| Inverter | ○ ✔ | ○ | ○ | ○ | ○ |
| Forsterker | ○ ✔ | ○ | ○ | ○ | ○ |
| NAND | ○ ✔ | ○ | ○ | ○ | ○ |

Maks poeng: 2

# 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 Brudd på sikkerhetsmål

Angi hvilket sikkerhetsmål som først og fremst brytes som resultat av hvert av følgende angrep:
**Finn de som passer sammen:**

| | Autentisitet | Konfidensialitet | Tilgjengelighet | Integritet |
|---|---|---|---|---|
| Modifisering av datatrafikk | ○ | ○ | ○ | ○ ✔ |
| Signalforstyrrelse i trådløst nettverk | ○ | ○ | ○ ✔ | ○ |
| SQL-injisering som endrer innhold | ○ | ○ | ○ | ○ ✔ |
| Avlytting av datatrafikk | ○ | ○ ✔ | ○ | ○ |
| Falsk DNS-tjener | ○ ✔ | ○ | ○ | ○ |
| Knekke fil-kryptering | ○ | ○ ✔ | ○ | ○ |

Maks poeng: 3

## 3.2 Sikkerhetsmål refleksjon

Sikkerhetsmål er egenskaper som ønskes ivaretatt i IT-systemer, og som ikke er eksakte størrelser. Målene er tett sammenvevd, påvirkes av hverandre, og kan til og med være i konflikt med hverandre.

**Velg riktig sikkerhetsmål i de to utsagnene under:**

Økt behov for konfidensialitet kan gå på bekostning av Velg alternativ (personvern, tilgjengelighet, integritet, autentisitet).

Behov for detaljert sporbarhet kan gå på bekostning av Velg alternativ (autentisitet, integritet, personvern, tilgjengelighet).

---

Maks poeng: 2

## 3.3 Begrepsforståelse

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

Hjelp

| | | |
|---|---|---|
| Hash-funksjoner | Trusselaktør | Dataminimering |
| Sårbarhet | Lagringsbegrensning | Digitale sertifikater |
| Brannmur | Innbruddsdeteksjon | Phishing |
| Risikoanalyse | Konsekvens | Tilgangskontroll |
| Autorisering | Spoofing | Databehandler |
| Trussel | | |

Autorisering ✔ er å lage en policy for tilgang til ressurser.

Hash-funksjoner ✔ brukes for å unngå lagring av passord i klartekst.

Innbruddsdeteksjc ✔ kan avdekke forsøk på digitale innbrudd i et datanettverk.

Spoofing ✔ er å forfalske en avsender i kommunikasjon.

Dataminimering ✔ er det å bare samle inn og behandle personopplysninger som er nødvendige for et formål.

Risikoanalyse ✔ er å vurdere sannsynlighet og konsekvens av potensielle sikkerhetshendelser.

Konsekvens ✔ kan være tap av omdømme på grunn av datalekkasje fra et selskap sitt kunderegister.

Trusselaktør ✔ er betegnelsen på den som vil utføre skadelig aktivitet.

---

Maks poeng: 4

## 3.4 Trusselmodellering

En liten bedrift jobber med forskning på og utvikling av nye og klimavennlige løsninger for kraftleveranse. Bedriften er redd for at konkurrenter skal stjele ideer, dokumenter og annet digitalt materiale som omhandler arbeidet deres (altså bedriftshemmeligheter), og f.eks. komme dem i forkjøpet med patenter på nye løsninger. Du er innleid som sikkerhetskonsulent for å hjelpe bedriften med trusselmodellering for å unngå lekkasje av denne type informasjon.

**a)** Å beskytte bedriftshemmelighetene er å sørge for Velg alternativ (tilgang til, tilgjengelighet til, konfidensialitet for, integritet for)informasjon.

**b)** Bedriften bruker trådløst nett i kontorlokalene sine. Hva vil være fornuftige sikkerhetstiltak mot avlytting av nettverkstrafikk?

**Velg ett eller flere alternativer**

- [ ] Sørge for signalforstyrrelser.
- [ ] Benytte sikre nettverksprotokoller. ✔
- [ ] Ha redundante IT-systemer.
- [ ] Bruke autentiseringsmekanismer for oppkobling til trådløst nettverk. ✔
- [ ] Ha sikkerhetskopi av alle data.
- [ ] Sørge for oppdatert programvare i trådløse aksesspunkter. ✔

**c)** En annen opplagt trussel er *datalekkasje* som følge av *sosial manipulasjon.* Hva vil være fornuftige sikkerhetstiltak for å unngå denne type hendelser?

**Velg ett eller flere alternativer**

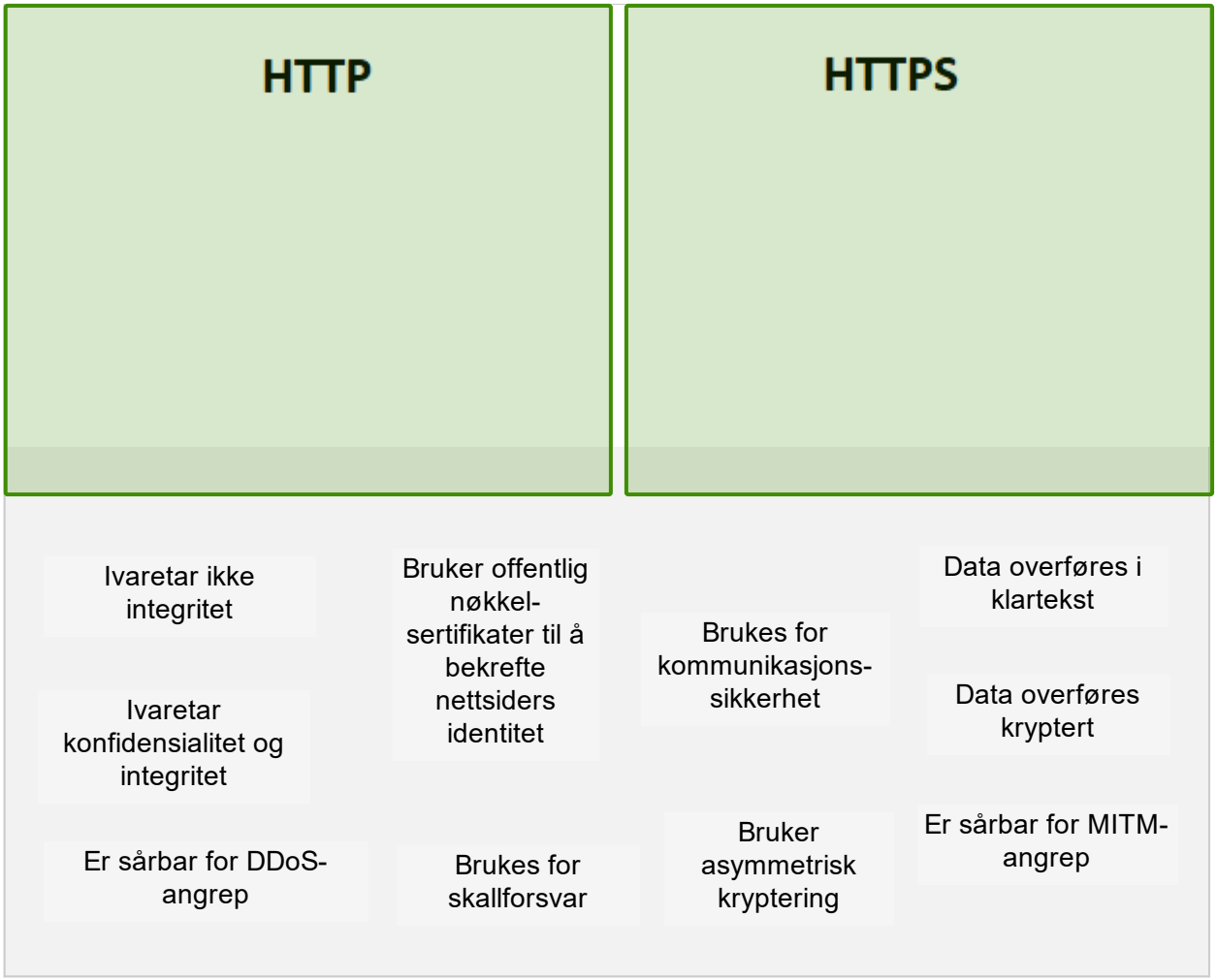
- [ ] Ha tilstrekkelig økonomistyring.
- [ ] Kurse ansatte i informasjonssikkerhet. ✔
- [ ] Sørge for at ingen ansatte har tilgang til mer informasjon enn de har strengt behov ✔
- [ ] Ha redundante IT-systemer.
- [ ] Sørge for at alle ansatte har tilgang til alle bedriftshemmeligheter.
- [ ] Ha gode rutiner for gjenoppretting av IT-systemene.

Maks poeng: 3

## 3.5 Sikker nettverkskommunikasjon

HTTP og HTTPS er begge protokoller som brukes for å overfør data over internett.

**Dra og slipp de ulike utsagnene slik at de passer inn med egenskapene til HTTP og HTTPS. Merk: Ikke alle alternativene passer inn.**




Maks poeng: 2

## 3.6 Ulike typer kryptering

Hash-funksjoner, symmetrisk og asymmetrisk kryptering er tre ulike former for kryptografi. I denne oppgaven skal du knytte riktig egenskap til riktig krypteringstype.

**Finn de som passer sammen:**

| | Ingen av delene | Hash-funksjoner | Symmetrisk kryptering | Asymmetrisk kryptering |
|---|---|---|---|---|
| Bruker én nøkkel for kryptering og en annen for dekryptering | ○ | ○ | ○ | ○ ✔ |
| Kalles også kryptovirus | ○ ✔ | ○ | ○ | ○ |
| Kan benyttes uten krypteringsnøkkel | ○ | ○ ✔ | ○ | ○ |
| Bør være kollisjonsresistent | ○ | ○ ✔ | ○ | ○ |
| Utgjør et viktig element i en PKI | ○ | ○ | ○ | ○ ✔ |
| Resultatet kan ikke dekrypteres | ○ | ○ ✔ | ○ | ○ |
| Kalles også hemmelig nøkkel-kryptering | ○ | ○ | ○ ✔ | ○ |
| Kalles også sjekksumalgoritme | ○ | ○ ✔ | ○ | ○ |
| Benyttes for autorisasjon | ○ ✔ | ○ | ○ | ○ |

Maks poeng: 3

## 3.7 PKI og kryptering

Jonas, Trygve og Sylvi kommuniserer digitalt ved å bruke en offentlig nøkkel-infrastruktur (PKI). Jonas har fått et nøkkelpar bestående av en privat nøkkel som kun er kjent for Jonas, og en offentlig nøkkel som er gjort kjent for flere, bl.a. både Trygve og Sylvi.

**a)** Hvilke utsagn er korrekte når dette nøkkelparet benyttes for digital signatur?
**Velg ett eller flere alternativer**

- [ ] Sylvi kan validere digital signatur Jonas har signert med sin private nøkkel. ✔
- [ ] Trygve kan validere digital signatur Jonas har signert med sin offentlige nøkkel.
- [ ] Jonas kan validere digital signatur Sylvi har signert med Jonas sin offentlige nøkkel.
- [ ] Trygve kan validere digital signatur Jonas har signert med sin private nøkkel. ✔

**b)** Hvilke utsagn er korrekte når dette nøkkelparet brukes for å kryptere meldinger/dokumenter?
**Velg ett eller flere alternativer**

- [ ] Bare Sylvi kan lese (dekryptere) en melding Jonas krypterer med sin private nøkkel.
- [ ] Jonas kan lese (dekryptere) meldingen Sylvi krypterer med Jonas sin offentlige nøkkel. ✔
- [ ] Kun Jonas kan lese (dekryptere) en melding Sylvi eller Trygve krypterer med Jonas sin offentlige nøkkel. ✔
- [ ] Trygve kan lese (dekryptere) meldingen Sylvi krypterer med Jonas sin offentlige nøkkel.

**c)** Hva er hovedformålet med en PKI?
**Velg ett alternativ**

- ○ Å lagre alle brukeres private nøkler på et sikkert sted.
- ○ Å forhindre at trusselaktører kan lese krypterte meldinger.
- ○ Å kryptere all kommunikasjon på internett.
- ○ Å sikre ektheten av offentlige nøkler og trygg nøkkeldistribusjon. ✔

**d)** Hvilke av følgende påstander om digitale sertifikater for en PKI er korrekte?

**Velg ett eller flere alternativer**

- [ ] Et digitalt sertifikat signeres av en sertifikatmyndighet (CA). ✔
- [ ] Et digitalt sertifikat knytter en offentlig nøkkel til en identitet. ✔
- [ ] Et digitalt sertifikat krypterer alle meldinger som sendes mellom brukere.
- [ ] Et digitalt sertifikat inneholder alle eierens private nøkler.

**e)** Hvilken rolle spiller en sertifikatmyndighet (CA) i en PKI?
**Velg ett alternativ**

- ○ De krypterer alle meldinger som sendes mellom brukere.
- ○ De lagrer alle brukeres private nøkler.
- ○ De utsteder og signerer digitale sertifikater. ✔
- ○ De utvikler nye krypteringsalgoritmer.

---

Maks poeng: 4

## 3.8 Personopplysningsvern

Du er ansatt som utvikler i en teknologibedrift, og har fått i oppdrag i å være med på utvikling av et nytt IT-system for en helseinstitusjon. Systemet vil behandle personopplysninger.

**a)** Personopplysningsloven sier noe om *Behandling av særlige kategorier av personopplysninger.* Hvilke av følgende type personopplysning går under denne katagorien?

**Velg ett eller flere alternativer**

- [ ] Telefonnummer
- [ ] Fagforeningsmedlemskap ✔
- [ ] Rasemessig eller etnisk opprinnelse ✔
- [ ] Navn
- [ ] IP-adresse
- [ ] Helseopplysninger ✔

**b)** I utviklingsprosessen er en av oppgavene å implementere *Innebygd personvern.* Hvorfor er det viktig å legge til rette for innebygd personvern i programvareutviklingen?

**Velg ett eller flere alternativer**

- [ ] For å gjøre systemene mer komplekse.
- [ ] For å sikre at systemene overholder personvernprinsippene. ✔
- [ ] For å beskytte de registrertes rettigheter i behandling av personopplysninger. ✔
- [ ] Fordi man ikke har innebygget sikkerhet.

**c)** Helseinstitusjonen har valgt å bruke en ekstern leverandørs skyløsning for å lagre pasientdata. Lagring av alle data (også personopplysninger) på den eksterne leverandørens datautstyr som er fysisk plassert i et EU-land, og overføring av data går over internett.
Hvilke utsagn nedenfor stemmer overens med føringer i Personopplysningsloven (GDPR) for helseinstitusjonens behandling av personopplysninger?

**Velg ett eller flere alternativer**

- [ ] Personopplysningsloven stiller krav til informasjonssikkerhet. ✔
- [ ] Når personopplysninger lagres hos et eksternt firma kan helseinstitusjonen se bort fra personopplysningsloven for sin behandling av personopplysninger.
- [ ] All behandling av personopplysninger skal skje med egnede tekniske og organisatoriske tiltak. ✔
- [ ] En pasient har aldri rett til innsyn i hvilke helseopplysninger som er lagret om seg.
- [ ] Helseinstitusjonen er juridisk ansvarlig for at data om pasienter behandles i samsvar med personopplysningsloven. ✔

---

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 Lett blanding - Nettverk

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

| | Sann | Usann |
|---|---|---|
| Det er kun tjenere som kan regnes som endesystemer i datanettverk. | ○ | ✔ |
| Internett er mange nettverk som er koblet sammen. | ✔ | ○ |
| Peer-to-Peer modellen er den vanligste aksessmodellen i datanettverk. | ○ | ✔ |
| Moderne trådløse nettverk (WiFi) bruker kommunikasjonsmodellen punkt-til-punkt. | ○ | ✔ |
| Et moderne kablet nettverk (Ethernet) med en svitsj bruker stjerne- eller tre-topologi. | ✔ | ○ |
| Nettverksprotokoller er et sett med regler om hvordan kommunikasjon skal foregå. | ✔ | ○ |
| IPv4 er en tilkoblingsorientert protokoll | ○ | ✔ |
| Hovedmotivasjonen bak IPv6 er å øke antallet globalt adresserbare IP-adresser. | ✔ | ○ |

Maks poeng: 4

## 4.2 Operativsystemer

Hvilke av utsagnene om operativsystemer er sanne?
**Velg ett eller flere alternativer**

- [ ] Alle moderne programmer kjører i kjernemodus for å få raskere tilgang til ressurser.
- [ ] Datamaskiner som kontrollerer komponenter som autopiloten i et fly har høye krav til pålitelighet, og har derfor ikke et operativsystem.
- [ ] En av hovedoppgavene til et operativsystem er å fordele resursene i datamaskine. ✔
- [ ] Moderne smarttelefoner bruker ikke operativsystemet sine tjenester for skedulering av programmer.
- [ ] En av hovedoppgavene til et operativsystem er å skjule detaljer om maskinvare for å gjøre det enklere å utvikle programmer. ✔
- [ ] Operativsystemer som nyere Windows og Linux er bygd opp etter monolittisk kjern modellen. ✔
- [ ] Et operativsystem vil kun sørge for rettferdig fordeling av prosessoren. Det er programmene selv som han ansvaret for å sørge for retferdig fordeling av minne (RAM).

---

Maks poeng: 3

## 4.3 Antall IP-adresser

Du skal sette opp et privat nettverk i en liten bedrift, og du får beskjed om at leverandøren av datanettverket har satt opp et 28-nettverk (CIDR-notasjon: /28).

Hvor mange IP-adresser kan deles ut av DHCP-tjeneren i dette nettverket? [ ] (14)

---

Maks poeng: 3

## 4.4 CIDR til punktnotasjon

Når du kobler en maskin til nettverket, får du følgende IP-adresse: *192.168.100.164*

Som nevnt i forrige oppgave har du fått vite fra leverandøren av nettverket at det er reservert et 28-nettverk. Din IP i CIDR-notasjon er da: *192.168.100.164/28*.

Hva er nettverksmasken til din maskin i punktnotasjon? [ ]

(255.255.255.240)

---

Maks poeng: 4

## 4.5 Subnet + Broadcast

Som nevnt i forrige oppgave så har du koblet en datamaskin til nettverket, og du har fått IP-adressen: *192.168.100.164*.
Nettverket er fremdeles et 28-nettverk, og IP-adressen i CIDR-notasjon er: *192.168.100.164/28*.

Hva er subnettadressen til nettverket? [ ] (192.168.100.160)

Hva er kringkastningsadressen til nettverket? [ ] (192.168.100.175)

---

Maks poeng: 6

## 4.6 Transportlagsprotokoller

Transportlaget i TCP/IP-modellen består hovedsakelig av to protokoller, TCP og UDP.

**Hvilke påstander om protokollene i transportlaget er sanne og hva er usanne?**

| | Sant | Usant |
|---|---|---|
| Transportlaget forholder seg bare til ende-til-ende, og har ingen kjennskap om hvordan data blir sendt på nettet. | ✔ | |
| Både TCP og UDP sørger for at data kommer frem i riktig rekkefølge. | | ✔ |
| Både TCP og UDP støtter multipleksing ved hjelp av porter. | ✔ | |
| Metningskontroll sørger for at kapasiteten i nettverket blir delt på alle forbindelsene. | ✔ | |
| UDP er den mest brukte av de to protokollene i transportlaget. | | ✔ |
| UDP er en rask protokoll, og egner seg derfor godt til overføring av store filer. | | ✔ |
| TCP er en tilkoblingsorientert protokoll. | ✔ | |
| Det er ikke mulig å bruke kryptering på applikasjonslaget når vi bruker UDP. | | ✔ |

Maks poeng: 2

## 4.7 HTTP

Hvilket av disse utsagnene er korrekt for en persistent forbindelse i HTTP?
**Velg et eller flere alternativer**

- [ ] Den samme TCP-forbindelsen blir gjenbrukt til flere runder med nye HTTP-forespø ✔ er.
- [ ] TCP-forbindelsen fortsetter å forsøke å koble seg opp, selv om den blir avsluttet eller brutt.
- [ ] Nyttelasten sendes mange ganger uavhengig av nettverksforhold for å være sikker på at de kommer frem.
- [ ] HTTP-forespørsler kan ikke multiplekses over denne forbindelsen.

---

Maks poeng: 1

## 4.8 HTTP-streaming

Hvilke utsagn stemmer om streaming av video over HTTP?
**Velg ett eller flere alternativer**

- [ ] Streaming over HTTP bruker kun UDP til overføring.
- [ ] Det er klienten som bestemmer kvaliteten som lastes ned, ikke tjeneren. ✔
- [ ] Med HTTP-streaming må man bufre hele videoen før avspilling kan starte.
- [ ] Video deles opp i små segmenter og forskjellige kvaliteter. ✔

---

Maks poeng: 2