# Retteveiledning Digital Representasjon - IN1020 H24

December 30, 2024

## 1 Oppgave 1: Tallsystemer

I denne oppgaven får vi oppgitt tre forskjellige tall, hvor notasjonen som bestemmer hvilket tallsystem de er skrevet i, er borte. Oppgaven spør hvilke tallsystemer de forskjellige tallene *kan* være skrevet i. Det finnes altså flere alternativer for et gitt tall.

**0f00d00d** kan kun være heksadesimalt, fordi sifferne **f** og **d** kun finnes i det heksadesimale tallsystemet.

**7777** kan være heksadesimalt, desimalt, eller oktalt, men ikke binært. Dette er fordi sifferet **7** ikke finnes i det binære tallsystemet.

**10101010** kan være heksadesimalt, desimalt, oktalt eller binært, fordi sifferne **0** og **1** finnes i alle disse fire tallsystemene.

## 2 Oppgave 2: Tallsortering

Oppgaven ber om å sortere fire tall representert i fire ulike tallsystemer. De skal sorteres i stigende rekkefølge fra venstre til høyre. Oppgaven er dermed en øvelse i å konverte fra hexadesimal, oktal og binært til titallsystemer.

- $1111_2$: $1 * 2^3 + 1 * 2^2 + 1 * 2^1 + 1 * 2^0 = 8 + 4 + 2 + 1 = 15$
- $32_8$: $3 * 8^1 + 2 * 8^0 = 24 + 2 = 26$
- $0x2a$: $2 * 16^1 + 10 * 16^0 = 32 + 10 = 42$

## 3 Oppgave 3: ASCII Hullbånd

Oppgaven ber om hva som står skrevet i et ASCII hullbånd (se Figur 2). Vi får oppgitt at hver "celle" i kortet inneholder et hull eller ikke, som henholdsvis betyr en "1" eller "0". Følgelig er informasjon representert binært (to tilstander). Hver kolonne representerer en karakter. Dette kan vi se på to forskjellige måter:

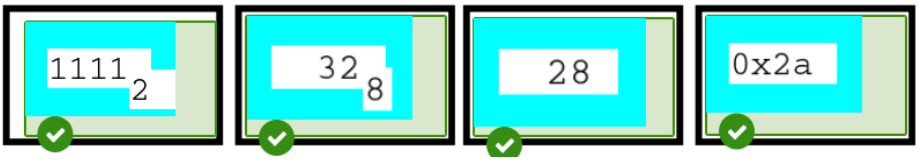



Figure 1: Oppgave 2: Tallsortering

1. Vi får oppgitt "LSB" og "MSB", som betyr "least/most significant bit". Dette er forklart i pensumboka.

2. hvert ASCII tegn trenger totalt sju bits (128 ASCII tegn), samme antall som vi ser i en kolonne.

Videre er teksten symmetrisk, så om vi leser fra høyre eller venstre, har ikke noe å si. ASCII tabellen fra eksamen er på hexadesimal, så vi kan oversette tegnene:

- $1001001_2 = 0x49$ (ASCII 'I')
- $1000110_2 = 0x46$ (ASCII 'F')
- $1111111_2 = 0x7F$ (ASCII 'DEL')

Oversettingen gjøres med metode vist på forelesning:

| Hex | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Binær | 0 | 1 | 10 | 11 | 100 | 101 | 110 | 111 | 1000 | 1001 | 1010 | 1011 | 1100 | 1101 | 1110 | 1111 |

ASCII 'DEL' er et spesialtegn som i praksis betyr "ignorer dette tallet". Teknisk sett er det riktige svaret "IFFI", men man får full uttelling for svar som "IFDELFI", "IFI" og variasjoner av dette.

# 4 Oppgave 4: Minnebruk

Denne oppgaven likner på en av deloppgavene i obligen. Minnet i LMC (brukt i forelesningen) har 100 celler til data. Man får oppgitt at 43 av dem er brukt av programmet, så det er igjen 57 celler. Dersom man får oppgitt at en vare er representert med 6 celler, er det altså plass til antall varer $N$:

$$N = \lfloor \frac{57}{6} \rfloor = 9 \tag{1}$$

Det er altså plass til totalt ni matvarer.

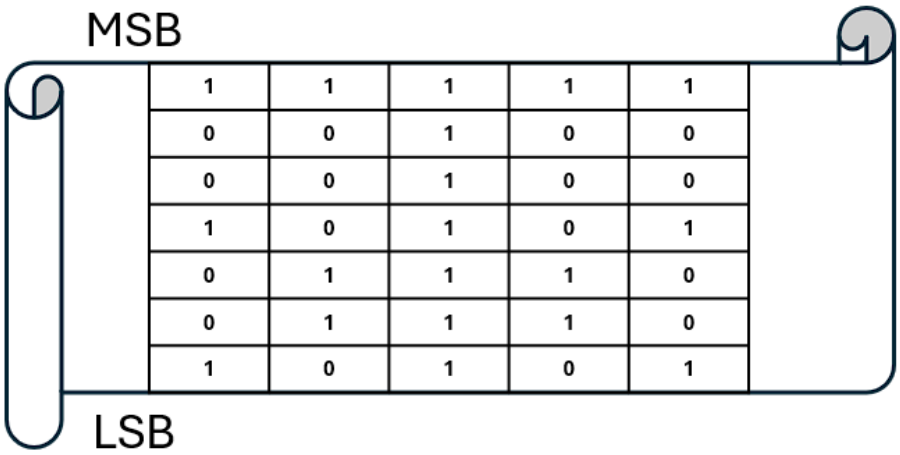



Figure 2: Oppgave 3: ASCII Hullbånd

# 5 Oppgave 5: LMC - Aritmetikk

- Programmet leser inn to tall, som lagres på etikett **a** og **b**.
- Programmet henter **a** i akkumulatoren.
- Programmet trekker det som ligger i etikett **a** fra tallet i akkumulatoren (**a**), vi får altså 0 i akkumulatoren etter dette ($a - a = 0$).
- Programmet gjentar subtraksjonen, denne gangen trekker vi det som ligger i etikett **a** fra 0, siden det er det som er i akkumulatoren. Vi får derfor -a ($0 - a = -a$)).
  - Teknisk sett har vi allerede en sterk indikasjon på hva svaret er gitt alternativene, men det er nok lurt å gå igjennom for å være sikker.
- Programmet legger det som ligger i etikett **b** til tallet i akkumulatoren, dvs $-a + b$.
- Programmet skriver ut svaret og avslutter på korrekt måte.

Riktig svar på oppgaven er derfor $-a + b$.

# 6 Oppgave 6: LMC - Maskinkode

Oppgaven spør om programmet virker korrekt. For å svare på dette må vi vite hva "DAT 508" betyr. For LMC - og maskiner generelt - er instruksjoner bare tall. LMC ser på det første sifferet (5) som en instruksjonskode, og de to siste (08) som en adressedel (med noen spesialtilfeller for IO instruksjoner).

Instruksjonskode 5 er "LDA" (Load Accumulator). Adressedelen er 8, som er minnecellen etikett **a** peker på. Mao. ser programmet slik ut:

```
          INP          00 INP
          STA a        01 STA 08
          INP          02 INP
          STA b        03 STA 09
          LDA a        04 LDA 08
          ADD b        05 ADD 09
          OUT          06 OUT
          HLT          07 HLT
a         DAT          08 DAT 00
b         DAT          09 DAT 00
```

Følger vi programflyten til dette programmet, ser vi at det virker som det skal. Bruk gjerne metoden vist i neste oppgave for å forstå programflyten.

# 7 Oppgave 7: Programflyt

For å svare på hva programmet gjør, må vi selv tolke en og en instruksjon, og følge nøye med på hva programmet gjør. For å komme i gang med dette kan det lønne seg å tegne programmet inn i en tabell, og tenke seg hva programmet endrer, i dette tilfellet akkumulatoren. Vi får oppgitt at bruker først gir som input 2, og så -1. Sjekk hver instruksjon, rekke for rekke, og følg med på hvordan akkumulatoren endrer seg igjennom programmet.

| Etikett | Instruksjon | Akkumulator | Etikett a | Etikett b |
|---|---|---|---|---|
| | INP | 2 | | |
| | STA a | 2 | 2 | |
| | INP | -1 | 2 | |
| | STA b | -1 | 2 | -1 |
| | SUB a | -3 | 2 | -1 |
| | STA a | -3 | -3 | -1 |
| | LDA b | -1 | -3 | -1 |
| | ADD a | -4 | -3 | -1 |
| | OUT | -4 | -3 | -1 |
| | HLT | -4 | -3 | -1 |
| a | DAT | | | |
| b | DAT | | | |

Riktig svar er dermed -4.

# 8 Oppgave 8: LMC - Hopping

Oppgaven spør om hva LMC skriver ut gitt en kode med bruk av mange hopp instruksjoner (BRA, BRP, BRZ). En tilleggsinformasjon her er at programtelleren er satt til "3". Når vi trykker "RUN" vil dermed den første instruksjonen som hentes og eksekveres, være den som ligger i minnecelle 3. Følger vi flyten derfra (bruk gjerne metode fra forrige oppgave) får vi skrevet ut **-2** og så **d**. Det gis poeng for å forstå flyten fra celle 0 også, hvor man vil få skrevet ut **0** og så **107**.

# 2024 - Sensurveiledning in1020 – maskinvaredelen

## Oppgave 2.1 - Minne/Cache

Riktig svar er **2656** og gir 5 poeng
Svar 3056 gir 4 poeng
Svar 2456 gir 3 poeng
Svar 2600 gir 2 poeng
Svar 3456 gir 1 poeng
Svar 2256 gir 0 poeng

## Oppgave 2.2 – Datapath

**Her får man 1 poeng per riktige svar.**
Instruksjonsformatet bestemmes av **Prosessorarkitekturen**.
Resultatet av en beregning lagres midlertidig i **Register**.
Dekoding av instruksjoner gjøres av **Instruction Decoder.** i **IF-fasen**.
*Her har vi også akseptert ALU og DE-fasen*
Styresignaler fra dekodingen sendes til **ALU** for å bestemme **OPERASJON** .

## Oppgave 2.3 – Godt og blandet

**Her får man både positive og negative poeng basert på hva man svarer.**
**1 poeng** En NAND-port kan brukes til å lage alle andre logiske porter
**-0.5 poeng** En CPU kan bare utføre instruksjoner som er lagret i RAM
**-1 poeng** Alle logiske porter må ha minst to innganger
**-1.5 poeng** Cache-minne er tregere enn hovedminnet (RAM)
**1 poeng** En halv-adder kan ikke håndtere mente-in
**0.5 poeng** En synkron krets trenger alltid en klokkepuls
**-0.5 poeng** En pipeline med 5 trinn utfører alltid 5 instruksjoner samtidig
**1 poeng** I en pipeline må alle trinn ta like lang tid

## Oppgave 2.4 – Abstraksjonsnivå

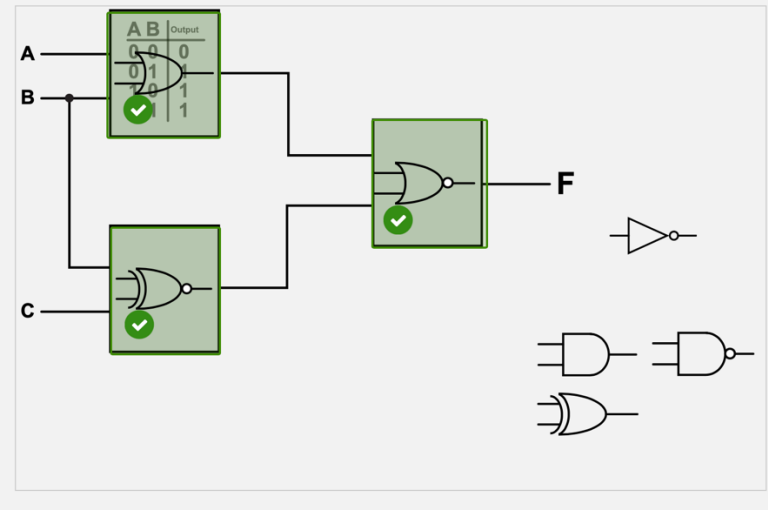
**Her får du 0.75 poeng for hver riktig plassering – og maks 3 poeng (ikke 3.75)**
CPU
ALU
Register

Inverter
Transistor

# Oppgave 2.3 – Kretsanalyse

**Hver riktig svar gir 1.5 og hvis alle tre er riktig så får man 5 poeng.**
**Beklageligvis så var det feil i funksjonsuttrykket. Det riktige er:**

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




# Oppgave 2.2 – Undring

Riktig svar er **Minne**
Her får man maks 2 poeng. De aller fleste har fått god uttelling her og oppgaven er manuelt kvalitetsikret. Ingen har fått trekk.

# Veiledning til fasit for eksamen i seksjon 3 «Datasikkerhet» H24

## Oppgave 3.1 *Sikkerhetsmål som først og fremst brytes som resultat av hvert av følgende angrep:*

0.5 poeng for riktig svar, ingen minuspoeng.

- Signalforstyrrelse i trådløst nettverk: Tilgjengelighet – trådløst nett fungerer ikke.
- Modifisering av datatrafikk: Integritet - datapakker kan være endret.
- Avlytting av datatrafikk: Konfidensialitet – uvedkommende kan ha fått tilgang til informasjon.
- Knekke fil-kryptering: Konfidensialitet – uvedkommende kan ha fått tilgang til informasjon.
- Falsk DNS-tjener: Autentisitet – annen DNS-tjener enn den man tror man kommuniserer med.
- SQL-injisering som endrer innhold: Integritet – innhold er endret.

## Oppgave 3.2 *Refleksjon over sikkerhetsmål*

1 poeng for hvert riktige svar, ingen minuspoeng

a) Tilgjengelighet. Strenge tiltak for å sikre at uvedkommende ikke kan få tilgang kan føre til at andre feilaktig ikke får tilgang til det de skal.
b) Personvern. Sporbarhet sikres ofte ved loggføring av hendelser, og kan inkludere informasjon om personer som har utført oppgaver, som igjen medfører behov for å lagre personopplysninger.

## Oppgave 3.3 *Kombiner riktig begrep med riktig tekst.*

0.5 poeng for riktig svar, ingen minuspoeng

- **Autorisering** er å lage en policy for tilgang til ressurser (mens tilgangskontroll er å *håndheve*).
- **Hash-funksjoner** brukes for å unngå lagring av passord i klartekst, passord *hashes*.
- **Innbruddsdeteksjon** kan avdekke forsøk på digitale innbrudd i et datanettverk. Brannmur gir delvis poeng, da enkelte brannmurer kan inneholde *system for innbruddsdeteksjon*.
- **Spoofing** er å forfalske en avsender i kommunikasjon (phishing er å *fiske etter opplysninger*).
- **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.

## Oppgave 3.4 *Trusselmodellering og sikkerhetstiltak*

0.5 poeng for hvert riktige svar, -0.25 poeng for galt svar innad i hver deloppgave. Se forelesning og øvingsoppgaver for detaljer.

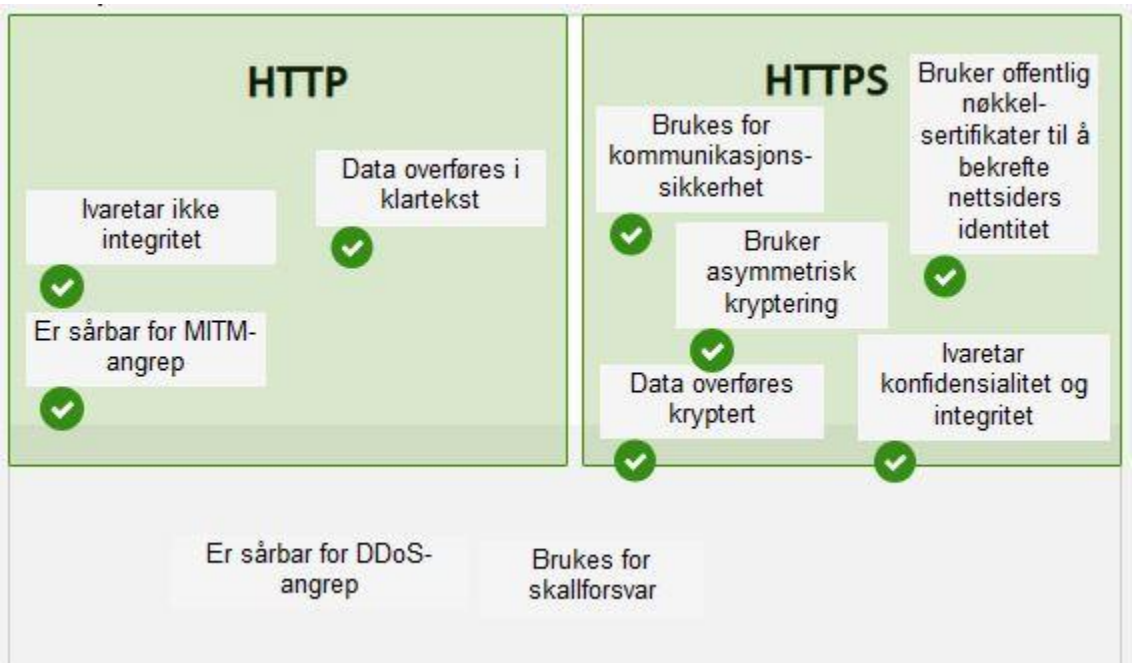
a) Å beskytte bedriftshemmelighetene er i dette tilfellet å sørge for *konfidensialitet***.**
b) Sikkerhetstiltak mot avlytting av nettverkstrafikk er bruk av sikre nettverksprotokoller (f.eks. HTTPS som krypterer datapakkene), ha autentiseringsmekanismer for oppkobling til det trådløse nettverket (dvs. ikke ha *åpent nett uten kryptert forbindelse* mellom wifi-ruter og enheten som kobler seg til,

hvor hvem som helst kan koble seg til). Det er også viktig å sørge for at programvaren i de trådløse aksesspunktene er oppdatert for å tette evt. nyoppdagede sårbarheter.

c) For å unngå datalekkasje som følge av sosial manipulasjon er det viktig å gi ansatte god opplæring for å unngå å bli lurt, altså kurse dem i informasjonssikkerhet. Et godt tiltak er også å sørge for at ansatte ikke har tilgang til informasjon de ikke har behov for tilgang til (prinsippet om *minste privilegium*) for å *minimere angrepsflaten* for denne typen angrep (minimere antall ansatte som kan lures til å lekke informasjon).

## Oppgave 3.5 *Egenskaper ved HTTP og HTTPS*

0.25 poeng for hvert riktige svar, -0.1 poeng for galt svar. Se forelesning og ukeoppgaver for detaljer, http og HTTPS er grundig gjennomgått.




- DDoS-angrep er angrep som forsøker å overbelaste kapasiteten til IT-tjenester eller nettverksinfrastruktur, ikke direkte angrep på *protokollene* (eller *egenskaper ved protokollene)*.
- *Skallforsvar* er å beskytte et segment av et nettverk mot uvedkommende, f.eks. ved å bruke en *brannmur* som all nettverkstrafikk inn/ut av nettverkssegmentet rutes gjennom.

## Oppgave 3.6 *Ulike typer kryptering*

0.33 poeng for riktig svar, ingen minuspoeng.

Se øvingsoppgaver og forelesning for detaljer, kryptering med hash-funksjoner, symmetrisk kryptering og asymmetrisk kryptering gjennomgås grundig.

Symmetrisk kryptering:

- Kalles også hemmelig nøkkel-kryptering, da samme hemmelige nøkkelen brukes til både kryptering og dekryptering.

Asymmetrisk kryptering:

- Bruker et *nøkkelpar*, altså én nøkkel for kryptering og en annen for dekryptering (nøkkelpar)
- I PKI brukes asymmetrisk kryptering med privat-offentlig nøkkelpar.

Hash-funksjoner:

- Vanligvis brukes ikke krypteringsnøkkel sammen med hash-funksjoner for å kryptere tekst til hash-verdi.
- Hash-funksjon er ikke-reverserbar, dvs. at resultatet (hash-verdien) ikke kan dekrypteres for å gjenskape den opprinnelige teksten.
- Annet navn på hash-funksjon er sjekksumalgoritme
- Bør være kollisjonsresistent, dvs. at to ulike tekster ikke kan resultere i samme hash-verdi.

Ingen av delene:

- Kryptovirus er en type skadelig programvare som krypterer informasjon for å gjøre det utilgjengelig for de som skal ha rettmessig tilgang.
- Autorisasjon er å *bestemme* hvem som skal ha tilgang til å gjøre hva.

## Oppgave 3.7 *PKI og kryptering*

0.5 poeng for riktig svar, -0.25 poeng for feil svar innad i hver deloppgave.

a) Oppgaven opplyser at nøkkelparet består av Jonas sin private og offentlige nøkkel. Jonas kjenner og kan bruke den private nøkkelen, mens Sylvi og Trygve kjenner og kan bruke den offentlige nøkkelen. Ved digital signatur kan den som kjenner den private nøkkelen *signere*, mens den som kjenner den offentlige nøkkelen kan *validere*.
b) Oppgaven opplyser at nøkkelparet består av Jonas sin private og offentlige nøkkel. Jonas kjenner og kan bruke den private nøkkelen, mens Sylvi og Trygve kjenner og kan bruke den offentlige nøkkelen. Ved kryptering av meldinger/dokumenter kan det som er kryptert med den offentlige nøkkelen dekrypteres med den tilhørende private nøkkelen.
c) Hovedformålet med en PKI er å sikre ektheten av offentlige nøkler og trygg nøkkeldistribusjon.
d) Et digitalt sertifikat knytter en offentlig nøkkel til en identitet, og sertifikatet signeres så av en sertifikatmyndighet.
e) Sertifikatmyndigheter utsteder og signerer digitale sertifikater.

## Oppgave 3.8 *Personopplysningsvern*

0.5 poeng for riktig svar, -0.25 poeng for feil svar innad i hver deloppgave.

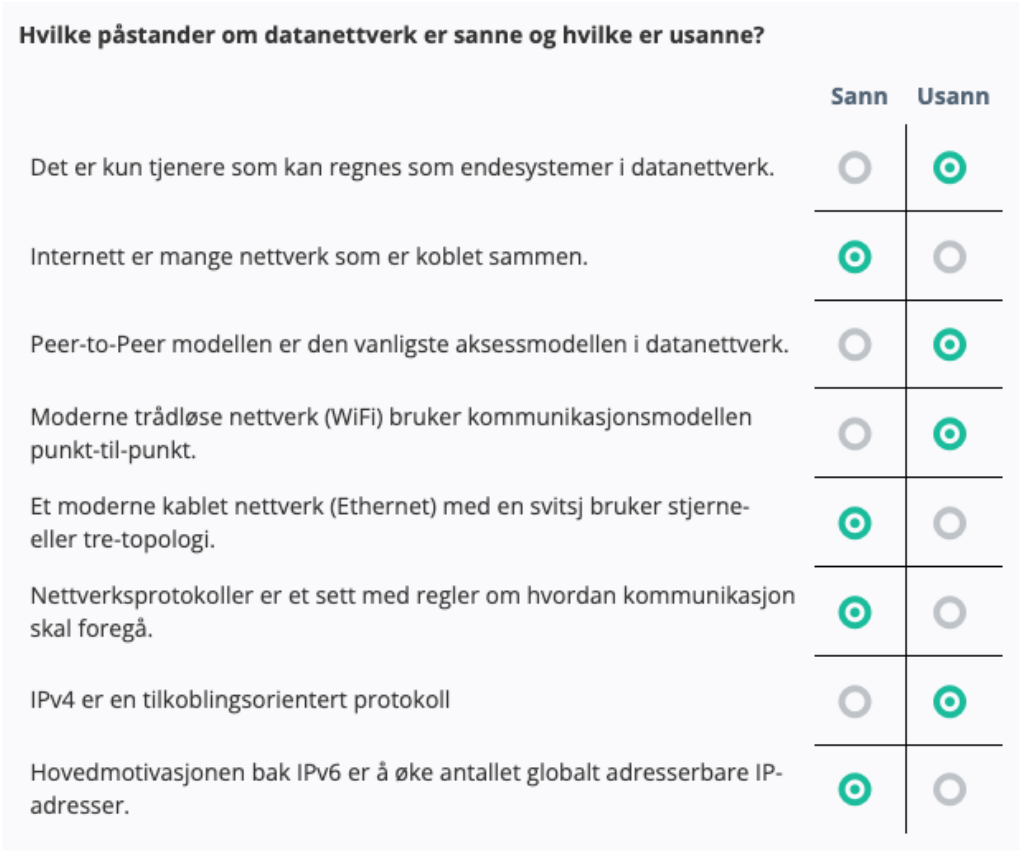
a) Helseopplysninger, Rasemessige eller etnisk opprinnelse, samt Fagforeningsmedlemskap går under særlig kategorier av personopplysninger.
b) Innebygd personvern er nødvendig for å sikre at systemene overholder personvernprinsippene, samt for å beskytte de registrertes rettigheter i behandling av personopplysninger.
c) Personopplysningsloven stiller krav til informasjonssikkerhet, den sier også at all behandling av personopplysninger skal skje med egnede tekniske og organisatoriske tiltak, samt at helseinstitusjonen (her *behandlingsansvarlig*) er juridisk ansvarlig for at data om pasienter behandles i samsvar med personopplysningsloven, også når *databehandler* av personopplysningene er en ekstern virksomhet (lagres og behandles hos en 3. part).

# Sensurveiledning IN1020 – Nettverk

Nettverksdelen i IN1020 gir ikke bonuspoeng. Det er åtte deloppgaver i seksjonen. På oppgaver med flervalg så gir feil svar -0.25, -0,5 eller -1 poeng avhengig av oppgaven.

## Oppgave 4.1 – Lett blanding- Nettverk

Dette er en sann/usann oppgave. Riktig svar gir 0,5 poeng, feil svar gir -0,5 poeng. Maks sum på oppgaven er 4 poeng.



**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. | ◉ | ○ |

## Oppgave 4.2 – Operativsystemer

Dette er en oppgave med flere svar. Riktig svar gir 1 poeng, feil svar gir -1 poeng. Maks sum på oppgaven er 3 poeng. Påstandene er hentet fra forelesningen om operativsystemer.

Riktige svar:
*En av hovedoppgavene til et operativsystem er å skjule detaljer om maskinvare for å gjøre det enklere å utvikle programmer.*

*En av hovedoppgavene til et operativsystem er å fordele resursene i datamaskinen.*

*Operativsystemer som nyere Windows og Linux er bygd opp etter monolittisk kjerne-modellen.*

## Oppgave 4.3 – Antall IP-adresser

Dette er også en oppgave hvor det kun er ett riktig svar. Rett svar gir 3 poeng.
I denne oppgaven er det viktig å huske at det er to IP-adresser som er reservert og ikke kan deles ut

Riktig svar:
*14*

## Oppgave 4.4 –CIDR til punktnotasjon

Her er kun ett svar riktig. Oppgaven gir 4 poeng.
For å finne punktnotasjon må vi se hvor mange 1'er bit som CIDR oppgir, altså 28. Oktetter med bare 11111111 vet vi er 255, så vi trenger kun å regne på siste oktett. 11110000 er 240.

Riktig svar:
*255.255.255.240*

## Oppgave 4.5– Subnett- og Broadcast-adresse.

I denne oppgaven er det også ett riktig svar. Oppgaven gir 3 poeng per svar, 6 totalt.

Første skritt er å regne om IP og nettmaske til binært.
For å finne adresse til subnettet gjør man en logisk AND operasjon.
Broadcast-adresse finner man ved å invertere nettmasken og gjøre en logisk OR operasjon.

Riktig svar subnettadresse:
*192.168.100.160*

Riktig svar kringkastningsadresse:
*192.168.100.175*

## Oppgave 4.6 – Transportlagsprotokoller

Dette er en sann/usann oppgave. Riktig svar gir 0,25 poeng, feil svar gir -0,25 poeng. Maks sum på oppgaven er 2 poeng.

**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. | ○ | ◉ |
| TCP er en tilkoblingsorientert protokoll. | ◉ | ○ |
| UDP er en rask protokoll, og egner seg derfor godt til overføring av store filer. | ○ | ◉ |
| Det er ikke mulig å bruke kryptering på applikasjonslaget når vi bruker UDP. | ○ | ◉ |
| Metningskontroll sørger for at kapasiteten i nettverket blir delt på alle forbindelsene. | ◉ | ○ |
| UDP er den mest brukte av de to protokollene i transportlaget. | ○ | ◉ |
| Både TCP og UDP støtter multipleksing ved hjelp av porter. | ◉ | ○ |

## Oppgave 4.7 – HTTP

Her kan man få 1 poeng. 1 poeng per riktig svar og -1 poeng for feil svar. Det er kun ett riktig svar på oppgaven. Oppgaven er hentet fra forelesningen «Tjenester i Internett»

Riktig svar:
*Den samme TCP-forbindelsen blir gjenbrukt til flere runder med nye HTTP-forespørsler.*

## Oppgave 4.8 – HTTP-streaming

Flervalgoppgave. Maks 2 poeng. 1 poeng per riktig svar. Feil svar gir -1 poeng.

Riktige svar:
- *Video deles opp i små segmenter og forskjellige kvaliteter.*
- *Det er klienten som bestemmer kvaliteten som lastes ned, ikke tjeneren.*