

## i Informasjon

# Eksamen IN1020 høsten 2022

### Tid

12. desember kl. 15:00-19:00  
Faglærerne vil gå en runde fra 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

Oppgavene er ulike varianter av flervalgsoppgaver. 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 mister 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.

En enkel kalkulator uten kommunikasjonsmulighet.

I tillegg vil en "on screen"-kalkulator være tilgjengelig i Inspira-systemet, under oppgavelinjen.

## i 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 og 1.7 er en del av seksjon 1.

## 1.1 HTML Fargekoder

HyperText Markup Language (HTML) er et markeringsspråk for formatering av nettsider der man blant mye annet kan vise tekst i forskjellige farger. I HTML representeres farger med en rød (R), grønn (G) og blå (B) verdi - såkalt RGB. Disse er vanligvis angitt i hexadesimal notasjon, der den første byten (fra venstre) er rød, den andre er grønn, og den tredje er blå.

Hvilke verdier for rød, grønn og blå har fargekoden 0xA07CD1?



Velg ett eller flere alternativer

- rød=148, grønn=124, blå=209
- rød=148, grønn=128, blå=191
- rød=160, grønn=124, blå=209
- rød=160, grønn=134, blå=179



---

Maks poeng: 1

## 1.2 2'er Komplement - variant 2

Du har følgende to bytes:

Byte A:

0	1	0	0	1	1	0	0
---	---	---	---	---	---	---	---

Byte B:

0	1	0	1	0	0	0	1
---	---	---	---	---	---	---	---

Regn ut en ny byte C som er summen av disse ( $C = A + B$ ). Hvilke verdier kan C ha?

Velg ett eller flere alternativer

157



126

-67

-99




---

Maks poeng: 3

## 1.3 Tallsystemer

Konverter til desimal (10-tall) systemet.

a)  $1101_2$  Velg alternativ ▼ (13, 51, 23, 135, Ingen av disse)

b)  $113_4$  Velg alternativ ▼ (23, Ingen av disse, 51, 13, 135)

c)  $0x33$  Velg alternativ ▼ (51, 135, 13, Ingen av disse, 23)

d)  $207_8$  Velg alternativ ▼ (51, 23, Ingen av disse, 135, 13)

---

Maks poeng: 5

## 1.4 Godt og Blandet

Sett riktig eller galt for påstandene under.

	Riktig	Galt
En maskin som er bygget på von neumann arkitektur har både kode og data i samme minne.	<input checked="" type="radio"/>	<input type="radio"/>
DAT er en vanlig instruksjon som LMC forstår.	<input type="radio"/>	<input checked="" type="radio"/>
Én byte kan representere 512 unike verdier.	<input type="radio"/>	<input checked="" type="radio"/>
ASCII har plass til 128 unike kontroll- eller karakter-symboler.	<input checked="" type="radio"/>	<input type="radio"/>
ASCII oversettes enkelt til UTF8 ved å sette det øverste bitet til null.	<input checked="" type="radio"/>	<input type="radio"/>
Vektorgrafikk er et vel egnet format for å lagre bilder tatt med smart-telefon.	<input type="radio"/>	<input checked="" type="radio"/>
LMC har totalt tre interne registre: program-teller, instruksjonsregister, og akkumulator.	<input type="radio"/>	<input checked="" type="radio"/>
LMC forstår totalt 9 forskjellige instruksjonstyper.	<input checked="" type="radio"/>	<input type="radio"/>

Maks poeng: 5

## 1.5 LMC-1

```

      INP
      STA a
      INP
      BRZ print
      LDA a
      SUB b
      STA a
print  LDA a
      OTC
      HLT
a      DAT
b      DAT 32
```

Hva skrives ut når denne koden kjøres og bruker gir følgende inndata: **114** og **999**?

**Velg ett eller flere alternativer**

- r
- T
- 999
- R
- q



---

Maks poeng: 3

## 1.6 LMC-2

```

                INP
                STA a
                INP
                STA b
loop           LDA a
                INSTRUKSJON 1
                INSTRUKSJON 2
                INSTRUKSJON 3
                INSTRUKSJON 4
                LDA a
                SUB en
                STA a
                BRA loop
slutt         LDA res
                OUT
                HLT
res           DAT 0
a             DAT
b             DAT
en           DAT 1

```

Du lager et lite program for å gange sammen to tall **a** og **b**, slik at

$res = a * b$

Du har skrevet programmet over, men det mangler noen instruksjoner. Hvilke?

Instruksjon 1:

Velg alternativ ▼ (BRZ slutt, BRA slutt, BRP slutt)

Instruksjon 2:

Velg alternativ ▼ (LDA b, STA a, LDA a, LDA res)

Instruksjon 3:

Velg alternativ ▼ (ADD en, ADD b, ADD a, ADD res)

Instruksjon 4:

Velg alternativ ▼ (Ingen instruksjon, STA res, STA b, STA a)

Maks poeng: 5

## 1.7 LMC-3

start	INP	00	INP
	BRZ slutt	01	BRZ 13
	STA in	02	STA 27
	LDA laster	03	LDA 28
	ADD in	04	ADD 27
	STA loop	05	STA 06
loop	HLT	06	HLT
	BRZ start	07	BRZ 00
	OTC	08	OTC
	LDA loop	09	LDA 06
	ADD en	10	ADD 26
	STA loop	11	STA 06
	BRA loop	12	BRA 06
slutt	HLT	13	HLT
lmc	DAT 76 // L	14	DAT 76
	DAT 77 // M	15	DAT 77
	DAT 67 // C	16	DAT 67
	DAT 0 // NULL	17	DAT 00
jul	DAT 74 // J	18	DAT 74
	DAT 117 // u	19	DAT 117
	DAT 108 // l	20	DAT 108
	DAT 0 // NULL	21	DAT 00
ifi	DAT 73 // I	22	DAT 73
	DAT 70 // F	23	DAT 70
	DAT 73 // I	24	DAT 73
	DAT 0 // NULL	25	DAT 00
en	DAT 1	26	DAT 01
in	DAT	27	DAT 00
laster	LDA 0	28	LDA 00

Koden over skriver ut én og én karakter fra ønsket adresse inntil en "null" leses fra minnet.

Etter å ha tastet inn "14", taster brukeren inn "18" og så "0". Hvilken tekst skrives ut?

("IFI" og ikke noe mer., "LMC", "Jul", og ikke noe mer.,  
 Programmet kræsjer., "IFI", "Jul", og ikke noe mer.)

Hvilken maskinkode finner vi på etikett **loop** etter at den sjette instruksjonen har blitt eksekvert?

(500, 914, 518, 906, 300, 514)

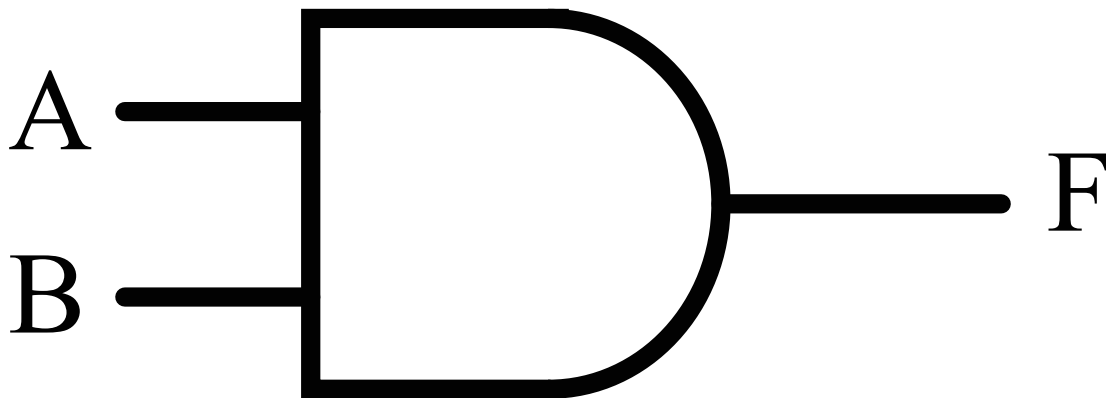
Maks poeng: 3

## i 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 Gates



Hvilke(n) port er avbildet over:  
**Velg ett eller flere alternativer**

- XNOR-port
- XOR-port
- AND-port
- NOR-port
- NAND-port
- OR-port
- NOT-port

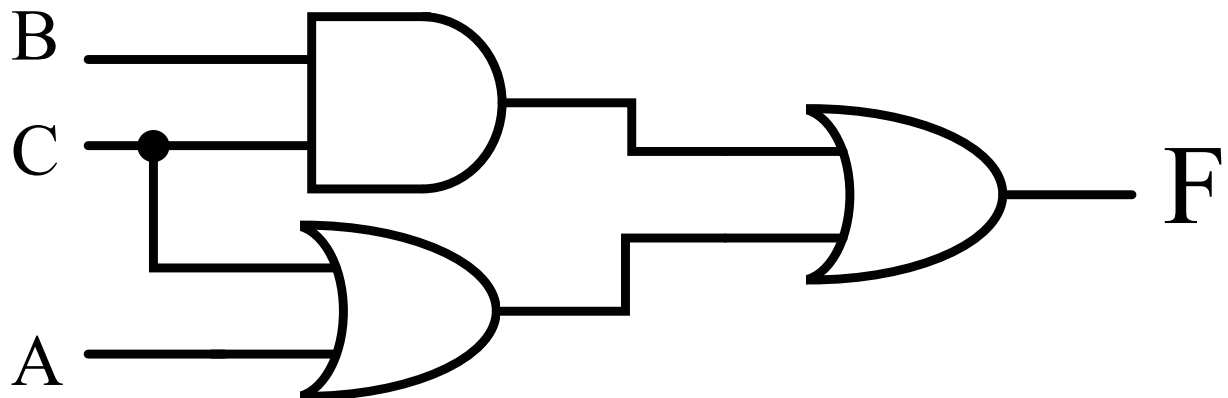


---

Maks poeng: 1



## 2.2 Kretsanalyse



Funksjonen F er gitt som:

**Velg ett eller flere alternativer**

- $F = AB$
- $F = A + B$
- $F = A + BC$
- $F = C + AB$
- $F = AC$
- $F = BC$
- $F = B + C$
- $F = ABC$
- $F = A + B + C$
- $F = A + C$
- $F = C + A$
- $F = B + AC$



Maks poeng: 5

## 2.3 Cache

Anta at det er igjen 3000 instruksjoner og at en instruksjon tar 1 klokkesykel, bortsett fra eventuelle cache-miss. Videre kan du anta at det vil være 50% cache-miss hvor det vil ta totalt 4 klokkesykel for hver instruksjon i cache-miss.

Hvor lang til vil det totalt ta?

**Velg ett eller flere alternativer**

- 7500 ✓
- 15000
- 8250
- 10000
- 9000
- 13250
- 5500
- 3000
- 6600
- 5000

---

Maks poeng: 3

## 2.4 Godt og blandet H2022

Er utsagnene sann eller usann?

	Sann	Usann
En transistor er en samling av strøm som utgjør 1 byte	<input type="radio"/>	<input checked="" type="radio"/>
Sekundærminne er flyktig minne	<input type="radio"/>	<input checked="" type="radio"/>
ALU ligger rett på utsiden av CPU	<input type="radio"/>	<input checked="" type="radio"/>
Når du får cache-miss betyr det at en del av minne er blitt ødelagt	<input type="radio"/>	<input checked="" type="radio"/>
Et register består av mange RAM	<input type="radio"/>	<input checked="" type="radio"/>
En databuss (BUS) frakter med seg informasjon mellom prosessoren og andre enheter	<input checked="" type="radio"/>	<input type="radio"/>
Den teknologiske utviklingen bidrar til færre transistorer på en chip	<input type="radio"/>	<input checked="" type="radio"/>
En full-adder kan brukes som subtraktor ved å ha mente-inn = 1	<input type="radio"/>	<input checked="" type="radio"/>
Klokkesignalet i en CPU er lagret i RAM	<input type="radio"/>	<input checked="" type="radio"/>
En 64-bits ALU krever 65 stk av 1-bits ALU	<input type="radio"/>	<input checked="" type="radio"/>

Maks poeng: 8

## 2.5 Pensum H2022

Hvilke av temaene under er en del av årets pensum? Dra-og-slipp temaene inn i de representative grå områdene. Du kan fint legge temaene oppå hverandre.

Ikke del av pensum  
Not part of curriculum

Med i årets pensum  
Within this years curriculum

Cache XOR Transistor

RAM CPU BUS Decoder

Karnaugh diagram ALU Multiplexor

Styresignal

Maks poeng: 3

## 2.6 Abstraksjonsnivå H2022

Plasser disse elementene i riktig rekkefølge med hensyn på abstraksjonsnivå

Høyeste nivå:  (Pipeline, STA 04, Transistor, Register)

(Transistor, STA 04, Register, Pipeline)

(Transistor, Pipeline, Register, STA04)

Laveste nivå:  (STA 04, Pipeline, Transistor, Register)

---

Maks poeng: 5

## i Seksjon 3

Du er nå i seksjon 3 - Sikkerhet.

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

### 3.1 Sikkerhetsmål

Sikkerhetsmål er et sentralt begrep innen informasjonssikkerhet. Hvilke av følgende defineres som sikkerhetsmål:

**Velg ett eller flere alternativer**

- Integritet ✓
- Autorisering
- Uavviselighet ✓
- Brannmur
- Tilgjengelighet ✓
- Orm
- Tilgangskontroll
- Tofaktor-autentisering

---

Maks poeng: 2

### 3.2 Sikkerhetstiltak: Konfidensialitet

Konfidensialitet er et sentralt krav i norsk personvernlovgivning. Hvilke av følgende sikkerhetstiltak kan sørge for å ivareta konfidensialitet for persondata som behandles i et IT-system:

**Velg ett eller flere alternativer**

- Bruk av kryptografi for data lagret i systemet ✓
- Bruk av skallforsvar ✓
- Sørge for redundante tjenester
- Sørge for sikkerhetskopi av alle data
- Identifisere alle brukere av IT-systemet
- Sørge for sikkerhetskopi av all maskinvare

---

Maks poeng: 2

### 3.3 Sikkerhetstiltak: Integritet

Integritet er et sentralt krav i norsk personvernlovgivning. Hvilke av følgende sikkerhetstiltak kan sørge for å ivareta integriteten for persondata som behandles i et IT-system:

**Velg et eller flere alternativer**

- Sørge for redundante tjenester
- Identifisere alle brukere av IT-systemet
- Sørge for sikkerhetskopi av maskinvaren
- Kryptere all nettverkstrafikk til, fra og internt i datasystemet. ✓
- Holde all programvare godt sikkerhetsoppdatert ✓
- Ha gode rutiner for tilgangskontroll i IT-systemet ✓

---

Maks poeng: 2

### 3.4 Autentisering

Hvordan kan tofaktor-autentisering med en kombinasjon av autentiseringsfaktorene *Noe man vet* og *Noe man har* for innlogging bidra til å forbedre sikkerheten i et IT-system?

**Velg ett eller flere alternativer**

- Det gjør det vanskeligere for angripere å utnytte brukerinformatjon lekket i f.eks. phishing-angrep. ✓
- Det begrenser hva brukerne har lov til å gjøre i et IT-system.
- Det gjør det vanskelig å lykkes med såkalte brute-force angrep. ✓
- Det gjør det unødvendig å ytterligere sikre data lagret i IT-systemet.

---

Maks poeng: 3



### 3.5 Symmetrisk kryptering

Symmetrisk kryptering er en av flere kategorier kryptering som benyttes innen databasert kryptografi.

**Hvilke påstander om symmetrisk kryptering er sanne og hvilke er usanne?**

	Sant	Usant
Benyttes til kryptering av hemmelige meldinger.	<input checked="" type="radio"/>	<input type="radio"/>
Baserer seg på bruk av et nøkkelpar bestående av en privat og en offentlig kryptografisk nøkkel.	<input type="radio"/>	<input checked="" type="radio"/>
Symmetrisk kryptering ødelegger meldingen slik at den aldri kan dekrypteres	<input type="radio"/>	<input checked="" type="radio"/>
Benyttes til såkalt digital signatur.	<input type="radio"/>	<input checked="" type="radio"/>
Sender og mottager deler én felles, hemmelig kryptografisk nøkkel.	<input checked="" type="radio"/>	<input type="radio"/>
Trygg utveksling av den hemmelige kryptografiske nøkkelen er en sikkerhetsutfordring.	<input checked="" type="radio"/>	<input type="radio"/>
Kan brukes for å sikre konfidensialitet for data.	<input checked="" type="radio"/>	<input type="radio"/>
Kan brukes for å sikre uavviselighet.	<input type="radio"/>	<input checked="" type="radio"/>

Maks poeng: 4

### 3.6 Asymmetrisk kryptering

Virksomheten du jobber i har behov for sterk sikkerhet og autentisitet til data og meldinger, og har innført en egen, lokal *offentlig-nøkkel infrastruktur* (PKI). Alle ansatte har fått tilordnet et kryptografisk nøkkelpar, bestående av en privat og en offentlig nøkkel. Siden du har tatt emnet IN1020, blir det din oppgave å forklare for kollegaene dine hvilke nøkler som skal benyttes til hvilke operasjoner.

**For hver operasjon nedenfor angi riktig nøkkel:**

Nøkkel sender benytter til *signering* (digital signatur):  (Senders offentlige nøkkel, Mottagers offentlige nøkkel, **Senders private nøkkel**, Mottagers private nøkkel).

Nøkkel mottager benytter for *validering* (digital signatur):   
(Mottagers private nøkkel, Senders private nøkkel, **Senders offentlige nøkkel**, Mottagers offentlige nøkkel)

Nøkkel sender benytter for *kryptering* (utveksling av hemmelig melding):

(Senders offentlige nøkkel, Mottagers private nøkkel, **Mottagers offentlige nøkkel**, Senders private nøkkel)

Nøkkel mottager benytter for *dekryptering* (utveksling av hemmelig melding):

(Mottagers offentlige nøkkel, Senders private nøkkel, **Mottagers private nøkkel**, Senders offentlige nøkkel)

---

Maks poeng: 3

### 3.7 Personvern og trusselmodellering

Viken fylkeskommune vil innføre et nytt digitalt system for gjennomføring av avsluttende skriftlig eksamen for elever i videregående skole.

En av løsningene de vurderer er en sky-tjeneste fra en ekstern IT-leverandør, tilgjengelig for elever, sensorer og skoleadministrasjonen som en web-applikasjon. Både lagring av data og kjøring av applikasjonen skjer på leverandørens datautstyr som står fysisk plassert i et EU-land, mens selve eksamen gjennomføres i en nettleser på skolens datamaskiner i skolens lokaler.

Eksamenssystemet må inneholde nok informasjon til å entydig identifisere elever og sensorer (personnummer, navn, kandidatnummer), elevenes besvarelser, samt sensors begrunnelse og karakter for hver enkelt eksamensbesvarelse vedkommende sensurerer.

#### Oppgave A)

Fylkeskommunen må vurdere krav til *personopplysningsvern* (GDPR), og du skal hjelpe dem på vei. Vurder følgende utsagn, og kryss av de som er korrekte med utgangspunkt i bruken av et eksamenssystem som beskrevet over:

#### Velg ett eller flere alternativer:

- Fylkeskommunen er ikke juridisk ansvarlig for at opplysninger om elever behandles i samsvar med personopplysningsloven, da eksamenssystemet i sin helhet er levert av et eksternt firma.
- Elevene har rett til innsyn i hvilke personopplysninger som er lagret om dem. ✓
- Personopplysningsloven stiller krav til informasjonssikkerhet; Konfidensialitet, integritet og tilgjengelighet. ✓
- Fylkeskommunen kan se bort fra personopplysningsloven for behandling av personopplysninger, siden det er helt nødvendig å behandle data om elever for å gjennomføre eksamen.

#### Oppgave B)

Det neste som bekymrer fylkeskommunen er *integritet* til dataene i eksamenssystemet. At f.eks. eksamensbesvarelser eller karakterer endres av uvedkommende. Hvilke av følgende kan utgjøre en trussel mot *integritet*, gitt opplysningene over:

**Velg ett eller flere alternativer**

- Rootkit* installert på en eksamenssensers datamaskin. ✓
- Dårlig kompetanse om informasjonssikkerhet hos selskapet som leverer eksamensløsningen. ✓
- Bruk av passord som eneste autentiseringsfaktor. ✓
- Man-in-the-middle-angrep* på nettverkstrafikken. ✓
- Mangel på redundante tjenester.
- Utgjengelighetsangrep fra utenforstående med ondsinnede hensikter.

---

Maks poeng: 9

**i Seksjon 4**

Du er nå i seksjon 4 - **Datanettverk**.

Oppgave nr 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8 og 4.9 er en del av seksjon 4.

**4.1 Klient-tjener**

Hva kjennetegner aksessmodellen klient-tjener?

**Velg ett eller flere alternativer**

- Nodene kan være både klient og tjener samtidig.
- Mange uavhengige noder samarbeider om å tilby en tjeneste.
- En klient initierer utvekslingen ved å koble til en tjener og spørre om å få utført en tjeneste. ✓
- En tjener lytter etter henvendelser og leverer tjenester på forespørsel. ✓
- Det finnes ingen sentralisert kontroll over tjenesten.

---

Maks poeng: 2

## 4.2 Linjeswitching

Hva er sant for et linjeswitchet nettverk?

Velg ett eller flere alternativer

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

---

Maks poeng: 2

## 4.3 Overføringshastighet

Du ønsker å laste ned en fil på 150 megabyte, og hastigheten på din Internettlinje er 50 megabit per sekund ned og 20 megabit per sekund opp. Hva er den teoretisk korteste overføringstiden?

Velg ett alternativ:

- 150 sekunder
- 60 sekunder
- 3 sekunder
- 7,5 sekunder
- 24 sekunder ✓

---

Maks poeng: 3

#### 4.4 Punktnotasjon til CIDR

En datamaskin har IP-adressen 172.16.100.18

Nettverksmasken er: 255.255.255.248

Hva er IP-adressen til maskinen i CIDR-notasjon?

**Velg ett alternativ:**

- 172.16.100.1/26
- 172.16.100.18/26
- 172.16.100.1/29
- 172.16.100.18/29



---

Maks poeng: 3

#### 4.5 Antall IP-adresser

Et subnett har nettverksmasken 11111111.11111111.11111111.11111000

Hvor mange gyldige IP-adresser kan tildeles verter i subnettet?

**Velg ett alternativ:**

- 8
- 6
- 32
- 30
- 256



---

Maks poeng: 2

## 4.6 Broadcast-adresse

Du har en maskin med følgende IP-adresse i CIDR-notasjon: 172.16.10.112/26

Hva er broadcast-adressen i dette subnettet?

**Velg ett alternativ:**

- 172.16.10.1
- 172.16.10.255
- 172.16.10.64
- 172.16.10.127
- 172.16.10.63
- 172.16.1.255



---

Maks poeng: 5

## 4.7 IPv6

Hva er hovedmotivasjonen ved å bytte ut IPv4 med IPv6?

**Velg ett alternativ**

- Lettere å koble sammen IP-adresser og MAC-adresser
- Det blir flere tilgjengelige porter per IP-adresse
- Øke antallet globalt adresserbare IP-adresser
- Gjøre det vanskeligere å utføre "man-in-the-middle" angrep.



---

Maks poeng: 2

## 4.8 Transportlagsprotokoller

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

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

	Sant	Usant
Både TCP og UDP sørger for at data kommer frem i riktig rekkefølge.	<input type="radio"/>	<input checked="" type="radio"/>
UDP er en rask protokoll, og egner seg derfor godt til overføring av store filer.	<input type="radio"/>	<input checked="" type="radio"/>
TCP er den mest brukte av de to protokollene i transportlaget.	<input checked="" type="radio"/>	<input type="radio"/>
Transportlaget forholder seg kun til ende-til-ende, og har ingen kjennskap om hvordan data sendes på nettet.	<input checked="" type="radio"/>	<input type="radio"/>
Det er ikke mulig å bruke kryptering på applikasjonslaget når vi bruker UDP.	<input type="radio"/>	<input checked="" type="radio"/>
TCP er en tilkoblingsorientert protokoll.	<input checked="" type="radio"/>	<input type="radio"/>
Metningskontroll sørger for at kapasiteten i nettverket deles på alle forbindelsene.	<input checked="" type="radio"/>	<input type="radio"/>
Flytkontroll sørger for at TCP ikke sender data raskere enn hva nettet har kapasitet til.	<input checked="" type="radio"/>	<input type="radio"/>

Maks poeng: 4



## 4.9 HTTP-streaming

Hvilke utsagn stemmer om streaming av video over HTTP?

**Velg ett eller flere alternativer**

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

---

Maks poeng: 2