

i Informasjon

UNIVERSITETET I OSLO

Det matematisk-naturvitenskapelige fakultet

Skriftlig eksamen i IN1020

2023 HØST

Varighet: 11.desember kl. 09:00-13:00

Tillatte hjelpemidler: Alle trykte og skrevne hjelpemidler.

En kalkulator er tilgjengelig i Inspira (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 10:00.

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 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.

Tilgjengelige ressurser i Inspira

- Enkel kalkulator
- Ascii-tabellen

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, 1.7 og 1.8 er en del av seksjon 1.

1.1 Dataformater

Under ser du eksempler på forskjellige ting man kan lagre i en datamaskin. Dra beskrivelsene til passende filtype for lagring i en datamaskin.

JPEG	GIF	H264
PNG	ASCII	Post script
MP3	HTML	UTF8

En komplisert logo av kun rette linjer og sirkler.

En film.

Et bilde som skal lagres uten tap av informasjon.

En liten sekvens (video) av noen få, små bilder som sendes over nettet.

En webside.

Et lydklipp.

En ordbok fra japansk til kinesisk.

En tekst som kun inneholder bokstavene A til Z.

Et stort bilde som lagres på en datamaskin med lite lagringsplass.

Maks poeng: 4.5

1.2 2'er Komplement

Du får oppgitt følgende byte:

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

Hvilke verdier kan denne representere?

Velg ett eller flere alternativer

- ☐ -30
- ☐ -45
- ☐ 132
- ☐ 190
- ☐ 172
- ☐ -68
- ☐ -84

Maks poeng: 2

1.3 Filtillatelser

User			Group			Other		
Read	Write	Execute	Read	Write	Execute	Read	Write	Execute

Alice har laget en fil "ferieplaner.py" på sin Linux maskin. Hun har gitt fila følgende (oktale) tillatelser:

774₈

Hvilke av følgende utsagn er riktig eller feil?

Finn de som passer sammen:

	Riktig	Galt
Andre brukere kan kun eksekvere filen.	☐	☐
Eier av filen kan lese og skrive, men ikke eksekvere filen.	☐	☐
Gruppe-eierne av filen kan lese og eksekvere filen.	☐	☐

Maks poeng: 1.5

1.4 Konvertering

Regn om 765_{10} til heksadesimal representasjon.

Angi svaret ved å dra de hexadesimale sifferne til riktige plasseringer.

0x



0	1	2	3	4	5	6	7
8	9	A	B	C	D	E	F

Maks poeng: 3

1.5 Tallsortering

Under får du oppgitt fire bytes på binærform. Disse representerer heltall lagret på toerkomplement-formen. Sortér tallene i økende rekkefølge (økende rekkefølge er fra venstre til høyre):

Minst / Smallest

Størst / Largest

00010110₂ < 00000000₂ < 10000000₂ < 10010000₂

Maks poeng: 5

1.6 LMC - Aritmetikk

Hva skriver LMC ut dersom bruker gir input **5** og så **1**?

	INP
	STA a
	INP
	ADD a
	SUB v
	OUT
	HLT
a	DAT
v	DAT 2

Velg ett alternativ:

- ☐ 5
- ☐ 4
- ☐ 2
- ☐ -2
- ☐ -1

Maks poeng: 2

1.7 LMC - ASCII

Du får oppgitt følgende program for LMC:

```
LDA 90  
OTC  
LDA 91  
OTC  
LDA 90  
OTC  
LDA 92  
OTC  
HLT
```

Initialisør minnet slik at **"IFI2"** skrives ut når koden kjøres.



Maks poeng: 3

1.8 LMC - Programflyt

	INP
	BRP fin
	STA v
	SUB v
	SUB v
fin	OUT
	HLT
v	DAT

Programmet ovenfor skriver ut **2**. Hva kan bruker ha gitt som **input** til LMC?

Velg ett eller flere alternativer

- ☐ -2
- ☐ 3 og så 1
- ☐ 2
- ☐ -1
- ☐ 5
- ☐ 4

Maks poeng: 3

1.9 LMC - Selvmodifiserende kode

Du får oppgitt følgende kode for LMC:

start	INP	00	INP
	ADD jump	01	ADD 03
	STA jump	02	STA 03
jump	DAT 600	03	DAT 600
	LDA a	04	LDA 10
	OTC	05	OTC
	BRA start	06	BRA 00
	LDA b	07	LDA 11
	OTC	08	OTC
	BRA start	09	BRA 00
a	DAT 35 // '#'	10	DAT 35
b	DAT 94 // '^'	11	DAT 94

Hva må bruker gi som input for å få skrevet ut "^^" og så stanse?

Første input:

Andre input:

Tredje input:

Maks poeng: 4

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 Kretsanalyse 23

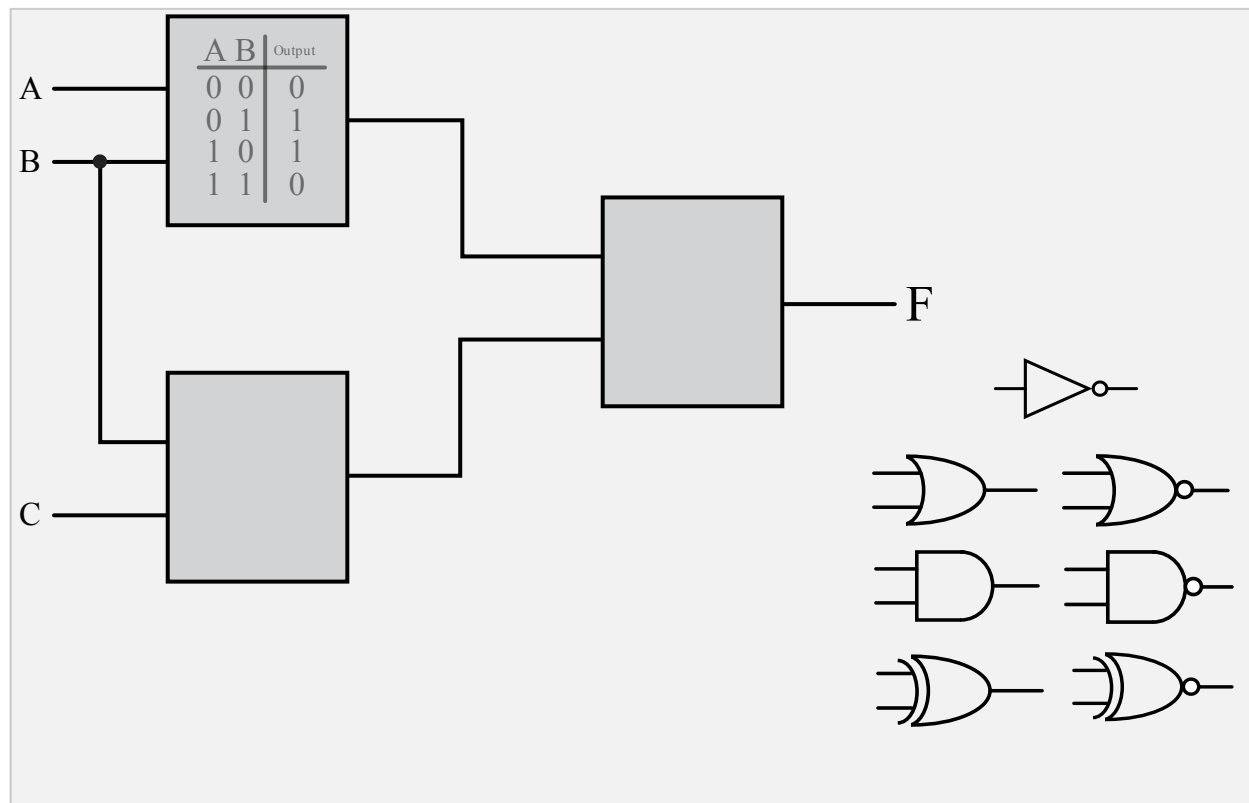
Kretsen har funksjonen

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

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

Hint! Husker du de ulike symbolene for et funksjonsuttrykk som er invertert?

Hint! I den ene gråboksen er sannhetsverditabellen til porten oppgitt.



Maks poeng: 5

2.2 Minne 23

I denne oppgaven skal du arbeide med en spesifikk datamaskin som har et hierarki av minneelementer bestående av registre, en fire-nivås cache, RAM og en flash-drive (minnepenn). Maskinens minnehierarki er utformet for å håndtere forskjellige dataaksess- og skriveoperasjoner med varierende hastigheter.

I henhold til informasjon levert av produsenten, har cache-hierarkiet følgende karakteristikk:

- Leseoperasjoner tar 5 klokkesykler per nivå i cache.
- Skriveoperasjoner tar 10 klokkesykler per nivå i cache.

Videre har du informasjon om de andre minneelementene:

- Leseoperasjoner fra RAM har en tilgangstid på 50 klokkesykler.
- Skriveoperasjoner til RAM har en tilgangstid på 100 klokkesykler.
- Leseoperasjoner fra Flash-drive (minnepenn) tar 760 klokkesykler.
- Skriveoperasjoner fra Flash-drive (minnepenn) tar 1120 klokkesykler.

HINT! For hver minneaksess operasjon, vær oppmerksom på at de oppgitte verdiene er en 'økt' tilgangstid.

Fyll ut riktig verdi i feltene (kun heltall):

(a) Hva er total antall klokkesykler i forsinkelse når du får cache-hit på nivå 3?

klokkesykler

(b) Hva er total antall klokkesykler det tar å skrive en verdi som er endret i pipeline tilbake til RAM?

klokkesykler

c) Anta at en optimalisering tillater at cache-nivå 1 og 2 kan oppdateres i parallell, mens de øvrige nivåene fortsatt krever sekvensiell oppdatering. Hva vil være den nye totale klokkesykel-forsinkelsen for å skrive en verdi til RAM?

klokkesykler

(d) Du skal beregne hvor mange klokkesykler det totalt vil ta å gjennomføre 100 instruksjon hvor det tar 1 klokkesykel per instruksjon uten minneaksessering. Ettersom du er ekspert på å lage gode programmer og kan masse om minnehierarki har du klart å lage rekkefølgen for instruksjonene dine slik at de som akssesserer minne alltid vil ha cache-hit på nivå 1. Hvor mange klokkesykler vil det hele ta når du forventer 20%

minneaksessering?

klokkesykler

Maks poeng: 5

2.3 Abstraksjonnivå 23

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

Høyeste	Velg alternativ (2 invertere, Volt, Pipeline, Register, logiske verdier)
	Velg alternativ (2 invertere, Pipeline, Logiske verdier, Register, Volt)
	Velg alternativ (2 invertere, Logiske verdier, Pipeline, Volt, Register)
	Velg alternativ (Pipeline, Register, 2 Invertere, Logiske verdier, Volt)
Laveste	Velg alternativ (Register, Pipeline, 2 Invertere, Volt, Logiske verdier)

Maks poeng: 3

2.4 Godt og blandet 23

Hvilke av disse utsagnene er sanne?

- ☐ Man kan lage enhver funksjon med å bare ha INV og OR
- ☐ Inngangen og utgangen på en inverter er fysisk koblet sammen.
- ☐ ALU står for Adder-Logikk-Unit
- ☐ Det er ikke mulig å ha et oddeantall trinn i en pipeline
- ☐ Det finnes bare en type transistorer.
- ☐ En utgang av en port kan være inngang på flere porter
- ☐ Det er kun en utgang på en port
- ☐ En XNOR er det inverterte av en XOR

Maks poeng: 4

2.5 Datapath 23

Velg de riktige alternativene for hvordan en instruksjon prosesseres.

HINT! husker du forelesningen "Pipeline" og "kretser som driver koden"?

Det er (Cache, BUS, ALU, PC) som har adressen til neste instruksjon.

Nå værende instruksjon blir i dekode-fasen (lagret, splittet opp, addert sammen, byttet).

Styresignalet til (GPU, ALU, RAM, CPU, PC) kommer fra (WB-steget, EX-steget, IF-steget, DE-steget).

I WB-steget sendes resultatet via en (BUS, Inverter, Klokke, CPU).

Maks poeng: 5

2.6 ALU 23

Gitt en ALU som skal gjøre følgende operasjoner:

Addere,
NAND,
XOR,
NOR,
XNOR

(a) Hvor mange bit må styresignalet være? bit.

(b) Hvor sikker er du på svaret ditt i (a)?

Her har du 100 % å dele ut fordelt på disse alternativene. MERK! du må fylle ut et tall i alle alternativene. Der du er helt sikker på at det er feil så fyller du ut 0, mens der du er sikker (eller usikker) på at det er riktig kan du fylle ut med et tall mellom 1-100.

svaret er 1 bit

svaret er 2 bit

svaret er 3 bit

svaret er 4 bit

svaret er 5 bit

Maks poeng: 3

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 Brudd på sikkerhetsmål

Angi hvilket sikkerhetsmål som typisk brytes som resultat av hvert av følgende angrep:

Finn de som passer sammen:

	Autentisitet	Integritet	Tilgjengelighet	Konfidensialitet
Løsepengevirus	☐	☐	☐	☐
Identitetstyveri	☐	☐	☐	☐
DDoS-angrep	☐	☐	☐	☐
DNS-modifisering	☐	☐	☐	☐
Spionprogramvare	☐	☐	☐	☐
Forfalskning av nettside	☐	☐	☐	☐

Maks poeng: 3

3.2 Sikkerhetsmål og sikkerhetstiltak

Du er deltager i et IT-prosjekt som utvikler et nytt digitalt pasientsystem for en gruppe privatpraktiserende psykologer. Systemet vil inneholde pasientopplysninger. Oppgaven din er å rådgi prosjektledelsen om nødvendige sikkerhetstiltak for pasientsystemet.

a) Aller først skal du identifisere sikkerhetsmål utover KIT som skal ivaretas i pasientsystemet. Hvilke av følgende er sikkerhetsmål som definert i IN1020:

Velg ett eller flere alternativer

- ☐ Personvern
- ☐ Autorisasjon
- ☐ Sporbarhet
- ☐ Brannvern
- ☐ Innbruddsdeteksjon

b) Velg de sikkerhetstiltakene du vil anbefale for å sikre *konfidensialitet* for data som behandles i pasientsystemet:

Velg ett eller flere alternativer

- ☐ Bruke sikre nettverksprotokoller for dataoverføring
- ☐ Loggføre all aktivitet i pasientsystemet
- ☐ Opplæring av alle databehandlere
- ☐ Sørge for gode rutiner for sikkerhetskopiering av data
- ☐ Bruke sjekksumalgoritmer for data som overføres i nettverk
- ☐ Krav om tofaktoraутентisering for innlogging
- ☐ Benytte ulike angrepsvektorer
- ☐ Kryptere alle data som lagres i systemet

c) Velg de sikkerhetstiltakene du vil anbefale for å sikre best mulig *tilgjengelighet* til data som behandles i pasientsystemet:

Velg ett eller flere alternativer

- ☐ Loggføre all aktivitet i pasientsystemet
- ☐ Kryptere alle data som lagres i systemet
- ☐ Bruke sikre nettverksprotokoller for dataoverføring
- ☐ Benytte ulike angrepsvektorer
- ☐ Installere antivirus-programvare
- ☐ Gjennomføre sikkerhetsøvelser
- ☐ Følge opp varslinger om nye sårbarheter
- ☐ Sørge for gode rutiner for sikkerhetkopiering av data

Maks poeng: 5

3.3 Begrepsforståelse

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

 [Hjelp](#)

Nulldagssårbarhet	Hash-algoritme	Verdier
Trusselmodellering	Dataorm	Asymmetrisk kryptering
PKI	Leveransekjedeangrep	Risiko
Personopplysninger	Trojaner	Digitale sertifikater

er en svakhet som ikke er kjent for leverandør av en tjeneste.

brukes for å sjekke dataintegritet.

brukes for å sikre ektheten av offentlige nøkler, samt trygg nøkkel-distribusjon.

har både en nyttig og en skadelig funksjon.

har lovpålagte krav om konfidensialitet, integritet og/eller tilgjengelighet.

er en kombinasjon av sannsynlighet for en hendelse og konsekvens av hendelsen.

Maks poeng: 3

3.4 Nettverkssikkerhet

Under utvikling av et nytt nettsted for en virksomhet blir du rådspurt om det er mest fornuftig å benytte protokollen HTTP eller HTTPS for kommunikasjon over nettverk mellom bruker og virksomhetens nettsted.

Hvilke av følgende utsagn er sanne hvis man velger **HTTP** som protokoll:

Velg ett eller flere alternativer

- ☐ Uvedkommende vil være i stand til å avlytte og lese datatrafikk mellom virksomhetens webtjener og en brukers nettleser.
- ☐ Integritet for data sendt mellom virksomhetens webtjener og en brukers nettleser blir ivaretatt.
- ☐ Hvis en bruker benytter kryptert forbindelse mellom sin datamaskin og sin trådløse hjemme-ruter, hindres både avlytting og modifikasjon av datatrafikken mellom brukerens nettleser og virksomhetens webtjener.
- ☐ Uvedkommende vil være i stand til å modifisere datatrafikk mellom virksomhetens webtjener og en brukers nettleser.

Maks poeng: 3

3.5 Egenskaper ved ulike typer kryptering

Symmetrisk og asymmetrisk kryptering er to typer kryptering som benyttes innen databasert kryptografi. I denne oppgaven skal du knytte riktig egenskap til riktig krypteringstype.

Dra og slipp utsagn om symmetrisk og asymmetrisk kryptering til riktig ramme. Merk at ikke alle utsagn passer inn i en av rammene, la de du mener ikke passer inn være.

SYMMETRISK		ASYMMETRISK
Kan bruke åpne kanaler for nøkkeldistribusjon	Ødelegger data slik at de ikke kan dekrypteres	Kan sikre uavviselighet
Benyttes for digital signering	Sender og mottager deler en felles hemmelig nøkkel	Brukes for HTTPS alene
Trygg nøkkelutveksling er utfordrende	Raskere og mer effektiv enn den andre	Nyttig for å kryptere store mengder data
Kan sikre autentisk dataopprinnelse	Nøkkelfri kryptering	Kan sikre autentisk dataopprinnelse

Maks poeng: 4

3.6 Digitale signaturer

Jonas ønsker å inngå en digitalt signert avtale (et dokument) med Trygve på en måte som gjør at det ikke er tvil om at avtalen er signert av ham, heller ikke ovenfor en 3. part som for eksempel pressen eller Stortinget.

a) Sikkerhetsmålet som ønskes oppnås ved å bruke av digital signatur som gitt over omtales

som (sporbarhet, autentisering, sikkerhetstiltak, autorisasjon, integritet, uavviselighet) .

b) Velg riktig eier og type nøkkel for signering og validering.

For å signere avtalen må Jonas bruke (sin egen, 3. partens, Trygves)

(private, symmetriske, offentlige) nøkkel.

For å validere den digitale signaturen må Trygve bruke (sin egen, Jonas sin,

3. partens) (offentlige, symmetriske, private) nøkkel.

c) Vil digital signering av et dokument sikre konfidensialitet for innholdet?

Velg et alternativ

☐ Ja

☐ Nei

d) Elektronisk sertifikat nevnes ofte sammen med digital signatur. Hvilke av nedenforstående utsagn er riktige for bruk av digitalte sertifikater?

Velg ett eller flere alternativer. Digitale sertifikater:

☐ knytter sammen en asymmetrisk og en symmetrisk nøkkel.

☐ hindrer svindlere i å opprette et gyldig domene.

☐ knytter sammen en offentlig nøkkel og eiers identitet.

☐ hindrer falske nøkler og falske tjenester.

Maks poeng: 4

3.7 Personopplysningsvern

Behandling av personopplysninger er strengt regulert i norsk og europeisk lovverk gjennom Personopplysningsloven.

a) Hvilket utsagn stemmer best med *lovkrav til behandling av personopplysninger*?

Velg ett alternativ:

- ☐ Behandling av personopplysninger stiller krav om samtykke fra den registrerte for all behandling.
- ☐ Personopplysninger skal behandles lovlig, rettferdig og åpent, og med krav om riktighet, dataminimering og formålsbegrensning.
- ☐ Personopplysninger skal behandles lovlig, rettferdig og åpent, og med krav om riktighet, dataminimering og formålsbegrensning. Behandlingen skal skje med egnede tekniske og organisatoriske tiltak slik at konfidensialitet, integritet og tilgjengelighet ivaretas.
- ☐ Behandling av personopplysninger skal skje med egnede tekniske og organisatoriske tiltak slik at konfidensialitet, integritet og tilgjengelighet ivaretas.

b) Hvilken brukergruppe har personopplysningsloven størst konsekvens for?

Velg ett alternativ

- ☐ Enkeltpesoner (de registrerte)
- ☐ Virksomheter
- ☐ Kriminelle

Maks poeng: 3

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 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.	☐	☐
Operativsystemet sørger for at flere programmer kan kjøre samtidig.	☐	☐
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 kjører i kjernemodus fordi dette er mer effektivt.	☐	☐
I operativsystemlaget er det modulen Enhetskontroll som har alt ansvaret for sikkerhet.	☐	☐

Maks poeng: 4

4.2 IPv6

Hva er hovedmotivasjonen ved å bytte ut IPv4 med IPv6?

Velg ett alternativ

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

Maks poeng: 1

4.3 Overføringshastighet

Du ønsker å laste ned en fil på 800 megabyte, og hastigheten på din Internettlinje er 50 megabit per sekund ned og 25 megabit per sekund opp. Hva er den teoretisk korteste overføringstiden?

Velg ett alternativ:

- ☐ 60 sekunder
- ☐ 32 sekunder
- ☐ 128 sekunder
- ☐ 256 sekunder
- ☐ 10 sekunder

Maks poeng: 2

4.4 Punktnotasjon til CIDR

En datamaskin har IP-adressen 213.58.192.58

Nettverksmasken er: 255.255.255.224

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

Velg ett alternativ:

- ☐ 192.168.1.1/24
- ☐ 213.58.192.1/27
- ☐ 213.58.192.58/26
- ☐ 213.58.192.1/26
- ☐ 213.58.192.58/27

Maks poeng: 4

4.5 Subnett-adresse

Gitt en maskin med IP adresse 213.58.192.58 og nettmaske 255.255.255.224.

Hva er adressen til maskinen sitt subnett?

Velg ett alternativ:

- ☐ 213.58.0.1
- ☐ 213.58.0.255
- ☐ 192.168.1.1
- ☐ 213.58.192.32
- ☐ 213.58.192.1
- ☐ 213.58.192.255

Maks poeng: 2

4.6 Broadcast-adresse

Gitt en maskin med IP adresse 213.58.192.58 og nettmaske 255.255.255.224.
Hva er broadcast-adressen i dette subnett?

Velg ett alternativ:

- ☐ 213.58.192.255
- ☐ 213.58.1.255
- ☐ 192.168.1.255
- ☐ 213.58.192.1
- ☐ 213.58.192.32
- ☐ 213.58.192.63

Maks poeng: 2

4.7 Antall IP-adresser

Subnett har nettverksmasken 255.255.255.224
Hvor mange gyldige IP-adresser kan tildeles verter i nettverket?

Velg ett alternativ:

- ☐ 256
- ☐ 30
- ☐ 128
- ☐ 32
- ☐ 126

Maks poeng: 2

4.8 Transportprotokoller

Hvilke protokoll(er) i transportlaget bruker tjenestene?

Flytt hver tjeneste til riktig protokoll.

HTTP

IMAP

FTP

DNS

DHCP

TCP

UDP

TCP og/eller UDP

Maks poeng: 5

4.9 Content Delivery Network

Hvile av alternativene er positive effekter av Content Delivery Networks?

Velg ett eller flere alternativer

- ☐ Sikrer mot datainnbrudd.
- ☐ Sparer ressurser i kjernenettverket.
- ☐ Flere maskiner fører til økt strømforbruk.
- ☐ Muliggjør bruk av kryptering under overføringen av data.
- ☐ Gjør at nettverket ikke kan kontrolleres av en statsmakt eller et selskap.
- ☐ Hindrer overbelastning av tjeneren ved å spre lasten over mange maskiner.
- ☐ Reduserer forsinkelsen for tilgang på innhold ved å flytte det nærmere brukeren fysisk.

Maks poeng: 3