

i Informasjon

Eksamen IN1020 høsten 2018

Tid

12. desember kl. 14.30-18.30

Faglærerne vil gå en runde fra kl 15.30.

Oppgavene

Oppgavene er flervalgsoppgaver der man kan angi så mange svar man vil i hver oppgave. Noen oppgaver vil 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 et hvert enkelt spørsmål.

Tillatte hjelpemidler

- Alle trykte og skrevne hjelpemidler.
- En kalkulator (kun med batteri, og uten kommunikasjonsmuligheter); dessuten vil det være en kalkulator i Inspira-systemet.

1(a) Porter / Kretsanalyse

Funksjonsuttrykket for kretsen over er:

Velg ett eller flere alternativer:

$F = \bar{a} + \bar{b}$



$F = \bar{a} \cdot \bar{b}$

$F = \overline{(ab)}$



$F = \overline{a + b}$

Maks poeng: 5

1(b) **K-map / Funksjonsuttrykk**

Hvilke av disse utlesningene av Karnaugh-diagrammet er gyldige:

Velg ett eller flere alternativer

- $F(a, b, c, d) = b\bar{c}d + \bar{a}d(c \oplus b) + \bar{a}\bar{b}\bar{c} + \bar{a}bd$ ✓
- $F(a, b, c, d) = d(a \oplus b \oplus c) + \bar{c}d(\overline{a \oplus b}) + \bar{a} \cdot \bar{c}(b \oplus d)$ ✓
- $F(a, b, c, d) = ab\bar{c}d + \bar{a}\bar{b}\bar{c} + \bar{a}bd + \bar{a}bd$ ✓
- $F(a, b, c, d) = ad(\bar{b}c + \bar{b}) + \bar{a}(\bar{b}c + bd)$ ✓
- $F(a, b, c, d) = \bar{c}d + \bar{a}bd + \bar{a}bd + \bar{a}\bar{b}\bar{c}$ ✓
- $F(a, b, c, d) = \sum(0, 1, 5, 7, 9, 11, 13)$ ✓

Maks poeng: 10

1(c) **Godt og blandet****Finn de som passer sammen**

	Usant	Sant
ALU og CPU er en og samme enhet, men har ulik klokkehastighet	<input type="radio"/> <input checked="" type="radio"/>	<input type="radio"/>
Maksterm er betegnelsen for maksimalt antall uttrykk som kan leses ut fra et Karnaughdiagram	<input type="radio"/> <input checked="" type="radio"/>	<input type="radio"/>
En av løsningene for å unngå Data Hazard er å koble utgangen på den første bit ALUen til inngangen av neste bit ALU	<input type="radio"/> <input checked="" type="radio"/>	<input type="radio"/>
Ved en cache-miss må data leses inn fra RAM	<input type="radio"/>	<input type="radio"/> <input checked="" type="radio"/>
Teknologisk utvikling gjør at vi kan lage større registre på en microchip.	<input type="radio"/>	<input type="radio"/> <input checked="" type="radio"/>
I en rippel-subtraksjonskrets kan vi kun bruke fulladder	<input type="radio"/>	<input type="radio"/> <input checked="" type="radio"/>
Det er bare ALU som bestemmer hastigheten i en pipeline	<input type="radio"/> <input checked="" type="radio"/>	<input type="radio"/>

Maks poeng: 10

2(a) **Binære tall 1**

Verdien 30_{10} (dvs 30 i 10-tallsystemet) kan også representeres i andre tallsystemer. Hvilke av disse verdiene er lik 30_{10} ?

Velg ett eller flere alternativer:

42_7



1000_3

11110_2



111_5

Maks poeng: 3

2(b) **Binære tall 2**

En byte inneholder disse bit-ene:

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

Hvilke verdier kan representeres av disse bit-ene?

Velg ett eller flere alternativer:

- 72
- 148
- 149
- 200
- 56



Maks poeng: 3

2(c) **Maskinkode 1**

start	INP	
	STA	50
	ADD	50
	ADD	50
	OUT	
slutt	HLT	

Hva skrives ut når denne koden kjøres og brukeren gir 7 som inndata?

Velg ett eller flere alternativer (men bare ett er korrekt):

- Det skrives ikke ut noe.
- 50
- 21
- 7
- 0



Maks poeng: 4

2(d) **Maskinkode 2**

start	LDA	x
	BRZ	slutt
	SUB	y
	STA	x
	INP	
	STA	w
	LDA	z
	SUB	w
	STA	z
	BRA	start
slutt	LDA	z
	OUT	
	HLT	
w	DAT	0
y	DAT	1
x	DAT	3
z	DAT	100

Hva skrives ut når denne koden kjøres og brukeren oppgir de tre verdiene **1**, **2** og **3** som inndata?

Velg ett eller flere alternativer (men bare ett er korrekt):

- 100
- 106
- 94
- 6
- Noe annet enn de andre alternativene



Maks poeng: 4

2(e) Maskinkode 3

Anta at minnet inneholder disse verdiene:

0:	901
1:	805
2:	508
3:	902
4:	000
5:	108
6:	308
7:	600
8:	000

Anta også at *programtelleren* (også kalt «program counter» eller «location counter») inneholder **0**. Hva blir da skrevet ut når vi starter prosessoren vår og brukeren gir verdiene **10, 1** og **-2** som inndata?

Velg ett eller flere alternativer (men bare ett er korrekt):

- 2
- 0
- Ingenting blir skrevet ut
- 2
- 11



Maks poeng: 4

2(f) **Maskinkode 4**

start	INP	
	BRZ	slutt
	BRP	k
	BRA	start
k	:	
	BRA	start
slutt	LDA	x
	OUT	
	HLT	
x	DAT	0
y	DAT	1
<hr/>		
a	LDA	x
	ADD	1
	STA	x
<hr/>		
b	LDA	1
	ADD	x
<hr/>		
c	LDA	x
	ADD	y
	STA	x
<hr/>		
d	ADD	x
	STA	x
<hr/>		
e	ADD	y
	STA	x

Dette programmet (i den tykke røde rammen) skal lese inn diverse tall. Det siste tallet skal være **0**, og det er ingen andre forekomster av 0. Programmet skal telle antall ekte positive tall (dvs tall som er >0) og skrive ut dette antallet. Negative tall skal ignoreres. Sekvensen

3 3 4 -1 -2 5 0

skal gi svaret **4** siden det er 4 tall som er >0.

Programmer mangler noen instruksjoner der det står et kolon (:). Hvilke instruksjoner mangler?

Velg ett eller flere alternativer

- Alternativ a
- Alternativ b
- Alternativ c
- Alternativ d
- Alternativ e



2(g) **Moore's lov**

Moore's lov sier at

Velg ett eller flere alternativer:

- Størrelsen på minnet (RAM) dobler seg annethvert år.
- Antallet kjerner i en CPU dobler seg hvert annet år.
- Klokkefrekvensen til datamaskiner dobler seg hvert annet år.
- Antall transistorer i en integrert krets dobler seg hver annet år. ✓
- Prisen på en datamaskin halveres annethvert år.

Maks poeng: 3

3(a) **TCP og UDP**

Hvilke av disse tjenestene tilbys av både TCP og UDP
Velg ett eller flere alternativer

- Metningskontoll
- Sjekksum (dataintegritet) ✓
- Multipleksing over en IP-adresse (porter) ✓
- Pålitelighet
- Flytkontroll

Maks poeng: 2

3(b) **Subnet - Kringkastingsadresse**

En gyldig IP-adresse på et subnett er 134.1.98.45. Nettverksmasken til subnettet er 255.255.248.0 Hva er kringkastingsadressen til dette subnettet?

Velg ett alternativ

- 134.1.103.255
- 134.1.99.255
- 134.1.111.255
- 134.1.98.255



Maks poeng: 2

3(c) **ARP-tabell**

Hva er en ARP-tabell?

Velg ett alternativ

- En liste, vedlikeholdt av en vert på et subnett, med IP-adresser og MAC-adresser til andre verter på samme subnett. ✓
- En liste over IP-adresser og portnummer brukt for å gjøre det mulig for private adresser på et subnett å koble seg opp mot andre maskiner på Internett (utenfor eget LAN)
- En liste over mulige ruter som en IP-pakke kan ta gjennom Internett.
- En tabell som viser når forskjellige ARP-pakker er klare til å sendes ut.

Maks poeng: 1

3(d) **Private IP-adresser**

Hvilke av disse IP-adressene er såkalte "private IP-adresser" som ikke skal brukes eksternt på Internett?

Velg ett eller flere alternativer

8.8.8.8

129.240.171.52

192.168.12.34

10.0.1.15



Maks poeng: 2

3(e) **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

3(f) **Mulige IP-adresser i subnett**

Et subnett er definert ved 192.168.0.0/30 (CIDR-notasjon). Hvor mange gyldige IP-adresser kan tildeles verter i subnettet?

Velg ett alternativ

- 254
- 2
- 16
- 255



Maks poeng: 2

3(g) **Klient-tjener**

Hva kjennetegner et klient-tjener aksessmodell?

Velg ett eller flere alternativer

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

Maks poeng: 2

3(h) Pakkeswitching

Hva er sant for et pakkeswitchet nettverk?

Velg ett eller flere alternativer

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

Maks poeng: 2

3(i) **Metningskontroll**

Oppgaven til metningskontroll er å...

Velg ett eller flere alternativer

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

Maks poeng: 2

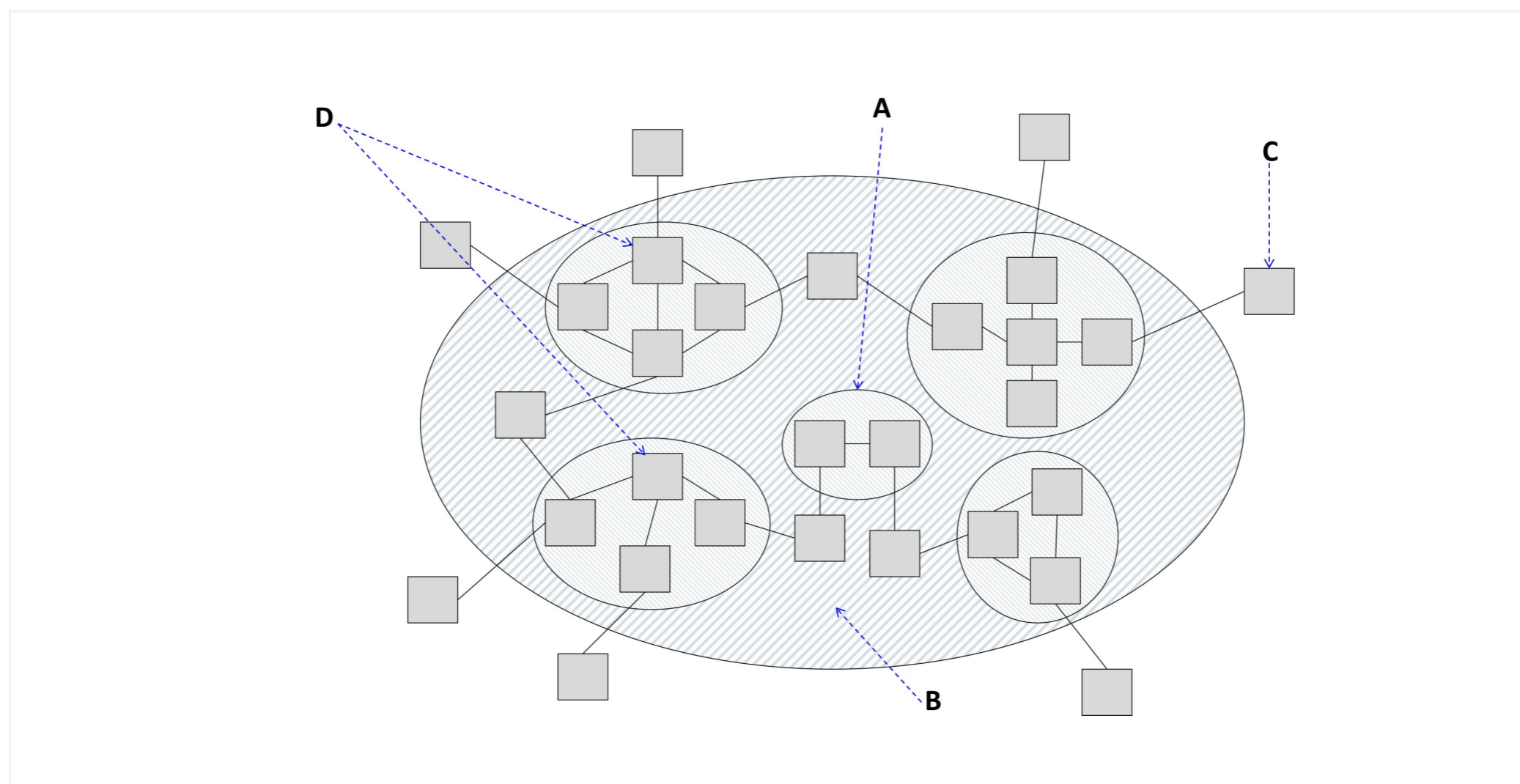
3(j) **Content Delivery Network**

Hvile av alternativene er positive effekter av Content Delivery Networks?

Velg ett eller flere alternativer

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

Maks poeng: 3

3(k) **Topologi i Internett**

Hva er riktig navn på etikettene?

Velg ett alternativ

- A) Gateway, B) Intermediate system, C) Router, D) Endesystem
- A) Server, B) Gateway, C) Intermediate system, D) Subnett
- A) Subnett, B) Nettverk C) Endesystem D) Intermediate system
- A) Repeater, B) Bridge, C) Gateway, D) Gateway



Maks poeng: 2

3(l) Linklaget

Hvilke påstander om linklaget er sanne?

Velg ett eller flere alternativer

- Dataenheter som sendes på linklaget kalles pakker.
- Sørger for rutingen av datatrafikken.
- Gjør feilsjekking av data. ✓
- Har ansvaret for å dele en bitstrøm opp i datarammer ✓
- Har bare ansvaret for at hvert bit blir riktig tolket hos mottakeren
- Sørger for pålitelig overføring mellom to enheter. ✓

Maks poeng: 3

4(a) **Sikkerhetsmål**

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

Velg ett eller flere alternativer:

- Autentisering av dataopprinnelse ✓
- Innbruddsdeteksjon
- Tilgjengelighet ✓
- Uavviselighet ✓
- Biometri
- Diskkryptering
- Logging

Maks poeng: 1.5

4(b) **Sikkerhetstiltak 1**

Sikkerhetstiltak kan delvis kategoriseres etter hvilken *fase* et tiltak er ment å fungere i. Vi skiller gjerne mellom det å *forebygge* angrep, det å *avdekke* et pågående angrep, eller å *korrigere* etter et angrep som har funnet sted.

Velg riktig katagori for de listede sikkerhetstiltakene.

	Forebyggende sikkerhetstiltak	Korrigerende sikkerhetstiltak	Avdekkende sikkerhetstiltak
Innbruddsdeteksjon	<input type="radio"/>	<input type="radio"/>	<input type="radio"/> ✓
Gjenopprette fra sikkerhetskopi	<input type="radio"/>	<input type="radio"/> ✓	<input type="radio"/>
Kryptering av nettverkstrafikk	<input type="radio"/> ✓	<input type="radio"/>	<input type="radio"/>

Maks poeng: 1.5

4(c) **Sikkerhetstiltak 2**

Hvilke av følgende er sikkerhetstiltak som kan bidra til å oppnå sikkerhetsmålet om konfidensialitet?

Velg ett eller flere alternativer:

- Å sørge for gode rutiner for sikkerhetskopiering av all informasjon.
- Å sørge for god opplæring av brukere, slik at de har kunnskap om hvordan konfidensiell informasjon skal behandles. ✓
- Å benytte tilgangskontroll for å begrense hvem og hva som gis tilgang til en ressurs. ✓
- Å benytte kryptografi for å gjøre informasjon uleselig for det eller de som ikke skal ha tilgang. ✓

Maks poeng: 3

4(d) **Brukerautentisering og passord**

Stortingets IT-organisasjon skal utarbeide et nytt, felles system for brukerautentisering til alle IT-systemene på Stortinget. De har besluttet at det skal benyttes passord som autentiseringsfaktor.

Det å utarbeide et trygt system og gode rutiner for å håndtere og lagre passord er viktig i ethvert system som involverer brukerautentisering med passord. Nedenfor er det listet fire krav som Stortinget har satt til passordhåndtering i sitt system.

For hvert krav, velg det mest relevante sikkerhetstiltaket for å sørge for å oppfylle kravet:

	Tilgangskontroll	Komplekse passord	Bruke salting	Bruke hash-algoritme
Forhåndsutregnede hash-tabeller skal ikke kunne benyttes for enkel passordknekking.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Det skal være vanskelig for angripere å knekke passord lagret i databasen, også når passord er både saltet og hashet.	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Det skal ikke være mulig å lese passord i klartekstform i databasen.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Kun autoriserte enheter/personer skal kunne lese passord-databasen.	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Maks poeng: 4

4(e) Asymmetrisk kryptering og nøkkelutveksling

Erna og Siv er midt i budsjettforhandlingene, og samarbeider om en rekke digitale dokumenter. De har nylig vært på kurs i informasjonssikkerhet, og har lært om blant annet asymmetrisk kryptering (offentlig-nøkkel-kryptering). De er enige om å benytte dette for sikker dokumentutveksling, og de har fått hvert sitt nøkkelsett bestående av privat og offentlig nøkkel.

A. Erna skal sende Siv et konfidensielt dokument, som det er viktig at beskyttes mot innsyn fra andre. Hvilken nøkkel må Erna benytte for å kryptere dokumentet før det sendes til Siv?

Velg ett alternativ:

- Ernas private nøkkel
- Ernas offentlige nøkkel
- Sivs offentlige nøkkel
- Sivs private nøkkel

B. Siv har utarbeidet et dokument som skal godkjennes og signeres digitalt av Erna før det er gyldig. Erna har fått tilsendt det digitale dokumentet, og vil signere det ved hjelp av asymmetrisk kryptering. Hvilken nøkkel skal Erna benytte når hun foretar det som kalles *digital signering*?

Velg ett alternativ

- Ernas private nøkkel
- Ernas offentlige nøkkel
- Sivs private nøkkel
- Sivs offentlige nøkkel

C. I praktisk bruk av asymmetrisk kryptering oppstår det behov for det vi kaller *digitale sertifikater*. Hva er hensikten med et digitalt sertifikat?

Velg ett alternativ

- Å knytte sammen en offentlig og en privat nøkkel.
- Å knytte en brukers identitet til en sertifikatutsteder.
- Å knytte sammen en offentlig nøkkel med eierens identitet.
- Å knytte sammen sertifikatutsteder og en offentlig nøkkel.

Maks poeng: 6

4(f) **Trusselmodellering**

For enkelhets skyld benytter en liten gruppe ansatte i en underavdeling i Forsvarsdepartementet en og samme brukeridentitet og passord for å autentisere seg i et saksbehandlingssystem.

Denne gruppen ansatte har en superbrukerrolle i saksbehandlingssystemet, som medfører utvidede privilegier sammenlignet med en ordinær ansatt i departementet. Blant annet har de privilegier til å både endre og slette *alle* lagrede dokumenter og saker.

Velg de utsagnene som er korrekte med bakgrunn i dette scenariet.

- Så lenge de ansatte har de samme privilegiene har det ingen hensikt å utstyre hver enkelt ansatt med en egen brukeridentitet.
- Det er mindre sannsynlig at passord kommer på avveie når det kun er ett felles passord å håndtere.
- Selv om de ansatte har de samme privilegiene er det nødvendig å kunne knytte hendelser til enkeltpersoner, og dermed enkeltbrukere, for å sikre sporbarhet. ✓
- Når hendelser i saksbehandlingssystemet ikke kan knyttes til en enkeltperson kan det være vanskelig å etterprøve endringer i systemet som skyldes for eksempel menneskelige feil. ✓

Maks poeng: 4

4(g) **Tastelogger**

Hensikten med en *tastelogger* er å fange opp det en bruker av en datamaskin skriver på det tilhørende tastaturet. Nedenfor er det listet en rekke utsagn om tasteloggere, hvor du skal velge de du mener er korrekte.

Velg ett eller flere alternativer:

- Offentlige tilgjengelige datamaskiner, som mange har fysisk tilgang til, er utsatt for tasteloggere. ✓
- En tastelogger er en form for ondsinnet spionvare, som gjerne spres som en trojaner. ✓
- En tastelogger er et vanlig sikkerhetstiltak som benyttes for å gjenopprette en brukers tastehistorikk i et Unix-shell.
- Bærbare datamaskiner med integrert tastatur er ikke utsatt for tasteloggere.
- Fysisk sikring av datamaskiner er et egnet sikkerhetstiltak mot tasteloggere. ✓

Maks poeng: 3

4(h) Risikoanalyse

Hvilke to hovedelementer er sentrale når det skal gjennomføres en risikoanalyse av et IT-system?

Velg to alternativer:

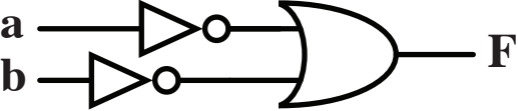
- Konsekvens av en hendelse
- Sannsynlighet for en hendelse
- Mulige rootkit
- Verdibasert trusselidentifikasjon
- Angrepsvektor som benyttes



Maks poeng: 2

Question 1
Attached





Question 2
Attached



		AB			
		00	01	11	10
CD	00	1			
	01	1	1	1	1
	11		1		1
	10				