

## i Informasjon om eksamen



# UiO • Institutt for informatikk

## Det matematisk-naturvitenskapelige fakultet

Avsluttende eksam i IN2120 Informasjonssikkerhet (Høst 2021).

Dato og tidspunkt: 3. desember 2021, kl.9:00 - 13:00 (4 timer).

Ingen hjelpemidler er tillatt.

Merk følgende:

- Oppgavene i denne eksamen er gruppert under 10 deler som tilsvarer omtrent 10 av forelesningene i dette emnet.
- Det er mulig å oppnå 10 poeng for hver del, totalt 100 poeng (= 100%).
- Man kan navigere frem og tilbake mellom oppgavene.
- Skåring for hver oppgave angis eksplisitt. Det kan gis negative poeng for feil svar/valg, men total poengsum for hele oppgaven er minimum 0 (selv om summen over alle svarene er negativ).
- Vær kortfattet når du skriver tekst som svar på en tekstoppgave. Svaret kan skrives på norsk eller engelsk.
- I navigasjonslinjen nederst på skjermen indikeres fullførte oppgaver med blå søyler.

Lykke til!

## i Del 1: Generelt

### Del 1: Generelt

## 1 1.1 Sikkerhetsmålsettinger



For hver angrepsbeskrivelse, angi på hvilken målsetting (eller ingen) det medfører brudd. Poeng: 0,5 for hver korrekt, -0,5 for for hver feil, 0 for intet valg, maks 3, minimum 0.

Angi målsettingen det medfører brudd på:

	System-integritet	Personvern	Konfidensialitet	Ingen	Data-integritet	Tilgjengelighet
Angriper endrer konfigurering av webtjener	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Angriper blokkerer overføring av en melding	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Angriper avlytter kryptert trafikk	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Angriper avskjærer en melding, endrer innholdet, og videresender meldingen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Angriper avlytter en kryptert forbindelse og klarer å dekode data	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Angriper får tilgang til anonymiserte persondata, og klarer å de-anonymisere persondataene	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Maks poeng: 3

## 2 1.2 Begreper

For hver beskrivelse, angi hvilket begrep som representerer beskrivelsen, ved å velge blant begrepene Trussel, Sårbarhet, Verdi, Risiko, Hendelse eller Ingen. Poeng: 0,5 for hver korrekt, -0,5 for for hver feil, 0 for intet valg, maks 3, minimum 0.

Angi riktig sikkerhetsbegrep:

	Ingen	Sårbarhet	Verdi	Risiko	Hendelse	Trussel
Kombinasjon av trussel, sårbarheter og verdier	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Brudd på konfidensialitet, integritet og/eller tilgjengelighet	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Skadelig aktivitet som kan utnytte sårbarheter og forårsake en sikkerhetshendelse	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Har krav om konfidensialitet, integritet, og/eller tilgjengelighet	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
At en type angrep ikke kan forhindres	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Angrep som ikke detekteres	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Maks poeng: 3

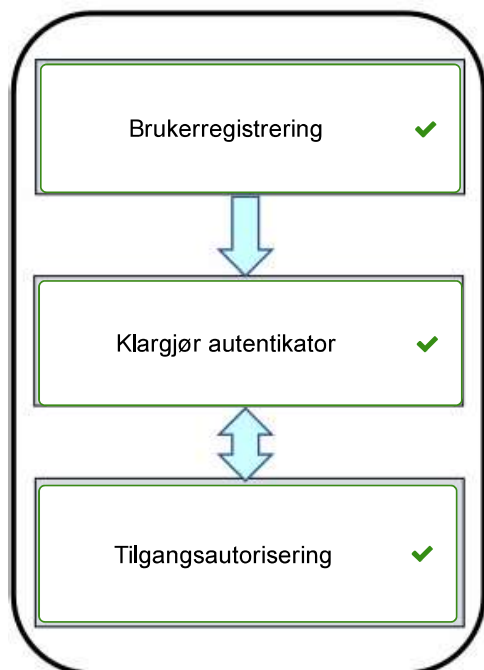
### 3 1.3 IAM

Tilordne trinnene til riktig felt i diagrammet for IAM (identitets- og tilgangshåndtering). Poeng: 0,5 for hver korrekt tilordning, -0,5 for hver feil tilordning, maks 3, minimum 0.

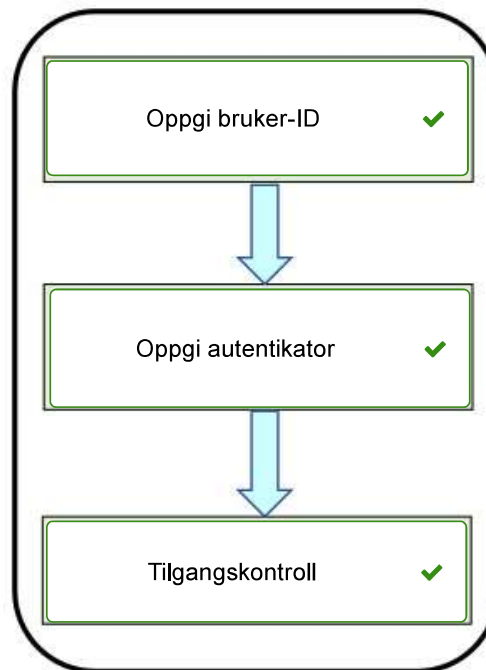
 Hjelp



#### Konfigureringsfase



#### Bruksfase



Maks poeng: 3

### 4 1.4 Meldingsautentisering

Angi hva som er korrekt for meldings/data-autentisering med MAC (Message Authentication Code) og digital signatur.

Poeng: 0,5 for riktig, -0,5 for feil, 0 for intet valg, maks 1, minimum 0.

**Angi det som er korrekt**

- Digital signatur kan valideres av mottager ✓
- MAC kan valideres av mottager ✓
- MAC er sterkere enn digital signatur.
- MAC kan valideres av tredjeparter

Maks poeng: 1

## i Del 2: Angrepsvektorer og skadevare

## Del 2: Angrepsvektorer og skadevare

## 5 2.1 Phishing

For hver beskrivelse, angi riktig type phishing ved å velge blant massephishing, spydphishing, hvalphishing, og klonephishing. Poeng: 0,5 for hver korrekt, -0.5 for for hver feil, 0 for intet valg, maks 2, minimum 0.

Angi riktig type phishing

	Massephishing	Spydphishing	Klonephishing	Hvalphishing
Du mottar phishing-epost som er irrelevant for deg	<input type="radio"/> ✓	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Du mottar phishing-epost som er relevant for deg	<input type="radio"/>	<input type="radio"/> ✓	<input type="radio"/>	<input type="radio"/>
Du mottar phishing-epost som ligner en tidligere epost fra en kollega	<input type="radio"/>	<input type="radio"/>	<input type="radio"/> ✓	<input type="radio"/>
Du er direktør og mottar phishing-epost om å autorisere en stor betaling	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/> ✓

Maks poeng: 2

## 6 2.2 Angrepstyper

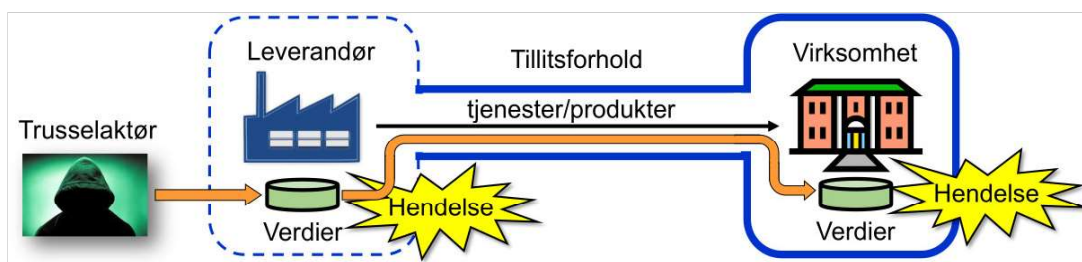
For hver beskrivelse, angi korrekt type angrep ved å velge blant Sidekekanal, Skjult kanal, MitM (Man-in-the-Middel) eller Ingen. Poeng: 0,5 for hver korrekt, -0.5 for for hver feil, 0 for intet valg, maks 2, minimum 0.

**Angi agrepstype som passer**

	Skjult kanal	Ingen	MitM	Sidekanal
Å sette opp en kryptert forbindelse gjennom TOR (The Onion Router)	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Å opptre som både avsender og mottager i en kryptert forbindelse	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Måle variasjon av tidsbruk ved kryptering med ulike nøkkelverdier	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Kalle funksjoner i et system med ulike tidsbruk med hensikt at det kan måles utenfor systemet	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Maks poeng: 2

## 7 2.3 Leveransekjedeangrep



Angi hva som er korrekt om leveransekjedeangrep.

Poeng: 0,5 for hver korrekt, -0.5 for for hver feil, 0 for intet valg, maks 2, minimum 0.

**Leveransekjedeangrep er angrep mot en virksomhet basert på kompromitterte tjenester/produkter levert av en tredjepart.**

Sant



Usant

**Leverandør er som regel erstatningsansvarlig for virksomhetens tap som følge av leveransekjedeangrep.**

Sant

Usant



**Leverandør lider som regel størst konsekvenser ved leveransekjedeangrep.**

Sant

Usant



**Leverandør har best grunnlag for å vurdere konsekvenser ved leveransekjedeangrep.**

Sant

Usant



Maks poeng: 2

## 8 2.4 Løsepengevirus

For hver beskrivelse, angi hva som er korrekt om tiltak for å forhindre eller respondere mot løsepengevirus. Poeng: 0,5 for hver korrekt, -0.5 for for hver feil, 0 for intet valg, maks 2, minimum 0.

### Kan forhindre/mitigere (konsekvens av) tap av data

- Sikkerhetskopi av data ✓
- Anonymisering av persondata
- Cyberforsikring for å betale løsepenger ✓

### Kan forhindre/mitigere (konsekvens av) brudd på personvern

- Sikkerhetskopi av data
- Anonymisering av persondata ✓
- Cyberforsikring for å betale løsepenger ✓

Maks poeng: 2

## 9 2.5 Skadevare

For hver karakteristik, angi riktig type skadevare. Poeng: 0,5 for hver korrekt, -0.5 for for hver feil, 0 for intet valg, maks 2, minimum 0.

### Angi riktig type skadevare

	Virus	Orm	Trojaner	Drive-by-script
Utføres automatisk uten brukermedvirkning	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> ✓
Integreres som del av legitim programvare	<input checked="" type="radio"/> ✓	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Har både en nyttig og en skadelig funksjon	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/> ✓	<input type="radio"/>
Spres automatisk uten brukermedvirkning	<input type="radio"/>	<input checked="" type="radio"/> ✓	<input type="radio"/>	<input type="radio"/>

Maks poeng: 2



## i Del 3: Kryptografi

### Del 3: Kryptografi

#### 10 3.1 Betingelser for sterk krypto

Angi nødvendige betingelser for å oppnå sterk kryptografi. Poeng: 1 for hver korrekt, -1 for for hver feil, 0 for intet valg, maks 2, minimum 0.

Angi korrekte betingelser




- Algoritmens design må holdes hemmelig
- Algoritmen må være resistent mot kryptanalyse ✓
- Algoritmen må være resistent mot kvantecomputere
- Algoritmen må beholde statistiske ujevnheter fra klartekst til chiffertekst
- Nøkkelrommet må være tilstrekkelig stort ✓

Maks poeng: 2

#### 11 3.2 Sikker krypteringsmodus

Diagrammet viser eksempel på kryptering med sikker og usikker krypteringsmodus. Tilordne krypteringsmodus (som kan være reelle eller ikke) til riktig felt i diagrammet. Poeng: 1 for hver korrekt tilordning, -1 for hver feil tilordning, maks 2, minimum 0

 [Hjelp](#)

	Symmetrisk modus	ECB-modus	Tellermodus
 Klartekst	 ECB-modus <span style="float: right;">✓</span>	 Tellermodus <span style="float: right;">✓</span>	Ingen Symmetrisk modus <span style="float: right;">✓</span>

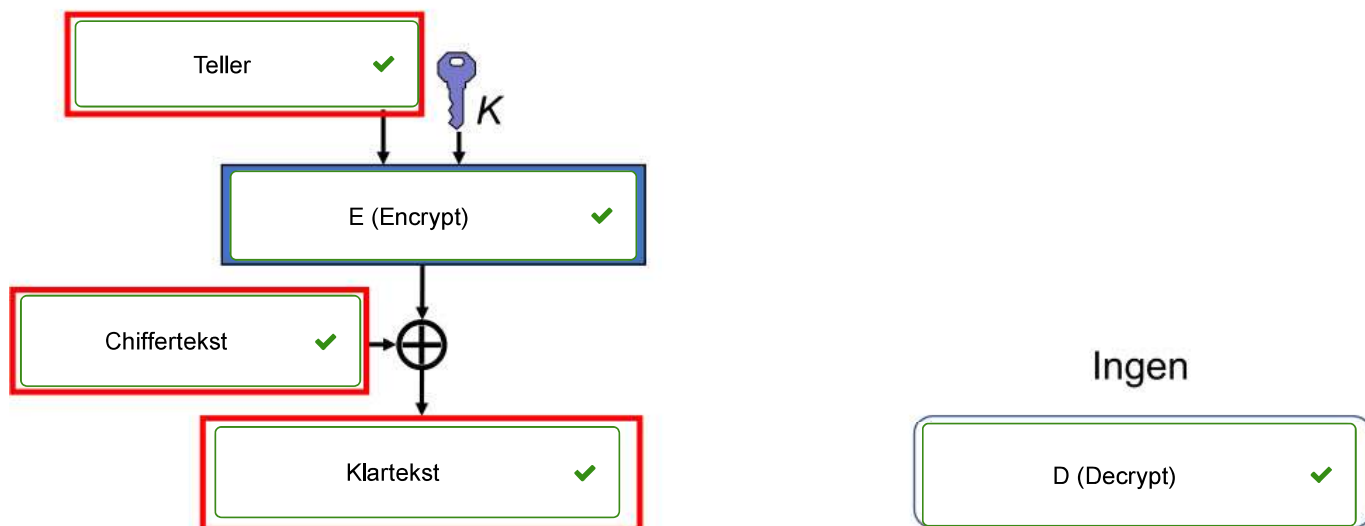
Maks poeng: 2

## 12 3.3 Tellermodus

Diagrammet viser prinsipp for dekryptering av en chiffterekstblokk i tellermodus. Tilordne funksjoner (som kan være reelle eller ikke) til riktig felt i diagrammet. Poeng: 0,5 for hver korrekt tilordning, -0,5 for hver feil tilordning, maks 2, minimum 0.

 [Hjelp](#)

### Dekryptering med tellermodus



Maks poeng: 2

### 13 3.4 Hashfunksjoner

Angi hva som er korrekt for sikre hashfunksjoner.

Poeng: 0,5 for riktig, -0,5 for feil, 0 for intet valg, maks 2, minimum 0.

**Hashfunksjoner er teoretisk mulig å invertere**

Sant



Usant

**Det er praktisk mulig å finne to datasett som gir samme hashverdi**

Sant

Usant



**Hashverdien har alltid samme størrelse uansett inndatasett**

Sant



Usant

**Endring av en enkelt bit i inndatasettet gjør at alle bits i hasverdien endres**

Sant

Usant



---

Maks poeng: 2

### 14 3.5 Digital signatur

Alice ønsker å sende en digitalt signert melding til Bob. Velg riktig eier og type nøkkel for signering og validering. Poeng: 0,5 for hvert korrekte valg, -0,5 for hvert feil valg, maks 2, minimum 0.

For å signere meldingen må Alice bruke  (Bobs, **sin egen**, dommerens)

(offentlige, symmetriske, **private**) nøkkel.

For å validere den digitale signaturen må Bob bruke  (dommerens, sin egen,

**Alices**)  (offentlige, private, symmetriske) nøkkel.

---

Maks poeng: 2

## i Del 4: Nøkkelhåndtering og PKI

Del 4: Nøkkelhåndtering og PKI

### 15 4.1 Nøkkelstørrelse

Poeng for svar på spørsmålene: 0,5 for riktig, -0,5 for feil, maks 2, minimum 0.

Anta et chiffer med krypteringsnøkler med størrelse 8 bits. Hvor mange ulike nøkler fins det?

Svar med et heltall:  (256).

Anta et chiffer med krypteringsnøkler der det fins 1024 forskjellige nøkler. Hva er nøkkelstørrelsen i antall bits. Svar med et heltall:  (10).

Hva er typisk nøkkelstørrelse for AES-algoritmen? Velg:  (128 bits, 1024 bits, 8 bits),

Hva er typisk nøkkelstørrelse for RSA-algoritmen? Velg:  (8 bits, 1024 bits, 128 bits)

---

Maks poeng: 2

### 16 4.2 Nøkkelkompromittering

Ved mistanke om nøkkelkompromittering kan visse kryptografiske funksjoner fremdeles tillates, Velg riktig alternativ. Poeng: 1 for hvert korrekte valg, -1 for hvert feil valg, maks 2, minimum 0.

Ved kompromittering av hemmelig symmetrisk nøkkel kan nøkkelen fremdeles benyttes til

(dekryptering, validering, kryptering, signering).

Ved kompromittering av privat asymmetrisk nøkkel kan nøkkelen fremdeles benyttes til

(dekryptering, kryptering, signering, validering)

---

Maks poeng: 2

## 17 4.3 Kryptoperioder

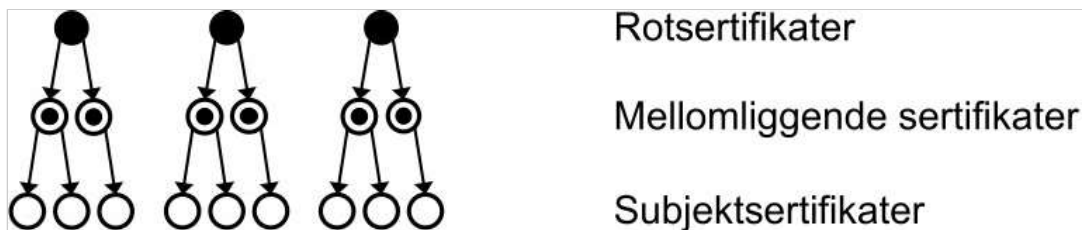
For hver periode, angi hvilken type nøkkel det gjelder. Poeng: 0,5 for hver korrekt, -0.5 for for hver feil, 0 for intet valg, maks 3, minimum 0.

**Angi hvilken type nøkkel det gjelder**

	hemmelig nøkkel	offentlig nøkkel	privat nøkkel
Beskyttelsesperiode for symmetrisk kryptering/dekryptering	<input type="radio"/> ✓	<input type="radio"/>	<input type="radio"/>
Proseseringsperiode for symmetrisk kryptering/dekryptering	<input type="radio"/> ✓	<input type="radio"/>	<input type="radio"/>
Beskyttelsesperiode for asymmetrisk signatur/validering	<input type="radio"/>	<input type="radio"/>	<input type="radio"/> ✓
Proseseringsperiode for asymmetrisk signatur/validering	<input type="radio"/>	<input type="radio"/> ✓	<input type="radio"/>
Beskyttelsesperiode for asymmetrisk kryptering/dekryptering	<input type="radio"/>	<input type="radio"/> ✓	<input type="radio"/>
Proseseringsperiode for asymmetrisk kryptering/dekryptering	<input type="radio"/>	<input type="radio"/>	<input type="radio"/> ✓

Maks poeng: 3

## 18 4.4 Sertifikater



For hver beskrivelse, angi riktig sertifikat (der Ingen også er et alternativ). Poeng: 0,5 for hver korrekt, -0.5 for for hver feil, 0 for intet valg, maks 3, minimum 0.

## Velg riktig sertifikat

	Rotsertifikater	Mellomliggende sertifikater	Subjektsertifikater	Ingen
Inneholder webtjeners offentlige nøkkel	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Inneholder webtjeners private nøkkel	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Er signert av webtjener	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Er selvsignert	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Er signert av rot-CA (ikke selvsignert)	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Brukes til signering av subjektsertifikater	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

Maks poeng: 3

## i Del 5: Nettverkssikkerhet

## Del 5: Nettverkssikkerhet

### 19 5.1 Internettstakken

Tilordne protokolltypene til riktig lag i internettstakken. Poeng: 0,5 for hver korrekt tilordning, -0,5 for hver feil tilordning, maks 3, minimum 0

 Hjelp

Internettprotokollen	Applikasjonsprotokoller
Transportprotokoller	Linkprotokoller



Maks poeng: 2

### 20 5.2 Sikkerhetsprotokoller

Velg riktig eksempel på sikkerhetsprotokoll for hvert lag i internettstakken. Poeng: 0,5 for hvert korrekte valg, -0,5 for hvert feil valg, maks 2, minimum 0.

Velg riktig sikkerhetsprotokoll

	TLS Record	Ingen	IPSec	TLS Handshake
Transportlaget	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Applikasjonslaget	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Linklaget	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
IP-laget	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

Maks poeng: 2

## 21 5.3 Perfekt fremoverhemmelighold

- Nevn en sikkerhetsprotokoll for nøkkelutveksling/nøkkeletablering som støtter perfekt fremoverhemmelighold/fremoversikkerhet (perfect forward secrecy)?
- Hva menes med perfekt fremoverhemmelighold?
- Hvordan oppnås perfekt fremoverhemmelighold?
- Nevn en sikkerhetsprotokoll som ikke støttet perfekt fremoverhemmelighold, og si hvorfor ikke (dvs. hvordan den etablerer øktnøkler/sesjonsnøkler).

Poeng: maks 4, minimum 0.

Skriv besvarelsen nedenfor

Format | **B** | *I* | U | ~~X~~ | ~~X~~ | ~~X~~ | | | | | | | | |

Σ |

a)  
1 poeng for: f.eks. En sikkerhetsprotokoll som gir perfekt fremoverhemmelighold er f.eks. TLS (1.3)

b)  
0,5 poeng for: Dreier seg om tilfellet der servers private nøkkel (langtidsnøkkel) blir kompromittert en gang i fremtiden  
0,5 poeng for: Tidligere øktnøkler som er utvekslet/etablert ved hjelp av langtidsnøkkelen forblir hemmelige fremover i tid, dvs blir ikke kompromittert, selv om langtidsnøkkel blir lekket.

c)  
1 poeng for: f.eks. med DH (Diffie-Hellman)

d)  
0,5 poeng for: f.eks. I TLS 1.2 var DH bare en opsjon for nøkkeletablering, slik at TLS 1.2 ikke alltid støttet perfekt fremoverhemmelighold. SSL er en tidligere versjon av TLS som ikke støttet perfekt fremoverhemmelighold.  
0,5 poeng for: Fordi hemmelig (frø-verdi for) øktnøkkel ble oversendt kryptert med tjenerens offentlige nøkkel.

Words: 0

Maks poeng: 4



## 22 5.4 Brannmurer

For hver egenskap, angi riktig type brannmur (der Ingen er et alternativ). Poeng: 0,5 for hver korrekt, -0.5 for for hver feil, 0 for intet valg, maks 2, minimum 0.

Angi riktig type brannmur

	Tilstandsbasert pakkefilter	Tilstandsløst pakkefilter	Ingen	Applikasjonsbrannmur
Kan støtte HSTS	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Har statiske regler	<input type="radio"/>	<input type="radio"/> ✓	<input type="radio"/>	<input type="radio"/>
Lager dynamiske regler	<input type="radio"/> ✓	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Kan støtte TLS-inspeksjon	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/> ✓

Maks poeng: 2

### i Del 6: Brukerautentisering

## Del 6: Brukerautentisering

## 23 6.1 Passordcracking

Passord lagres på forskjellige måter i passorddatabaser. Hvis en slik database blir lekket vil angripere forsøke å cracke (avdekke) passordene. For hver lagringsmåte (som kan være reel eller ikke), angi hvordan passord kan crackes. Poeng: 0,5 for hver korrekt, -0.5 for for hver feil, 0 for intet valg, maks 2, minimum 0.

Angi hvordan passord kan crackes

	Vanskelig å cracke	Uten hashtabell	Ingen	Med hashtabell
Lagret som hashverdi	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/> ✓
Lagret som salt	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Lagret i klartekst	<input type="radio"/>	<input type="radio"/> ✓	<input type="radio"/>	<input type="radio"/>
Lagret som saltet hashverdi	<input type="radio"/> ✓	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Maks poeng: 2

## 24 6.2 Biometrisk system

Poeng for hvert svar: 0,5 for riktig, -0,5 for feil, maks 3, minimum 0.

Når terskelverdien for match (for å bli godtatt) heves, vil FMR  (forbli uendret, øke, minske).

Et ideelt biometrisk system er når  ( $FMR = FNMR = EER = 0$ ,  $FMR = FNMR$ ,  $FMR = 0$ ,  $FNMR = 0$ )-

PAD (Presentation Attack Detection) er å

(oppdage forsøk på forfalskning av biometri, oppdage når en genuin bruker blir feilaktig avvist, oppdage når en ikke-genuin bruker blir feilaktig godtatt).

Å oppdage forfalskning av biometri er  (enkelt med, vanskelig på tross av) lav EER (Equal Error Rate).

Anta at et biometrisk system har blitt testet med 100 genuine brukere, og 100 ikke-genuine brukere. Testingen viste at systemet hadde  $FMR = 0,05$ , og  $FNMR = 0,07$ .

Hvor mange ikke-genuine brukere ble godtatt? Svar med heltall:  (5).

Hvor mange genuine brukere ble avvist? Svar med heltall:  (7).

Maks poeng: 3

## 25 6.3 Autentiseringsenheter

For hver karakteristikk, angi tilhørende type autentiseringsenhet. Poeng: 0,5 for hver korrekt, -0.5 for for hver feil, 0 for intet valg, maks 3, minimum 0.

### Angi type autentiseringsenhet

	OTP-brikke	Pass og ID-kort	Online-enhete	Sekundærkanal
Brukes i FIDO-løsninger	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Har som regel klokke	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Brukes i BankID på mobil	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/> <input checked="" type="radio"/>
Brukes i BankID	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Blir autentisert av leser/terminal	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Brukes for overføring av autorisasjonskode/mønster til bruker	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/> <input checked="" type="radio"/>

Maks poeng: 3

## 26 6.4 Rammeverk for e-autentisering

Tre rammeverk for e-autentisering er

- NIST SP800-63-3, USA 2017
- eIDAS, EU 2014
- RAU (Rammeverk for autentisering og uavviselighet), Norge 2008

For hver karakteristikk, angi tilhørende rammeverk for e-autentisering. Poeng: 0,5 for hver korrekt, -0.5 for for hver feil, 0 for intet valg, maks 2, minimum 0.

### Angi tilhørende rammeverk for e-autentisering

	NIST, USA 2017	RAU, Norge 2008	eIDAS, EU 2014
Beskriver krav til ID-føderering	<input type="radio"/> ✓	<input type="radio"/>	<input type="radio"/>
Beskriver 3 kategorier krav til autentiseringsløsninger	<input type="radio"/>	<input type="radio"/>	<input type="radio"/> ✓
Beskriver ikke krav til registrering av ID	<input type="radio"/>	<input type="radio"/> ✓	<input type="radio"/>
Definerer 4 autentiseringsnivåer	<input type="radio"/>	<input type="radio"/> ✓	<input type="radio"/>

Maks poeng: 2

## i Del 7: Identitets- og tilgangshåndtering

### Del 7: Identitets- og tilgangshåndtering

### 27 7.1 ID-modeller

To modeller for identitetshåndtering er silo-modellen og føderert modell.

For hver karakteristik, angi tilhørende modell for identitetshåndtering. Poeng: 0,5 for hver korrekt, -0.5 for for hver feil, 0 for intet valg, maks 2, minimum 0.

Angi tilhørende modell for identitetshåndtering

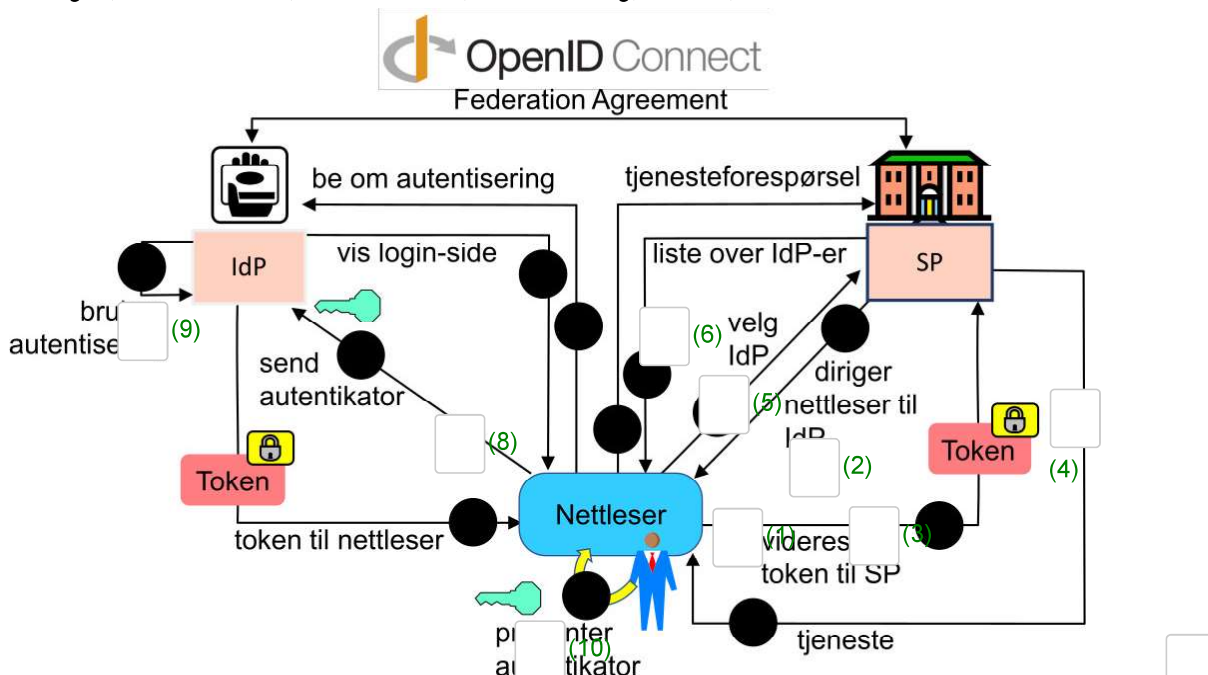
	Silo	Føderert
Gjøre at bruker får mange passord	<input type="radio"/> ✓	<input type="radio"/>
Gjør det lett å dele informasjon om brukere	<input type="radio"/>	<input type="radio"/> ✓
SP og IdP er samme entitet	<input type="radio"/> ✓	<input type="radio"/>
Benyttes i ID-porten	<input type="radio"/>	<input type="radio"/> ✓

Maks poeng: 2

### 28 7.2 Open ID Connect

Figuren viser scenarioet for brukerautentisering med OIDC. Sett inn tall 1 - 12 i hver melding for å vise rekkefølgen av meldingene i scenarioet.

Poeng: 0,5 for korrekt tall, 0 for for feil tall, 0 for intet valg, maks 6, minimum 0.



Maks poeng: 6

(7) (12) (11)

## 29 7.3 Tilgangskontroll

Fire modeller for tilgangskontroll er ABAC, DAB, MAC og RBAC.

For hver karakteristikk, angi tilhørende modell for tilgangskontroll. Poeng: 0,5 for hver korrekt, -0.5 for for hver feil, 0 for intet valg, maks 2, minimum 0.

Angi riktig modell

	RBAC	MAC	ABAC	DAC
Egner seg når det er et fast sett med jobbfunksjoner	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Brukes i Windows/Linux	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Er en generell modell	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Støtter spesielle krav i militære systemer	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Maks poeng: 2

### i Del 8: Ledelse av informasjonssikkerhet

## Del 8: Ledelse av informasjonssikkerhet

## 30 8.1 ISO/IEC-standarder

To prominente standarder for ledelse av informasjonssikkerhet er ISO/IEC 27001 og 27002.

For hver karakteristikk, angi tilhørende standard (eventuelt begge eller ingen). Poeng: 0,5 for hver korrekt, -0.5 for for hver feil, 0 for intet valg, maks 3, minimum 0.

### Angi tilhørende standard

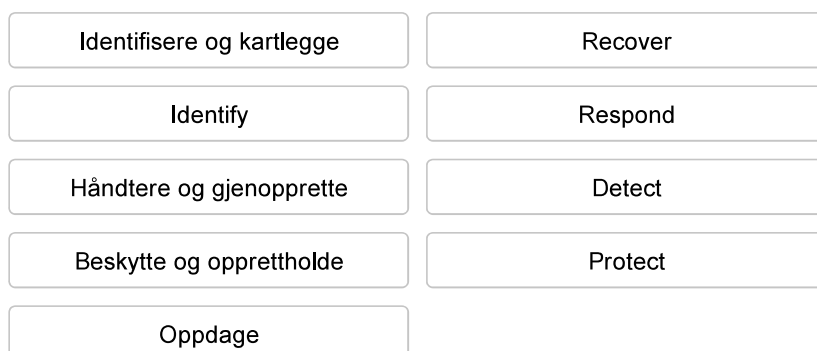
	ISO/IEC 27001	ISO/IEC 27002	Begge	Ingen
Beskriver tiltaksbank for sikkerhet	<input type="radio"/>	<input type="radio"/> ✓	<input type="radio"/>	<input type="radio"/>
Beskriver ISMS	<input type="radio"/> ✓	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Er gratis	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Kommer opprinnelig fra BSI (British Standard)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/> ✓	<input type="radio"/>
Er obligatorisk i norsk statlig forvaltning	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Danner grunnlag for sertiifisering av virksomheter	<input type="radio"/> ✓	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Maks poeng: 3

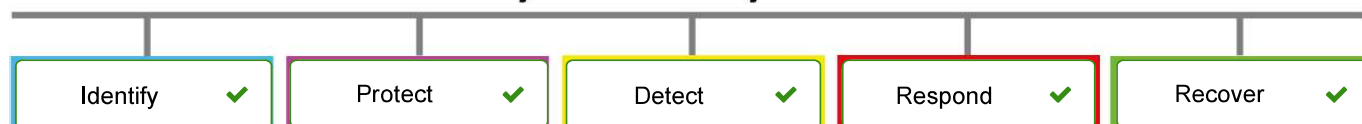
## 31 8.2 Rammeverk for cybersikkerhet

Figuren viser NIST og NSM sine rammeverk for cybersikkerhet som beskriver kategorier med sikkerhetstiltak/prinsipper i en logisk rekkefølge fra venstre mot høyre. Tilordne kategoriene til riktig felt i diagrammet for NIST og NSM sine rammeverk. Poeng: 0,5 for hver korrekt tilordning, -0,5 for hver feil tilordning, 5 for alle riktig, minimum 0.

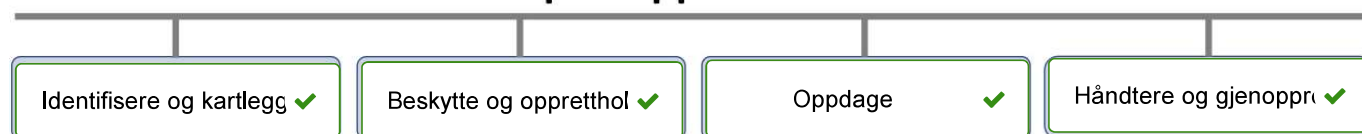
 Hjelp



### NIST Cyber Security Framework



### NSM Grunnprinsipper for IKT-sikkerhet



Maks poeng: 5

## 32 8.3 Modenhetsnivåer

CMMI (Capability Maturity Model Integration) definerer modenhetsnivåer for styring og ledelse av informasjonssikkerhet. Velg riktig nivå ut i fra beskrivelsen.

Poeng: 1 for hver korrekt, 0 for feil, maks 2, minimum 0.

Ledelsesforankring forventes fra modenhetsnivå  (5: Optimalisert, 4: Systematisert, 3: **Formalisert**, 2: Fragmentert, 1: Tilfeldig, 0: Fraværende).

Risikobasert styring og ledelse forventes fra modenhetsnivå  (5: Optimalisert, 4: **Systematisert**, 3: Formalisert, 2: Fragmentert, 1: Tilfeldig, 0: Fraværende).

Maks poeng: 2



## i Del 9: Innebygd informasjonssikkerhet

### Del 9: Innebygd informasjonssikkerhet

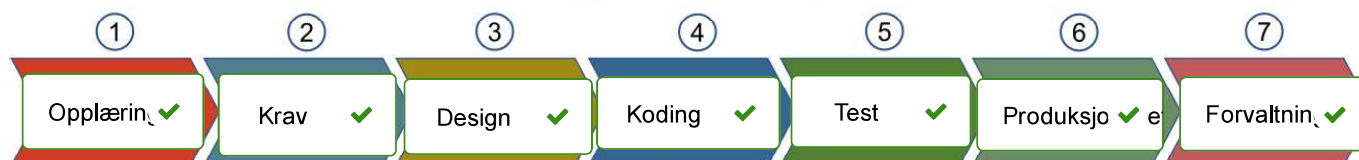
#### 33 9.1 Syklus for innebygd informasjonssikkerhet

Figuren viser 7 faser i syklus for innebygd informasjonssikkerhet. Tilordne fasene til riktig felt i figuren. Poeng: 0,5 for hver korrekt tilordning, -0,5 for hver feil tilordning, 4 for alle riktig, minimum 0.

 Hjelp

Test	Koding	Krav
Produksjonssetting	Design	Opplæring
Forvaltning		

#### Syklus for innebygd informasjonssikkerhet



Maks poeng: 4

Justert skåring for denne oppgaven er basert på lengden av sekvensen med trinn i riktig rekkefølge. Hvis det f.eks. er spesifisert 5 trinn i riktig rekkefølge gir det 2.5 poeng. Eventuell spesifisering av feil trinn imellom har ingen negativ betydning. Det gis ikke minuspoeng for feilplassert spesifisering av trinn.

## 34 9.2 STRIDE

STRIDE er en modell utviklet av Microsoft for trusselmodellering som er ment å bruke under programvareutvikling. Hver bokstav i STRIDE er forbokstaven for en type trussel. Velg hva hver type trussel betyr (der noen betydninger er irrelevante).

Poeng: 0,5 for hver korrekt, -0,5 for feil, maks 3, minimum 0.

Spoofing (identitetstyveri) er brudd på  (autentisitet, autorisering, integritet, konfidensialitet, sikkerhetskultur, tilgangskontroll, tilgjengelighet, uavviselighet/sporbarhet/regnskapelighet).

Tampering (tukling/kompromittering) er brudd på  (autentisitet, autorisering, integritet, konfidensialitet, sikkerhetskultur, tilgangskontroll, tilgjengelighet, uavviselighet/sporbarhet/regnskapelighet).

Repudiation (avvising) er brudd på  (autentisitet, autorisering, integritet, konfidensialitet, sikkerhetskultur, tilgangskontroll, tilgjengelighet, uavviselighet/sporbarhet/regnskapelighet).

Information disclosure (datatyveri og lekkasje) er brudd på

(autentisitet, autorisering, integritet, konfidensialitet, sikkerhetskultur, tilgangskontroll, tilgjengelighet, uavviselighet/sporbarhet/regnskapelighet).

Denial of service (tjenestenekt) er brudd på  (autentisitet, autorisering, integritet, konfidensialitet, sikkerhetskultur, tilgangskontroll, tilgjengelighet, uavviselighet/sporbarhet/regnskapelighet).

Elevation of privilege (utvidet tilgang) er brudd på  (autentisitet, autorisering, integritet, konfidensialitet, sikkerhetskultur, tilgangskontroll, tilgjengelighet, uavviselighet/sporbarhet/regnskapelighet)

---

Maks poeng: 3

### 35 9.3 Sikker programvareutvikling

Sikker Smidig og DevOps er to modeller for sikker programvareutvikling.

For hver karakteristikk, angi tilhørende modell (eventuelt begge eller ingen). Poeng: 0,5 for hver korrekt, -0.5 for for hver feil, 0 for intet valg, maks 3, minimum 0.

Finn de som passer sammen:

	Sikker smidig	DevOps	Begge	Ingen
Dekker opplæring i informasjonssikkerhet	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Dekker forvaltning	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fokuserer på "shift left"	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Må være skybasert	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Fokuserer på sikkerhet	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Har sprintsyklus som sentralt begrep	<input type="radio"/> <input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Maks poeng: 3

## i Del 10: Cyberoperasjoner

### Del 10: Cyberoperasjoner

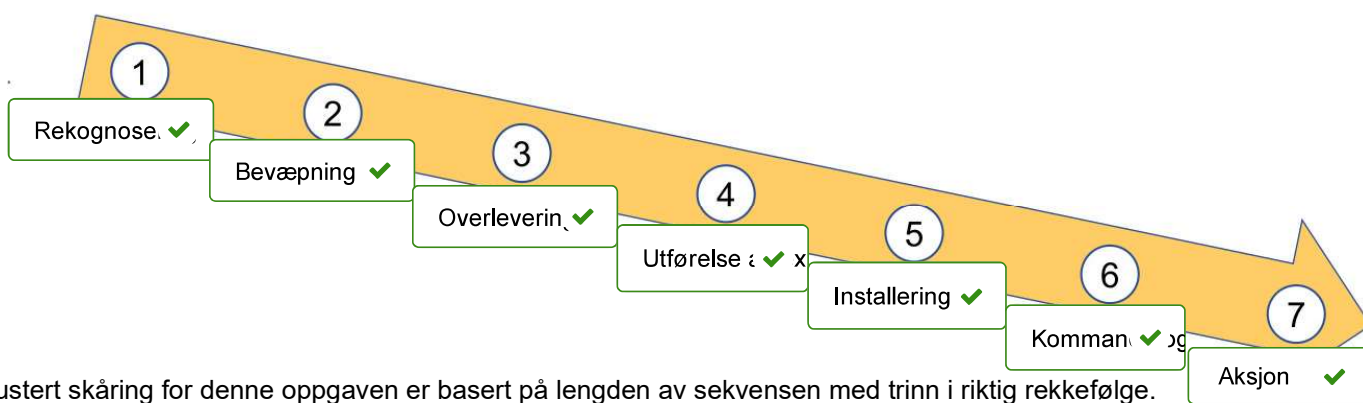
## 36 10.1 Cyber Kill Chain

Figuren viser 7 trinn i Cyber Kill Chain. Tilordne trinn til riktig felt i figuren. Poeng: 0,5 for hver korrekt tilordning, -0,5 for hver feil tilordning, 4 for alle riktige, minimum 0.

 Hjelp

Overlevering	Kommando og kontroll
Rekognosering	Aksjon
Bevæpning	Installering
Utførelse av exploit	

## Cyber Kill Chain



Justert skåring for denne oppgaven er basert på lengden av sekvensen med trinn i riktig rekkefølge. Hvis det f.eks. er spesifisert 5 trinn i riktig rekkefølge gir det 2.5 poeng. Eventuell spesifisering av feil trinn imellom har ingen negativ betydning. Det gis ikke minuspoeng for feilplassert spesifisering av trinn.

Maks poeng: 4

## 37 10.2 APT

Velg riktig utsagn i hver setning,

Poeng: 1 for riktig, -1 for feil, maks 4, minimum 0.

"Kill" i Cyber Kill Chain betyr at

Velg alternativ  (Angriperen kan drepe/skade (kille) offeret på denne måten, Forsvarerne kan potensielt stoppe (kille) angrepet på hvert trinn).

En APT (Advanced Persistent Threat) er en

Velg alternativ  (trusselflate som er avansert, gruppering med en aktivitetsprofil for cyberangrep).

En APT er "avansert" fordi Velg alternativ  (rikelige ressurser for angrep er tilgjengelige, kun avanserte teknikker brukes).

En APT er "persistent" fordi Velg alternativ  (trusselaktøren har tålmodighet, trusselflaten er vanskelig å minske)

Maks poeng: 4

**38 10.3 MITRE ATT&CK**

MITRE ATT&CK beskriver såkalte teknikker og taktikker. Velg riktig utsagn i hver setning relatert til MITRE ATT&CK.

Poeng: 1 for riktig, -1 for feil, maks 2, minimum 0.

En "teknikk" beskriver  (hvordan en angriper oppnår et (del)mål, hvordan en trussel kan forhindres).

En taktikk beskriver  (et sett med teknikker som kombineres for å stoppe en trussel, et (del)mål for angriperen).

---

Maks poeng: 2

**i Slutt**

## Slutt på eksamen