# 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!**

# 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:**

| | Ingen | Konfiden-sialitet | Tilgjen-gelighet | System-integritet | Data-integritet | Personvern |
|---|---|---|---|---|---|---|
| Angriper avlytter en kryptert forbindelse og klarer å dekryptere data | ○ | ○ | ○ | ○ | ○ | ○ |
| Angriper endrer konfigurering av webtjener | ○ | ○ | ○ | ○ | ○ | ○ |
| Angriper avlytter kryptert trafikk | ○ | ○ | ○ | ○ | ○ | ○ |
| Angriper avskjærer en melding, endrer innholdet, og videresender meldingen | ○ | ○ | ○ | ○ | ○ | ○ |
| Angriper får tilgang til anonymiserte persondata, og klarer å de-anonymisere persondataene | ○ | ○ | ○ | ○ | ○ | ○ |
| Angriper blokkerer overføring av en melding | ○ | ○ | ○ | ○ | ○ | ○ |

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:**

| | Hendelse | Risiko | Verdi | Sårbarhet | Ingen | Trussel |
|---|---|---|---|---|---|---|
| Skadelig aktivitet som kan utnytte sårbarheter og forårsake en sikkerhetshendelse | ○ | ○ | ○ | ○ | ○ | ○ |
| At en type angrep ikke kan forhindres | ○ | ○ | ○ | ○ | ○ | ○ |
| Har krav om konfidensialitet, integritet, og/eller tilgjengelighet | ○ | ○ | ○ | ○ | ○ | ○ |
| Angrep som ikke detekteres | ○ | ○ | ○ | ○ | ○ | ○ |
| Brudd på konfidensialitet, integritet og/eller tilgjengelighet | ○ | ○ | ○ | ○ | ○ | ○ |
| Kombinasjon av trussel, sårbarheter og verdier | ○ | ○ | ○ | ○ | ○ | ○ |

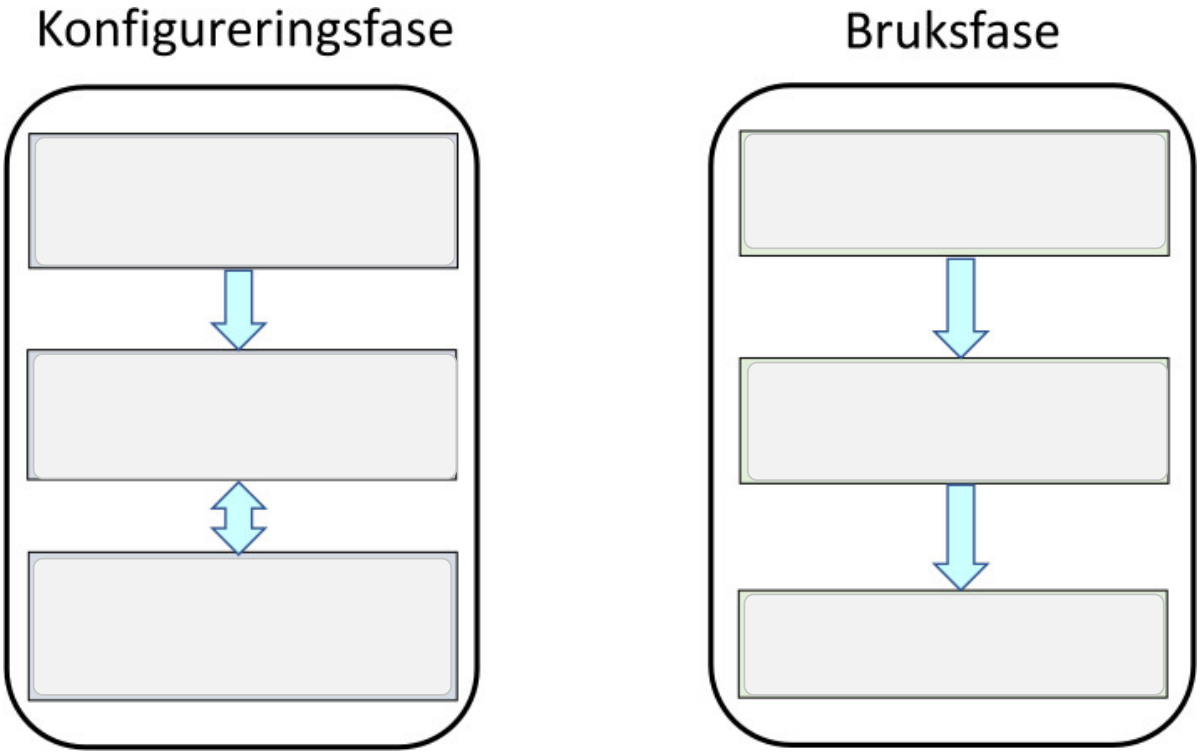
Maks poeng: 3

## 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

| | | |
|---|---|---|
| Oppgi bruker-ID | Brukerregistrering | Klargjør autentikator |
| Tilgangsautorisering | Tilgangskontroll | Oppgi autentikator |




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**

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

Maks poeng: 1

## Del 2: Angrepsvektorer og skadevare

# Del 2: Angrepsvektorer og skadevare

## 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**

| | Spydphishing | Massephishing | Hvalphishing | Klonephishing |
|---|---|---|---|---|
| Du mottar phishing-epost som er irrelevant for deg | ○ | ○ | ○ | ○ |
| Du er direktør og mottar phishing-epost om å autorisere en stor betaling | ○ | ○ | ○ | ○ |
| Du mottar phishing-epost som ligner en tidligere epost fra en kollega | ○ | ○ | ○ | ○ |
| Du mottar phishing-epost som er relevant for deg | ○ | ○ | ○ | ○ |

Maks poeng: 2

# 6 2.2 Angrepstyper

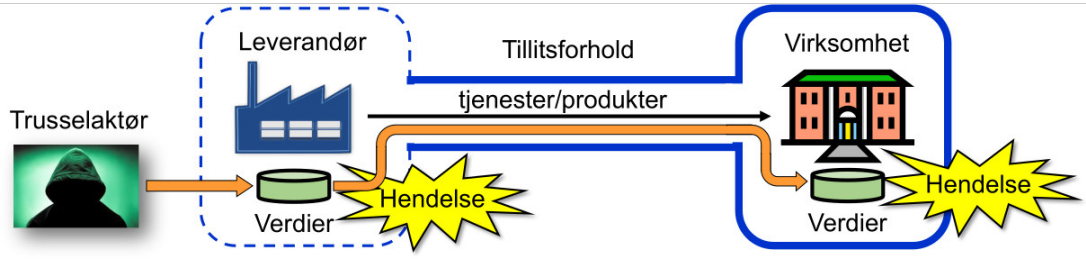
For hver beskrivelse, angi korrekt type angrep ved å velge blant Sidekekanal, Skjult kanal, MitM (Man-in-the-Middel) eller Ingen. Poeng: 0,5 for hver korrekt, -0.5 for for hver feil, 0 for intet valg, maks 2, minimum 0.

**Angi agrepstype som passer**

| | Skjult kanal | Ingen | Sidekanal | MitM |
|---|---|---|---|---|
| Å opptre som både avsender og mottager i en kryptert forbindelse | ○ | ○ | ○ | ○ |
| Kalle funksjoner i et system med ulike tidsbruk med hensikt at det kan måles utenfor systemet | ○ | ○ | ○ | ○ |
| Måle variasjon av tidsbruk ved kryptering med ulike nøkkelverdier | ○ | ○ | ○ | ○ |
| Å sette opp en kryptert forbindelse gjennom TOR (The Onion Router) | ○ | ○ | ○ | ○ |

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/miitigere (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 karakteristikk, 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**

| | Drive-by-script | Virus | Orm | Trojaner |
|---|---|---|---|---|
| Utføres automatisk uten brukermedvirkning | ○ | ○ | ○ | ○ |
| Har både en nyttig og en skadelig funksjon | ○ | ○ | ○ | ○ |
| Integreres som del av legitim programvare | ○ | ○ | ○ | ○ |
| Spres automatisk uten brukermedvirkning | ○ | ○ | ○ | ○ |

Maks poeng: 2

## 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

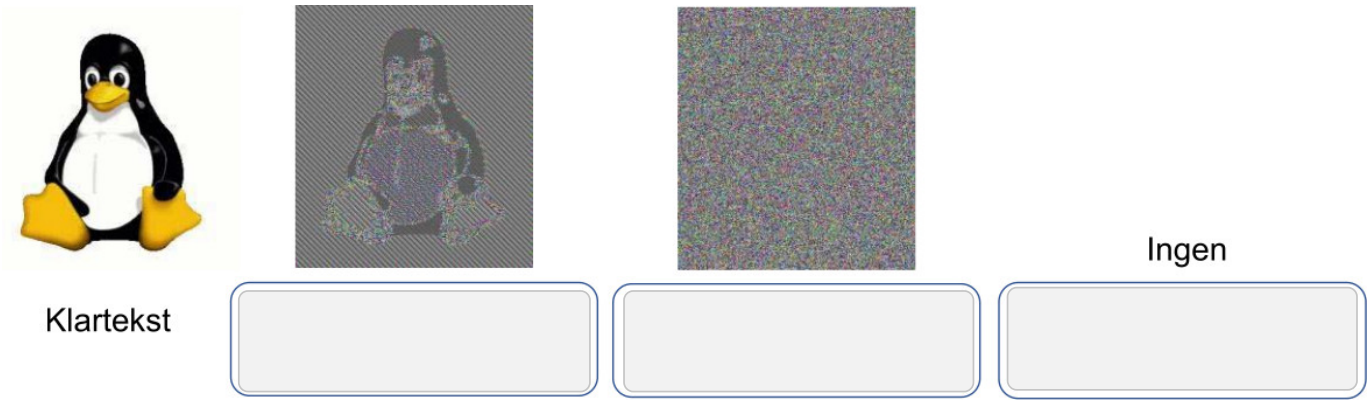
Maks poeng: 2

## 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

ECB-modus | Tellermodus | Symmetrisk modus



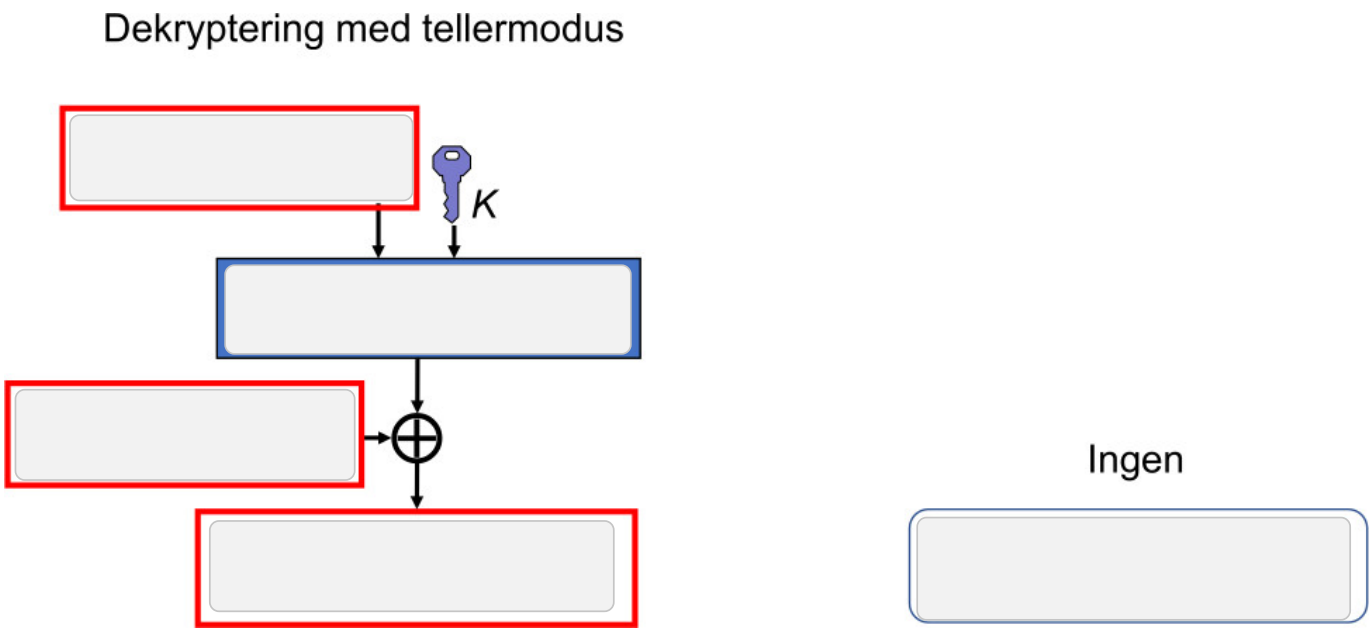

Maks poeng: 2

## 12 3.3 Tellermodus

Diagrammet viser prinsipp for dekryptering av en chiffertekstblokk 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

D (Decrypt) | E (Encrypt) | Teller | Chiffertekst | Klartekst




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 Velg alternativ (sin egen, dommerens, Bobs) Velg alternativ (offentlige, private, symmetriske) nøkkel.

For å validere den digitale signaturen må Bob bruke Velg alternativ (dommerens, Alices, sin egen) Velg alternativ (offentlige, symmetriske, private) nøkkel.

Maks poeng: 2

# 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 krypteringsnøkkler med størrelse 8 bits. Hvor mange ulike nøkler fins det? Svar med et heltall: [ ] .

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

Hva er typisk nøkkelstørrelse for AES-algoritmen? Velg: Velg alternativ (1024 bits, 128 bits, 8 bits),
Hva er typisk nøkkelstørrelse for RSA-algoritmen? Velg: Velg alternativ (1024 bits, 128 bits, 8 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 Velg alternativ (validering, kryptering, dekryptering, signering).
Ved kompromittering av privat asymmetrisk nøkkel kan nøkkelen fremdeles benyttes til Velg alternativ (dekryptering, validering, kryptering, signering)

---

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 | ○ | ○ | ○ |
| Prosesseringsperiode for symmetrisk kryptering/dekryptering | ○ | ○ | ○ |
| Beskyttelsesperiode for asymmetrisk signatur/validering | ○ | ○ | ○ |
| Prosesseringsperiode for asymmetrisk signatur/validering | ○ | ○ | ○ |
| Beskyttelsesperiode for asymmetrisk kryptering/dekryptering | ○ | ○ | ○ |
| Prosesseringsperiode for asymmetrisk kryptering/dekryptering | ○ | ○ | ○ |

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 | ○ | ○ | ○ | ○ |
| Inneholder webtjeners private nøkkel | ○ | ○ | ○ | ○ |
| Er signert av webtjener | ○ | ○ | ○ | ○ |
| Er selvsignert | ○ | ○ | ○ | ○ |
| Er signert av rot-CA (ikke selvsignert) | ○ | ○ | ○ | ○ |
| Brukes til signering av subjektsertifikater | ○ | ○ | ○ | ○ |

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

| | |
|---|---|
| Applikasjonsprotokoller | Transportprotokoller |
| Linkprotokoller | Internettprotokollen |


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**

| | IPSec | Ingen | TLS Handshake | TLS Record |
|---|---|---|---|---|
| Transportlaget | ○ | ○ | ○ | ○ |
| IP-laget | ○ | ○ | ○ | ○ |
| Linklaget | ○ | ○ | ○ | ○ |
| Applikasjonslaget | ○ | ○ | ○ | ○ |

Maks poeng: 2

# 21 5.3 Perfekt fremoverhemmelighold

a) Nevn en sikkerhetsprotokoll for nøkkelutveksling/nøkkeletablering som støtter perfekt fremoverhemmelighold/fremoversikkerhet (perfect forward secrecy)?

b) Hva menes med perfekt fremoverhemmelighold?

c) Hvordan oppnås perfekt fremoverhemmelighold?

d) 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

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**

| | Ingen | Tilstandsbasert pakkefilter | Tilstandsløst pakkefilter | Applikasjons-brannmur |
|---|---|---|---|---|
| Kan støtte HSTS | ○ | ○ | ○ | ○ |
| Kan støtte TLS-inspeksjon | ○ | ○ | ○ | ○ |
| Lager dynamiske regler | ○ | ○ | ○ | ○ |
| Har statiske regler | ○ | ○ | ○ | ○ |

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**

| | Med hashtabell | Uten hashtabell | Ingen | Vanskelig å cracke |
|---|---|---|---|---|
| Lagret som salt | ○ | ○ | ○ | ○ |
| Lagret som hashverdi | ○ | ○ | ○ | ○ |
| Lagret som saltet hashverdi | ○ | ○ | ○ | ○ |
| Lagret i klartekst | ○ | ○ | ○ | ○ |

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 Velg alternativ (forbli uendret, øke, minske).

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

PAD (Presentation Attack Detection) er å

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

Å oppdage forfalskning av biometri er Velg alternativ (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 godatt? Svar med heltall: .

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

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**

| | Online-enhete | OTP-brikke | Sekundærkanal | Pass og ID-kort |
|---|---|---|---|---|
| Brukes i FIDO-løsninger | ○ | ○ | ○ | ○ |
| Blir autentisert av leser/terminal | ○ | ○ | ○ | ○ |
| Brukes for overføring av autorisasjonskode/mønster til bruker | ○ | ○ | ○ | ○ |
| Har som regel klokke | ○ | ○ | ○ | ○ |
| Brukes i BankID på mobil | ○ | ○ | ○ | ○ |
| Brukes i BankID | ○ | ○ | ○ | ○ |

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 autentiserinig 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 | eIDAS, EU 2014 | RAU, Norge 2008 |
|---|---|---|---|
| Definerer 4 autentiseringsnivåer | ○ | ○ | ○ |
| Beskriver ikke krav til registrering av ID | ○ | ○ | ○ |
| Beskriver krav til ID-føderering | ○ | ○ | ○ |
| Beskriver 3 kategorier krav til autentiseringsløsninger | ○ | ○ | ○ |

Maks poeng: 2

## i Del 7: Identitets- og tilgangshåndtering

# Del 7: Identitets- og tilgangshåndtering

# 27 7.1 ID-modeller

To modeller for identitetshåndterinig er silo-modellen og fødert modell.

For hver karakteristikk, 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**

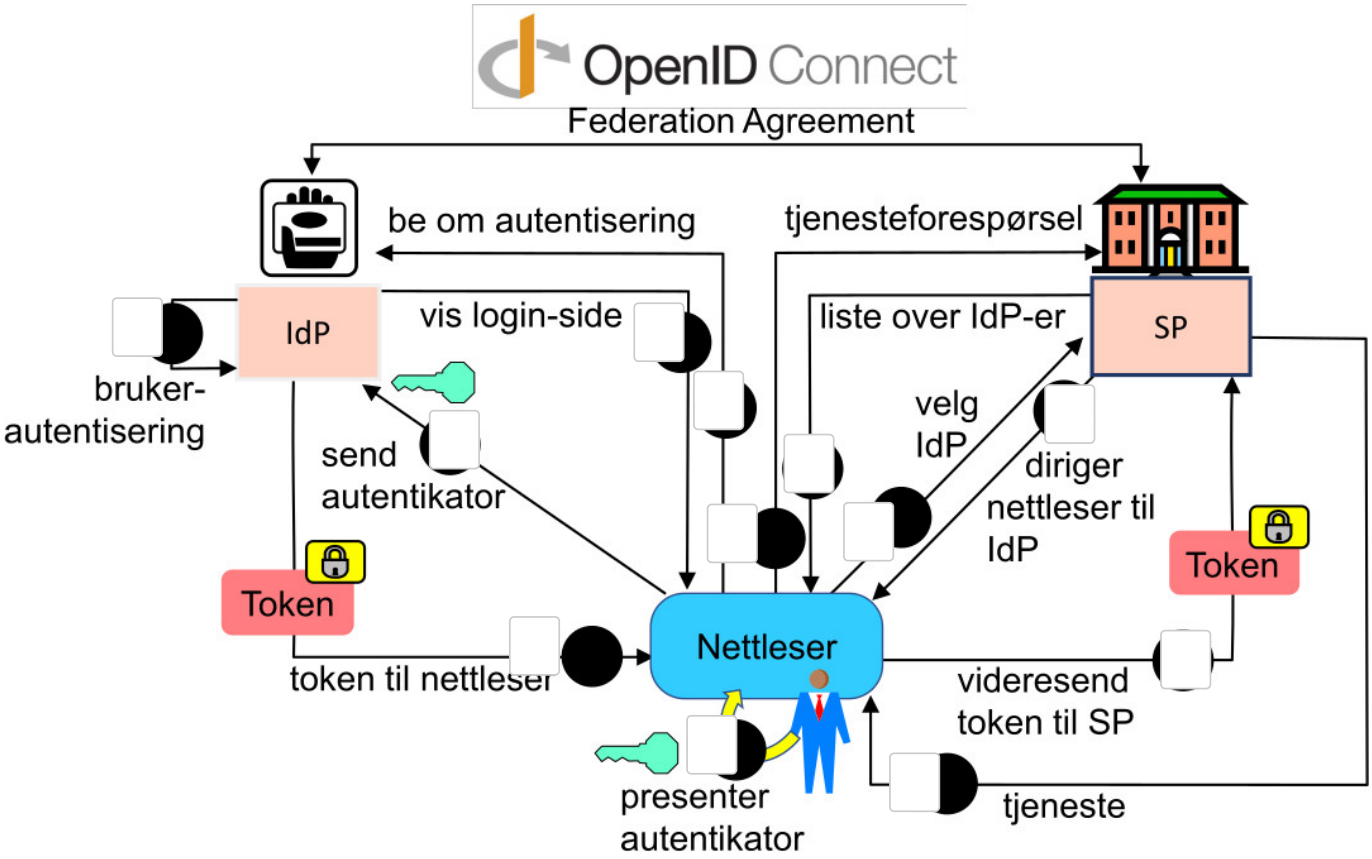
| | Silo | Føderert |
|---|---|---|
| Benyttes i ID-porten | ○ | ○ |
| Gjøre at bruker får mange passord | ○ | ○ |
| SP og IdP er samme entitet | ○ | ○ |
| Gjør det lett å dele informasjon om brukere | ○ | ○ |

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

## 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**

| | DAC | RBAC | ABAC | MAC |
|---|---|---|---|---|
| Er en generell modell | ○ | ○ | ○ | ○ |
| Brukes i Windows/Linux | ○ | ○ | ○ | ○ |
| Støtter spesielle krav i militære systemer | ○ | ○ | ○ | ○ |
| Egner seg når det er et fast sett med jobbfunksjoner | ○ | ○ | ○ | ○ |

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 | ○ | ○ | ○ | ○ |
| Beskriver ISMS | ○ | ○ | ○ | ○ |
| Er gratis | ○ | ○ | ○ | ○ |
| Kommer opprinnelig fra BSI (British Standard) | ○ | ○ | ○ | ○ |
| Er obligatorisk i norsk statlig forvaltning | ○ | ○ | ○ | ○ |
| Danner grunnlag for sertiifisering av virksomheter | ○ | ○ | ○ | ○ |

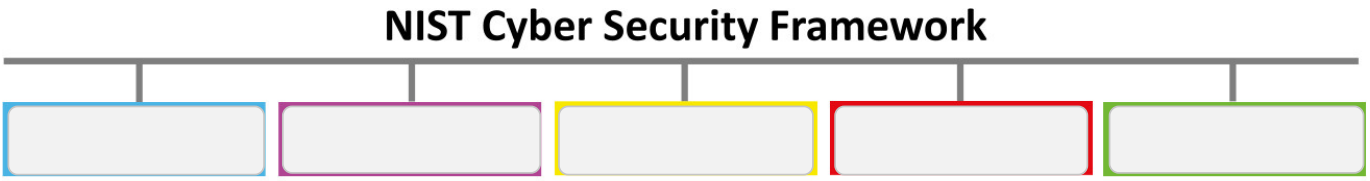
Maks poeng: 3

## 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

| | |
|---|---|
| Recover | Beskytte og opprettholde |
| Detect | Protect |
| Identify | Håndtere og gjenopprette |
| Respond | Identifisere og kartlegge |
| Oppdage | |





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 Velg alternativ (5: Optimalisert, 4: Systematisert, 3: Formalisert, 2: Fragmentert, 1: Tilfeldig, 0: Fraværende).

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

Maks poeng: 2

## Del 9: Innebygd informasjonssikkerhet

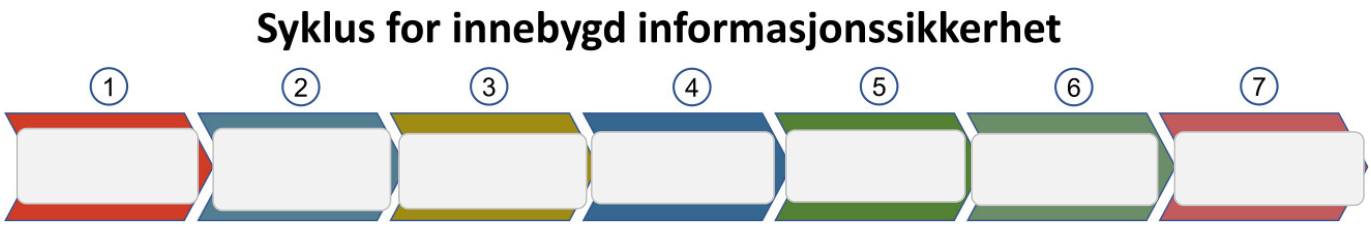
# Del 9: Innebygd informasjonssikkerhet

## 33 9.1 Syklus for innebygd informasjonssikkehet

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

| | | |
|---|---|---|
| Opplæring | Design | Koding |
| Krav | Test | Produksjonssetting |
| Forvaltning | | |




Maks poeng: 4

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

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

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

Information disclosure (datatyveri og lekkasje) er brudd på Velg alternativ (autentisitet, autorisering, integritet, konfidensialitet, sikkerhetskultur, tilgangskontroll, tilgjengelighet, uavviselighet/sporbarhet/regnskapelighet).

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

Elevation of privilege (utvidet tilgang) er brudd på Velg alternativ (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 | ○ | ○ | ○ | ○ |
| Dekker forvaltning | ○ | ○ | ○ | ○ |
| Fokuserer på "shift left" | ○ | ○ | ○ | ○ |
| Må være skybasert | ○ | ○ | ○ | ○ |
| Fokuserer på sikkerhet | ○ | ○ | ○ | ○ |
| Har sprintsyklus som sentralt begrep | ○ | ○ | ○ | ○ |

Maks poeng: 3

## i Del 10: Cyberoperasjoner

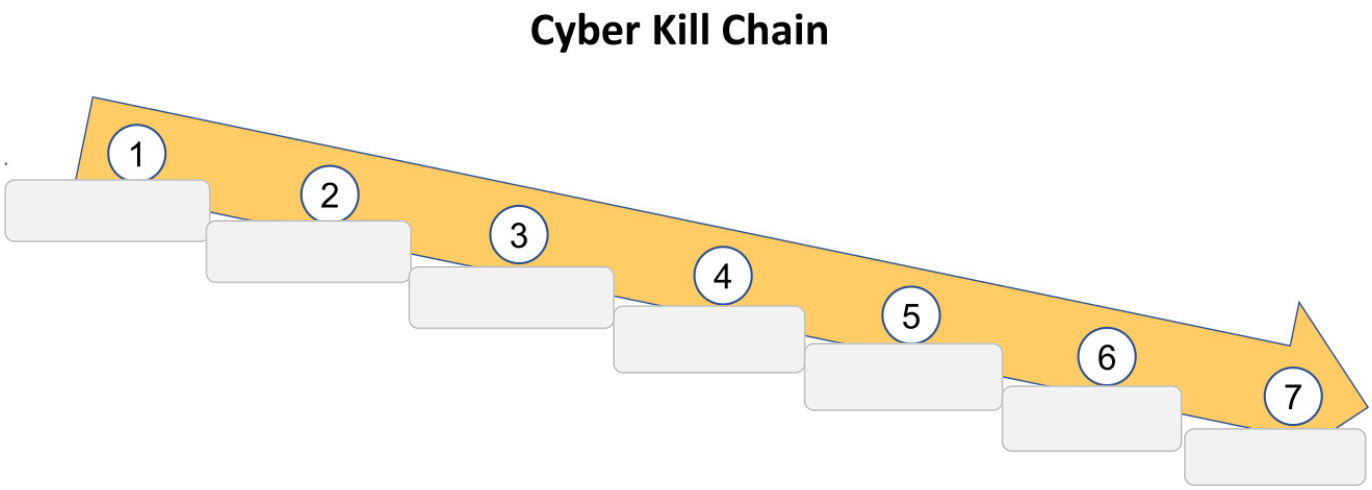
# Del 10: Cyberoperasjoner

# 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 riktig, minimum 0.

Hjelp

| | |
|---|---|
| Aksjon | Utførelse av exploit |
| Kommando og kontroll | Rekognosering |
| Installering | Overlevering |
| Bevæpning | |




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 (kun avanserte teknikker brukes, rikelige ressurser for angrep er tilgjengelige).
En APT er "persistent" fordi Velg alternativ (trusselflaten er vanskelig å minske, trusselaktøren har tålmodighet)

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 Velg alternativ (hvordan en angriper oppnår et (del)mål, hvordan en trussel kan forhindres).
En taktikk beskriver Velg alternativ (et (del)mål for angriperen, et sett med teknikker som kombineres for å stoppe en trussel).

Maks poeng: 2

## i Slutt

# Slutt på eksamen