

UiO : Institutt for informatikk

Datateknologi og sikkerhet

IN1020 – Introduksjon til datateknologi

09.11.2021

Kristin Skar
kritisk@ifi.uio.no

Praktisk informasjon

Undevisning:

- Oppsummeringsforelesninger 16. og 18. november.
- Gruppeundervisning til og med uke 47

Prøveeksamen IN1020 åpen:

https://uio.inspera.no/

- Tilgjengelig fram til 8. desember
- Om eksamen i Inspera: https://www.uio.no/studier/eksamen/innlevering/

Hvorfor kan bruk av USB minnepinner utgjøre en *sikkerhetstrussel* mot sikkerhetsmålet konfidensialitet?
Velg ett eller flere alternativer

- ☑ De kan stjeles.
- ☑ De kan bringe med seg skadevare som omgår andre sikkerhetsmekanismer.
- ☒ De kan utilsiktet bli kryptert av for eksempel løsepengevirus.
- ☒ De kan bruke for mye strøm og på den måten påvirke en datamaskin negativt.

Eksempel: Løsepengevirus

Eksempel: *WannaCry ransomware attack*

- Dataorm som spredde seg svært raskt. Krypterte filer og filsystem ikke bare lokalt på en maskin med MS Windows, men også på monterte nettverksdisker.
- Utnyttet kjent sårbarhet i fildelingsprotokollen SMB.
- Store og kritiske virksomheter rammet

Ytterligere info:

https://nsm.no/aktuelt/presseoppdatering-om-losepengevirus



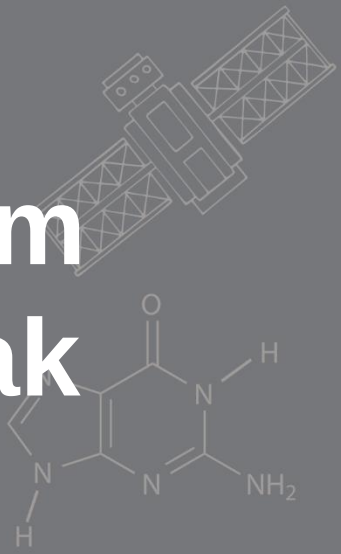
Løsepengevirus: Mottilak

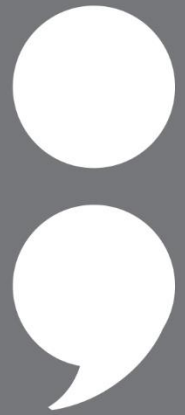
- Antivirus
- Ta regelmessig sikkerhetskopier
- Ha gode rutiner for gjenoppretting
- ØVE på gjenoppretting
- Redundante systemer
- Holde datasystemene sikkerhetsoppdatert
- Holde programvare sikkerhetsoppdatert
- Brannmur og innbruddsdeteksjon

- Ikke eksponere tjenester online
- God beskyttelse *mellom* ulike systemer
- Brukere som ikke åpner vedlegg eller lenker
- Gode passordrutiner
- God brukerhåndtering, f.eks. fjerne ikke-aktive brukere
- God sikkerhetskultur

Kryptering som sikkerhetstiltak







UiO : Institutt for informatikk

Kryptering (repetisjon)

- Hovedmål:
  - Sikre konfidensialitet og/eller integritet
  - Brukes også til autentisering av dataopprinnelse og for å oppnå uavviselighet.
- Krypteringsformer:
  - Hash-algoritmer (enveis-kryptering)
  - Symmetrisk (én hemmelig delt nøkkel)
  - Asymmetrisk (nøkkelpar: offentlig + privat nøkkel)

Symmetrisk kryptering



- Håkon har en boks med lås.
- Låsen har en nøkkel, en og samme nøkkel låser boksen både igjen og opp.
- Når Håkon vil beskytte noe (holde noe hemmelig), låser han det ned i boksen.
- Kun Håkon, som har nøkkelen, kan låse opp igjen.
- **Opplagt**!

Symmetrisk kryptering



- Håkon ønsker å overlevere et privat dokument til Omid.
- Håkon overleverer *den eneste* ekstranøkkelen til Omid, slik at han også kan låse opp boksen.
- Håkon putter dokumentet i boksen og sender den til Omid.
- Omid får boksen, låser opp med sin kopi av nøkkelen, og mottar dokumentet uten at andre kan få tak i det.
- Kun Håkon og Omid kan låse boksen opp og igjen.

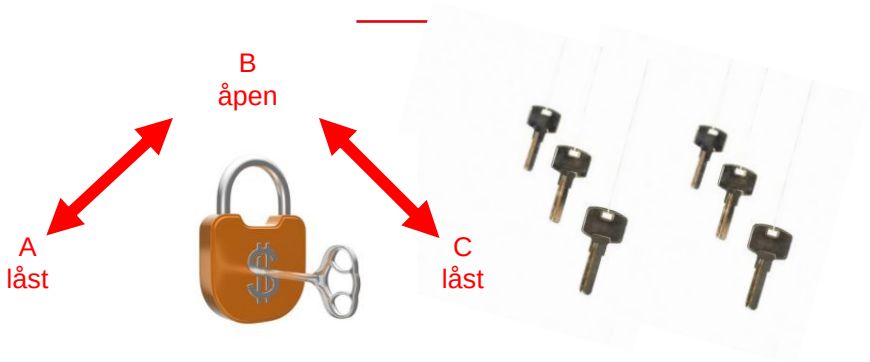
Oppsummering symmetrisk kryptering

- Avsender og mottager benytter identisk nøkkel til hhv. kryptering og dekryptering.
- Anvendes til kryptering av data, kryptering av meldinger

- **Hvilke sikkerhetsmål kan ivaretas?**
  - Konfidensialitet? **JA**
  - Integritet? I praksis **JA**
  - Autentisering av dataopprinnelse? **JA**
  - Uavviselighet? **NEI**

- Farer: Nøkkel på avveie, nøkkel tapt

Asymmetrisk kryptering

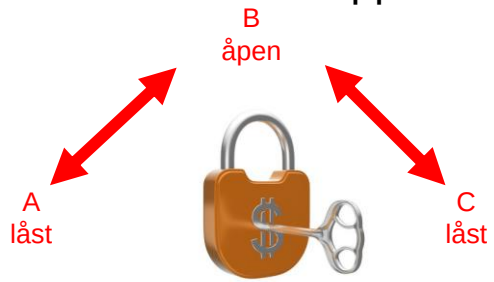


- Håkon har nok en boks med lås, men denne låsen er spesiell.
- Den har to ulike nøkler:
  - Én som kun kan vris **med** klokken (fra A til B til C)
  - Én som kun kan vris **mot** klokken (fra C til B til A)
- Den første nøkkelen holder Håkon for seg selv. Vi kaller denne Håkons «private nøkkel»
- Den andre nøkkelen kopierer Håkon i mange eksemplarer og deler ut til alle som vil ha. Dette er Håkons «offentlige nøkkel».

Asymmetrisk kryptering, scenario 1

Du vil overrekke Håkon et privat, «hemmelig», dokument:

1. Du putter brevet i boksen til Håkon (som er åpen).
2. Du låser boksen med din versjon av nøkkelen, dvs. en kopi av den *offentlige nøkkelen*, som du har fått av Håkon. Din nøkkel kan kun brukes *mot klokken*, så du låser til posisjon A.
3. Boksen er nå låst, og sendes Håkon!
4. Den eneste som kan låse opp boksen er nå Håkon, innehaveren av det vi kalte den *private nøkkelen*. Dette er den eneste nøkkelen som kan låse opp boksen *med klokken* til B.
5. Voilá!



Oppsummering asymetrisk kryptering for meldingsutveksling:

- Sender benytter mottagers offentlige nøkkel for å kryptere en melding. Mottager benytter sin private nøkkel til å dekryptere meldingen.
- Anvendes til trygg overføring av data/meldinger

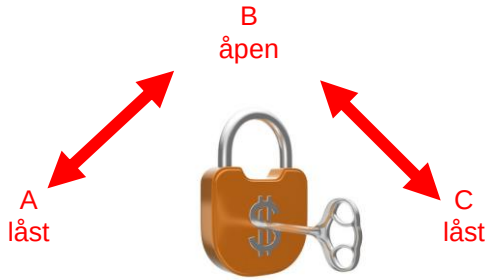
- **Hvilke sikkerhetsmål kan ivaretas?**
  - Konfidensialitet? **JA**
  - Integritet? I praksis **JA**
  - Autentisering av dataopprinnelse? **NEI**
  - Uavviselighet? **NEI**

Asymmetrisk kryptering, scenario 2

Noen overleverer deg med boksen og sier den er fra Håkon

1. Javel?
2. Ok, jeg har jo en kopi av Håkons offentlige nøkkel, så jeg finner den fram og forsøker å låse opp.
3. Vet at nøkkelen skal brukes mot klokken, forsøker dette.
4. Boksen går opp!
5. Hm, det kan jo bare betyr én ting: Boksen må være låst med Håkons private nøkkel, og innholdet må komme fra ham…

Dette kalles *digital signatur.*



Asymmetrisk kryptering for digital signering:

- Sender krypterer (og dermed signerer) en melding med sin private nøkkel. Mottager dekrypterer meldingen med senders offentlige nøkkel.
- Anvendes for å ivareta tillitt til at data/meldinger kommer fra en hevdet mottager.

- **Hvilke sikkerhetsmål kan ivaretas?**
  - Konfidensialitet? **NEI**
  - Integritet? I praksis **JA**
  - Autentisering av dataopprinnelse? **JA**
  - Uavviselighet? **JA**

- Farer: Nøkkel på avveie, falske nøkler

Krypteringsnøkler



- **Styrken i kryptografisk sikkerhet** avhenger av
  - Størrelsen/lengden på nøkkelen.
  - Håndtering og beskyttelse av nøklene.
  - Styrken i den kryptografiske algoritmen.

- **God nøkkelhåndtering** er basisen for trygg generering, lagring, distribusjon og destruksjon av nøkler.

Oppgave:

Nøkkelutveksling

Kryptografi benyttes for å beskytte informasjon mot innsyn og modifikasjon. For å kryptere og dekryptere informasjon benyttes kryptografiske nøkler. Ved assymetrisk kryptering benytter man seg av et nøkkelpar som består av en privat og en offentlig nøkkel.

Hva må til for å sikre trygg oppbevaring av en offentlig assymetrisk nøkkel?

Velg et eller flere alternativer

- ✗ Det er viktig å vite hvem som benytter en offentlige nøkkel, og brukere og systemer må derfor autentisere seg før bruk for å kunne sikre sporbarhet.
- ✗ Den offentlige nøkkelen er allmenn tilgjengelig, og trenger derfor ingen spesiell beskyttelse.
- ✗ Den offentlige nøkkelen må oppbavares på en måte som sikrer konfidensialitet samt nøkkelens integritet og ektehet.
- ✓ Den offentlige nøkkelen må oppbevares på en måte som sikrer nøkkelens integritet og ektehet.

Nøkkelutveksling og sertifikater

- Utfordring: Hvordan stole på at en offentlig nøkkel er ekte?
  Løsning: *Et sertifikat* som følger den offentlige nøkkelen knytter sammen nøkkel og en identitet.
- Neste utfordring: Hvordan stole på at sertifikatet er ekte?
  Løsning: *Sertifikatet* utstedes av en betrodd virksomhet (sertifikat-myndighet - CA), som går god for at nøklene er autentiske – altså *tilhører identiteten den utgir seg for å tilhøre*.

Men hva er et sertifikat?



- Et sertifikat består av den offentlige nøkkelen, samt en rekke attributer knyttet til nøkkelen:
  – *Eier, gyldighetsperiode, utsteder, kryptoalgoritme brukt, nøkkelstørrelse, etc.*

- Attributtene pakkes sammen og signeres av sertifikatutstederen = vi har et sertifikat

(En standard for sertifikater er såkalt X.509)

Og hvordan distribuere offentlige nøkler?

Man lager en «Offentlig-nøkkel infrastruktur» (PKI)

- PKI er et *rammeverk* for *utstedelse, administrasjon og bruk* av digitale sertifikater med offentlige nøkler
- **Hovedformål**: Sikre *ektheten* av offentlige nøkler, samt forenkle nøkkel-distribusjonen.
- PKI må inneholde:
  - En policy for sertifikat-håndtering
  - Teknologi for å implementere policyen
  - Prosedyrer for hvordan håndtere og forvalte nøklene
  - Tillittsmodell for sertifikatene med offentlige nøkler

Oppsummering: Hvordan fungerer en PKI?

- Hver eneste offentlige nøkkel bakes inn i hvert sitt *elektroniske sertifikat* som knytter nøkkel og identitet sammen.
- Et *sertifikat* utstedes av en *tiltrodd sertifikatutsteder* (Certificate Authority), som går god for den offentlige nøkkelens ekthet.
- Den tilhørende private nøkkelen kan oppbevares på en datamaskin, på SIM-kortet i en mobil, på et smartkort, i banken (Bank ID).
- Sertifikatene med de offentlige nøklene gjøres tilgjengelig for alle mottagere som skal kryptere og dekryptere meldinger.

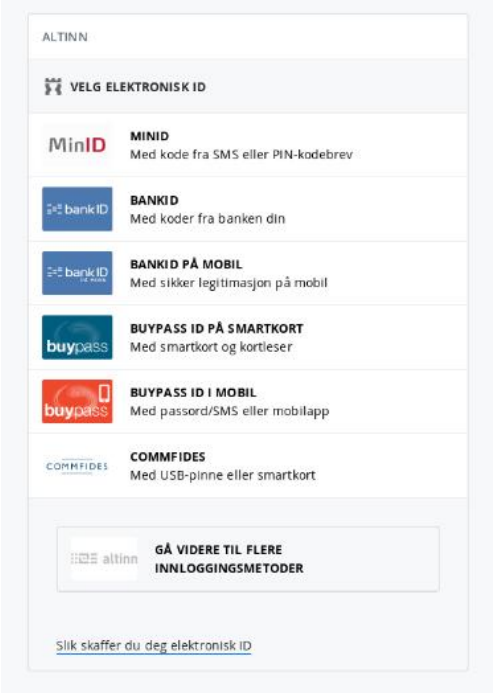
(I praksis mer komplekst enn dette, da man opererer med *hierarki av sertifikater*, *tillitskjeder*, mm. Utenfor IN1020-pensum ☺)

Eksempler på PKI-er i bruk

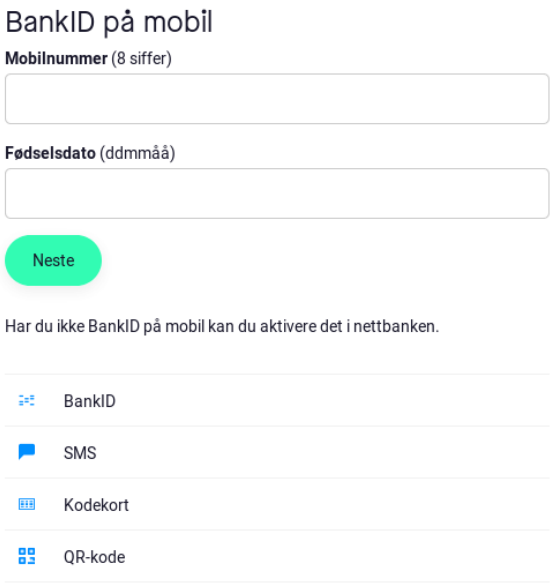
- Sikker kommunikasjon i helsevesenet:
  - eResept, elektronisk sykemelding, etc
  - Knytter melding til individ (signatur med personlig sertifikat for lege) og sikre konfidensialitet (kryptering av forsendelse).

- Publikumsrettede PKIer i Norge:
  - MinID (offentlig), BankID, Buypass, Commfides (private)
  - Difi tilbyr ID-porten, en felles infrastruktur for innlogging til offentlige tjenester, basert på ovenfornevnte.

- Web PKI eller Browser PKI
  - Nettlesere kjenner den offentlige nøkkelen til alle betrodde sertifikatutstedere (CA), og bruker denne til å forsikre seg om at sertifikatet er gyldig.



Eksempel: Tjenesten BankID



- Tilbyr en «elektronisk legitimasjon» - eID
- Obligatorisk to-faktor-autentisering
- Baserer seg på en PKI:
  - BankID på mobil: SIM-lagret privat nøkkel
  - BankID: Banklagret privat nøkkel
- Bruksområder:
  - Autentisering og digital signering basert på kryptografi
- Brukes (som en av flere eIDer) av offentlige tjenester og banker

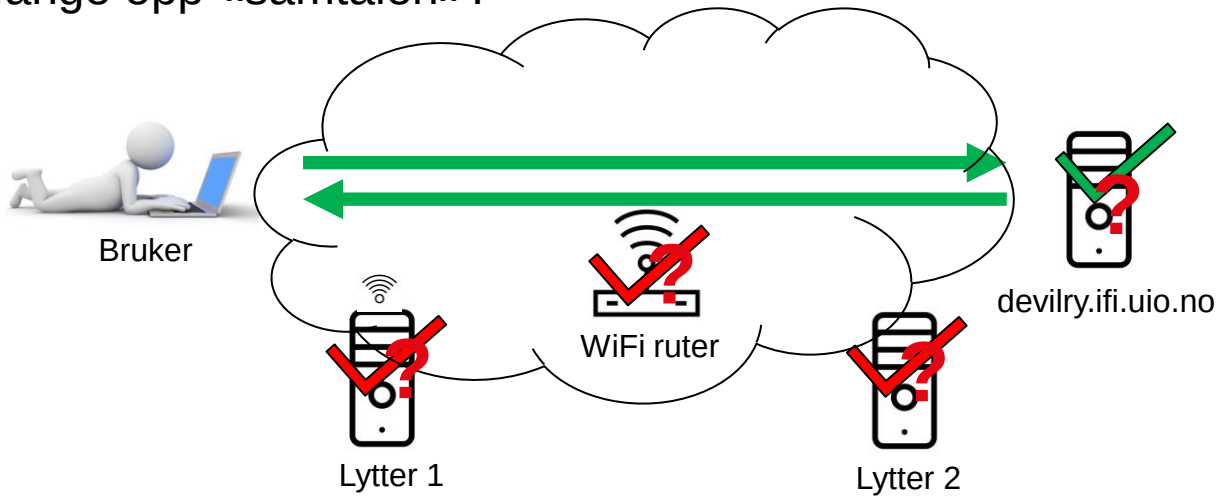
For den interesserte:
https://vipps.no/documents/29/BankID_sertifikatpolicy_v2.0_for-kvalifiserte-sertifikater-fysiske-personer-banklagret.pdf

Illustrasjon: Sikkerhet i trådløse nett

Kommunikasjonskanal til devilry.ifi.uio.no

Ukryptert forbindelse (eks. http) via ukryptert nett.

Hvem kan fange opp «samtalen»?

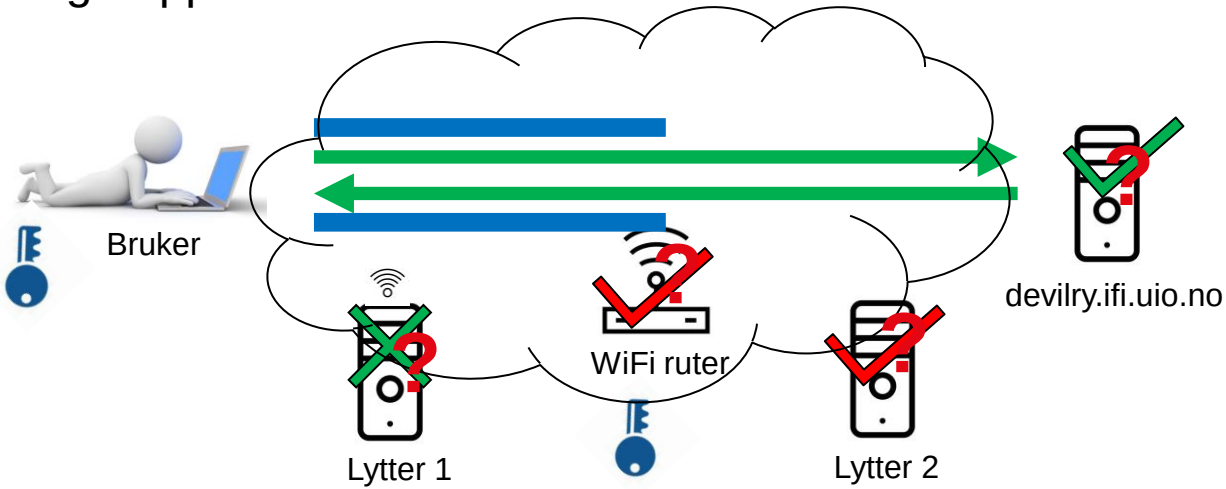


Sikkerhet i trådløse nett

Kommunikasjonskanal til devilry.ifi.uio.no.

Kryptert forbindelse til WiFi-ruter.

Hvem kan fange opp «samtalen»?

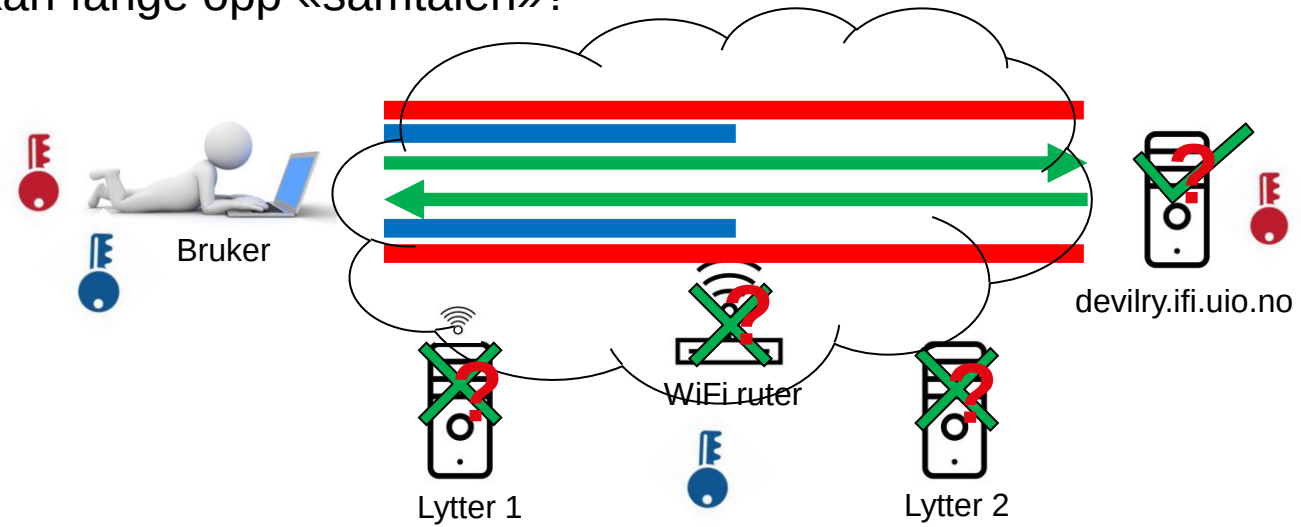


Sikkerhet i trådløse nett

Kommunikasjonskanal til devilry.ifi.uio.no.

HTTPS-forbindelse til wifi-ruter og devilry.ifi.uio.no.

Hvem kan fange opp «samtalen»?



Eksempel på sårbarhet:
Heartbleed



- OpenSSL er en svært vanlig brukt *implementasjon* av TLS-protokollen
- Heartbleed var en sårbarhet *introdusert* i OpenSSL i 2012, men ble ikke offentlig kjent før i 2014.
- Gjorde det mulig for hvem som helst (på internett) å lese minnet til systemer som var beskyttet med OpenSSL:
  - Mulig for angripere å få tak i private nøkler
  - Mulig for uvedkommende å avlytte alle data som ble transportert mellom tjenester og brukere

Lærdom: Selv kritisk programvare basert på åpen kildekode kan inneholde sårbarheter

Oppgave:

I hvilke situasjoner benyttes gjerne kryptografi som sikkerhetstiltak?

Velg et eller flere alternativer

- [x] For trygg lagring av informasjon på utrygge langringsenheter.
- [x] For trygg overføring av informasjon i datanettverk.
- [ ] For å bidra til å detektere innbrudd i datasystemer.
- [x] For å sikre korrekt sikkerhetskopiering av informasjon.

Dagens læringsmål

Kryptering som sikkerhetstiltak:

- Symmetrisk kryptering og bruksområder
  - Hva kjennetegner symmetrisk kryptering
  - Hvordan kryptere data og melding(er)
- Asymmetrisk kryptering og oversikt over bruksområder og utfordringer:
  - Hva kjennetegner asymmetrisk kryptering
  - Bruksområder, hvordan:
    - Kryptering av data og melding(er)
    - Digital signatur
  - Hvorfor vi trenger sertifikater og Offentlig nøkkel-infrastruktur (PKI)

Takk for i dag!

mn.uio.no/ifi

