IN1020, Gruppe 5

Uke 8

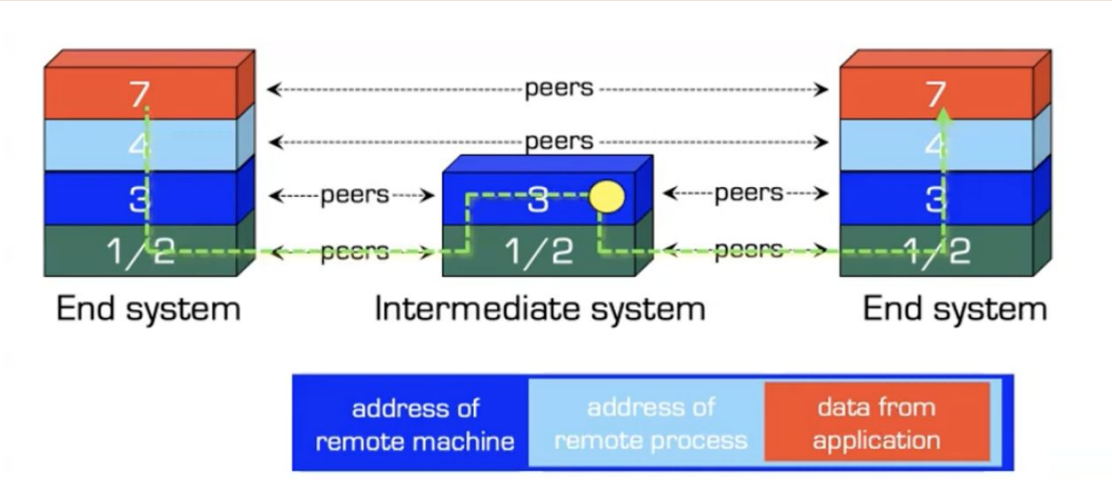
Velkommen :)

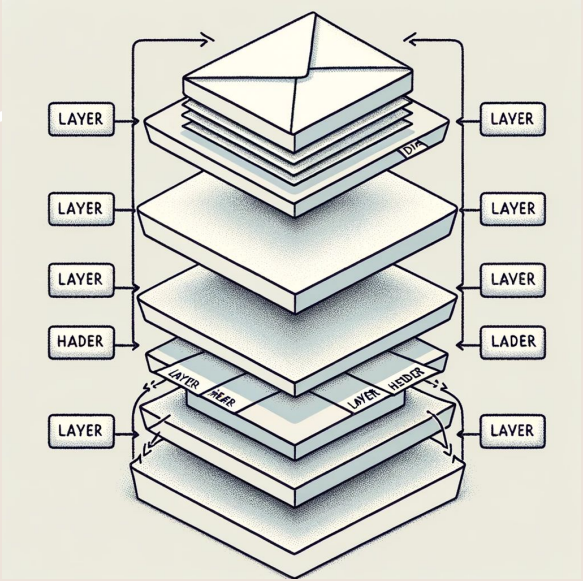
Agenda

- Repetisjon:
  - Lagdelingsmodellen
  - aksessmodellen
- Kryptografi:
  - Symmetriske og asymmetrisk kryptering

Menti

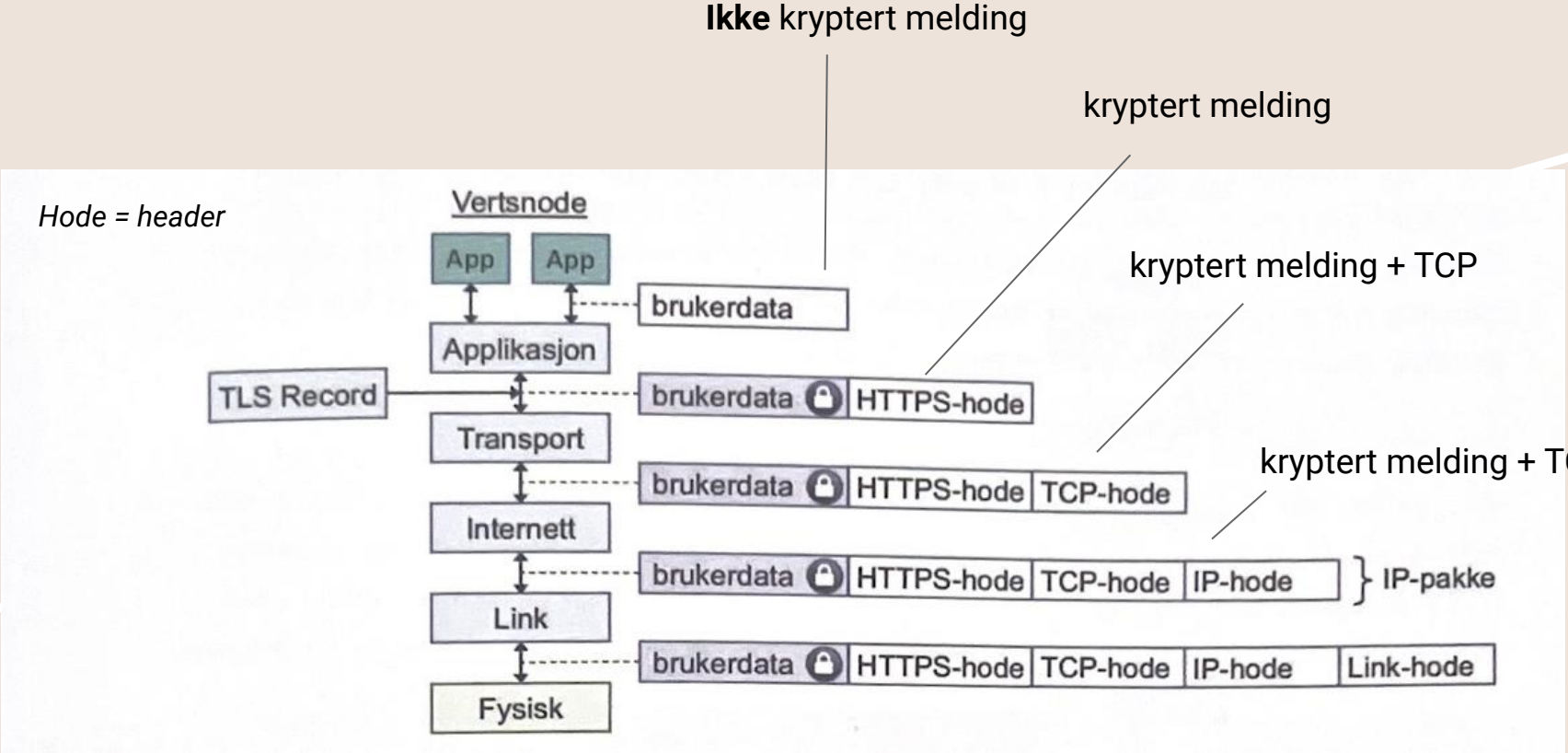
- Kommunikasjonen nedover lagene med hjelp av protokoll kan beskrives som å sende et brev i en konvolutt.
- Hvert lag legger til sin egen protokoll-informasjon for å sikre korrekt overføring.
- Dette er som å legge til adresser og annen relevant informasjon på en konvolutt.
- På mottakersiden blir denne informasjonen fjernet lag for lag





AI - generert

Protokollene

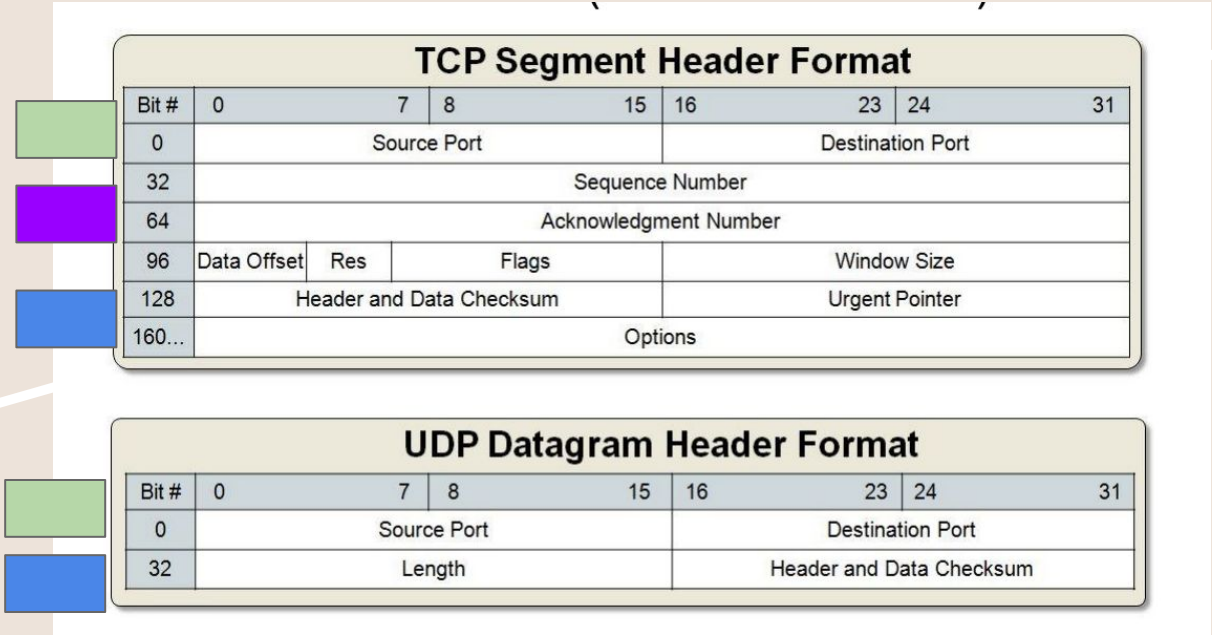


Transportlaget

- *Grønn*: En pakke må først gjennom porten
- *Lilla*: TCP har ACK, UDP har ikke
- *Blå*: Resten er for innholdet i dataen

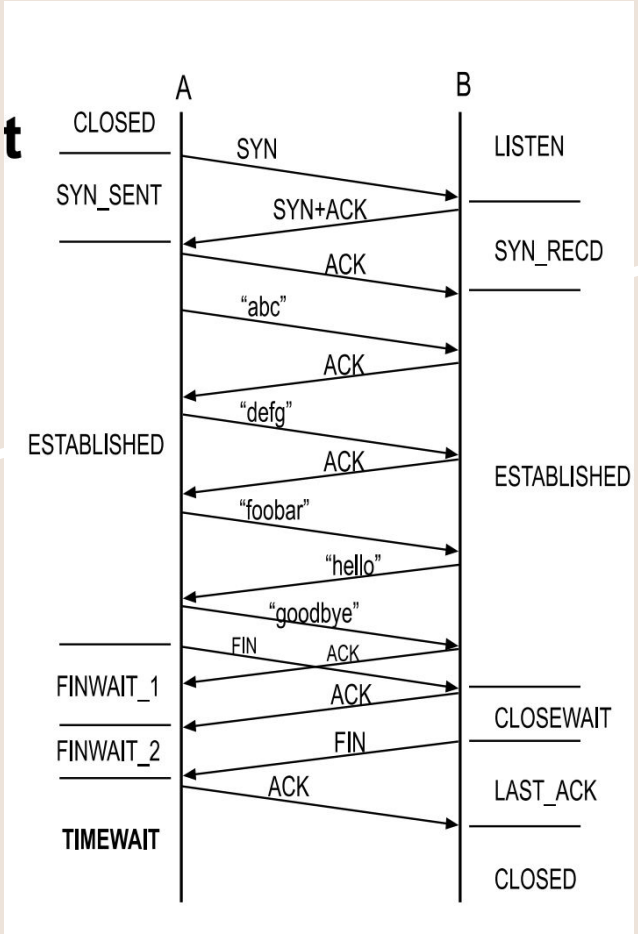
TCP: HTTP, E-post, filoverføring, etc.

UDP: Strømming av video og lyd



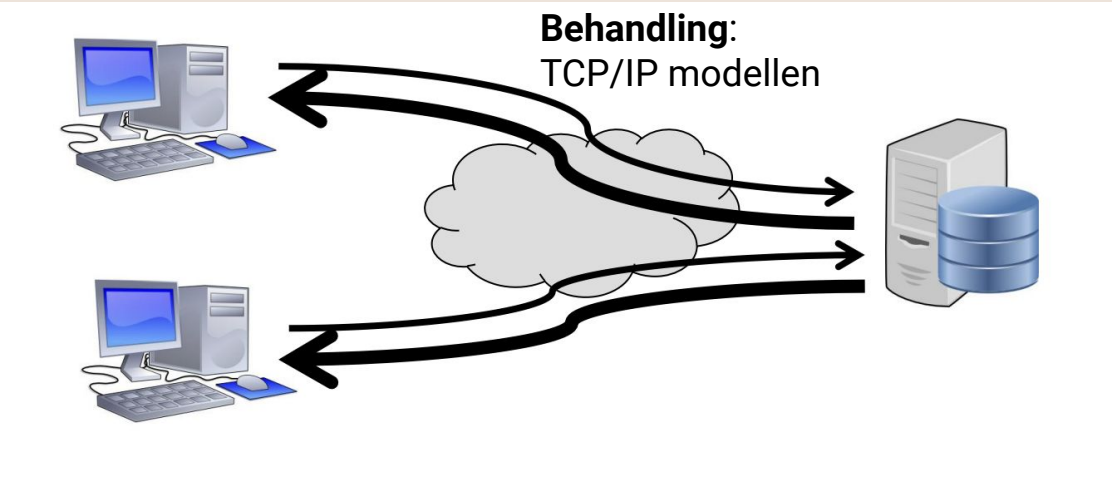
ACK = Kvittering

Egenskap	TCP	UDP
Oppsett av forbindelse (3-way handshake)	Ja, 3-veis håndtrykk kreves for å etablere forbindelsen.	Nei, ingen forbindelsesoppsett.
Pakkene leveres i riktig rekkefølge	Ja, TCP garanterer at pakkene blir levert i riktig rekkefølge.	Nei, ingen garanti for rekkefølge.
Pålitelighet	Ja, TCP er pålitelig. Pakker sendes på nytt hvis kvitteringen (ACK) ikke kommer frem.	Nei, UDP gir ingen pålitelighetsgarantier.
Flytkontroll og metningskontroll	Ja, TCP har innebygd flytkontroll og metningskontroll for å unngå overbelastning av nettverket.	Nei, UDP har ingen innebygd flytkontroll eller metningskontroll.
Feilsjekking av nyttelasten (sjekksum)	Ja, TCP bruker en sjekksum for å kontrollere integriteten til dataene.	Ja, UDP bruker også en sjekksum for å kontrollere integriteten til dataene.



Klient-og tjener

Forespørsel:
Søker på “IN1020” i Google



Respons:
Webserveren sender nettsiden forespurt

Forbindelssestrategier

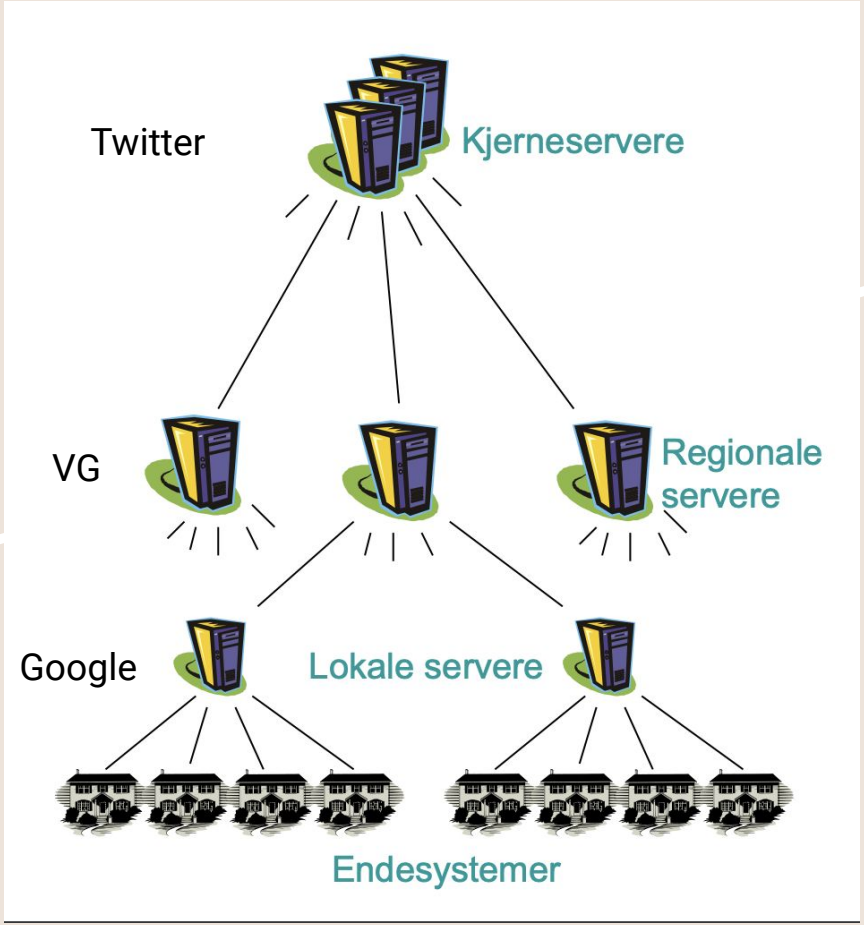
- Pull: Klienten ber om en tjeneste (vanligste metoden)
- Push: Tjeneren «dytter» en tjeneste (beskjed) til klienten
- Publish-subscribe: Push, tjeneren dytter ut beskjeder til en gruppe av abonnenter

CDN

1. **Lokale servere:** Dette er severe som er plassert fysisk nært brukerne. Ofte innenfor samme bygning

2. **Regionale servere:** Dette er servere som betjener en bestemt geografisk region

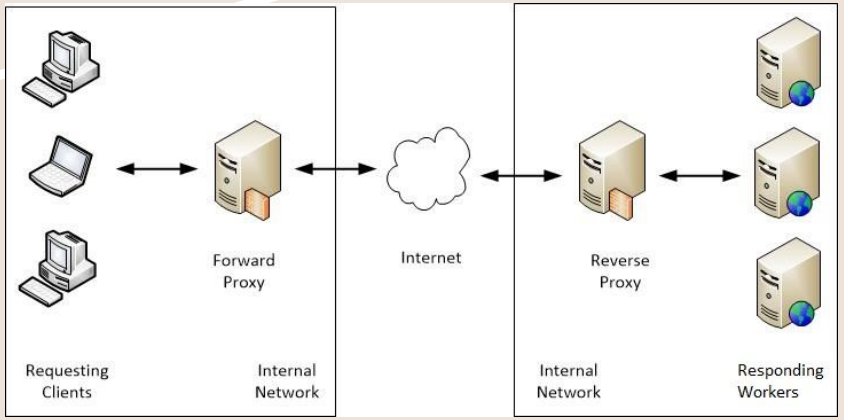
3. **Kjerneservere:** Ment for store nettsider som blir brukt av flere brukere fra hele verden.



Proxy – cache

Mellomlagrer data for slik at man ikke behøver å gå helt til kilden

- **Forward Proxy:** Står nær klienten og mellomlagrer data for klientene, slik at de ikke trenger å gå helt til kilden.
- **Reverse Proxy:** Står nær tjener og mellomlagrer data fra én eller flere tjenere, slik at klienten slipper å gå helt til kilden.

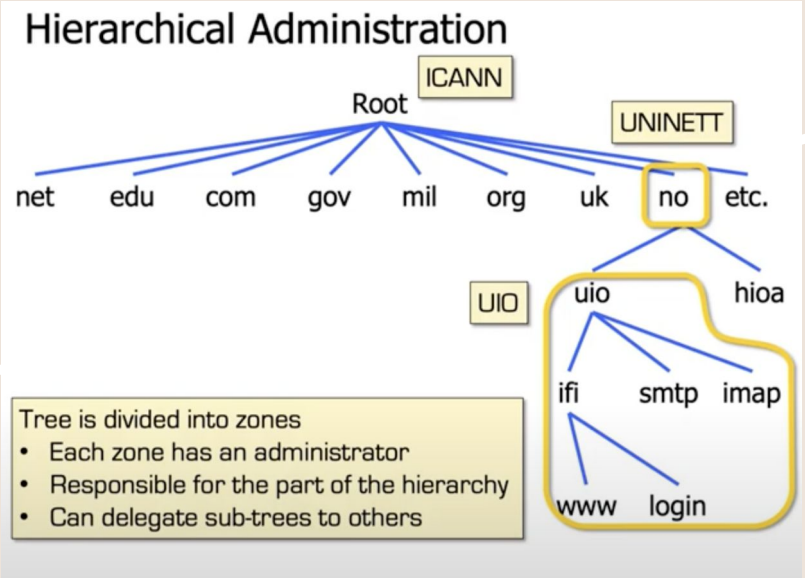


DNS

- Bruk av DNS (Domain Name System)
- Nettadresser f.eks. www.google.com
- Bak navnet ligger det en IP-adresse
- Strukturen begynner fra enden:

f.eks.: .com → google.com → mail.google.com

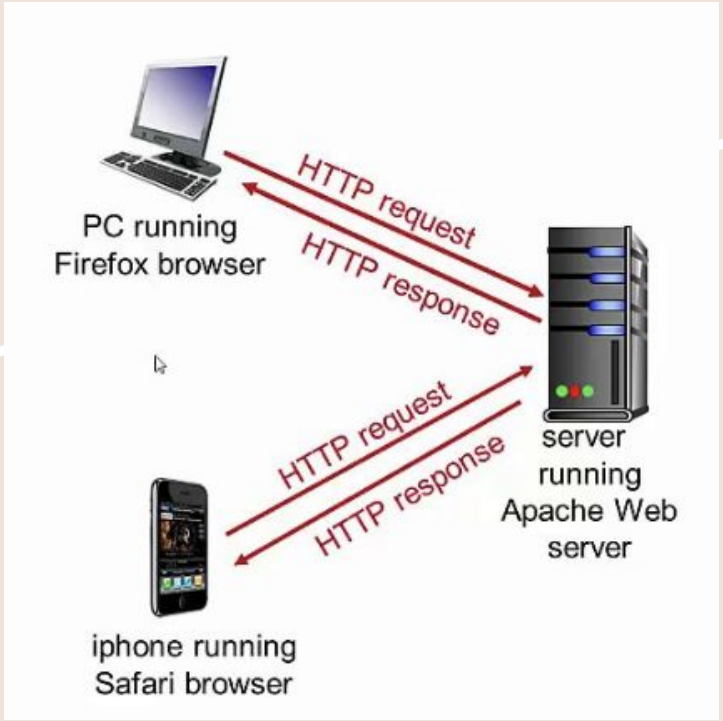
- Hver sone har en ansvarlig administrator
- Toppnivådomenet = (TLD)



HTTP

- Dette er HTTP applikasjonslagets protokoll for web
- Klienten: nettleser som spør etter, får og viser webobjekter
- Tjener: sender webobjektet som svar på forespørsel

1. HTTP: bruker TCP som transport:
2. Klienten oppretter en TCP-forbindelse il tjeneren, port 80
3. Tjeneren godtar TCP-forbindelsen fra klienten
4. HTTP-meldinger (protokollmeldinger på applikasjonslaget) utveksles
5. TCP-forbindelsen lukkes



HTTP/1.x response statuskoder (eksempler)

200 OK

- Forespørselen var vellykket, objektet kommer senere i meldingen

301 Moved Permanently

- Objektet har byttet plassering. Referanse til ny plassering kommer senere I meldingen.

400 Bad Request

- Forespørselen var uforståelig for tjeneren

404 Not Found

- Dokumentet ble ikke funnet på tjeneren

505 HTTP Version Not Supported

Kryptering

SSL -> TLS - > HTTPS

Applikasjonslaget
Transportlaget
IP/Internett
Linklaget
Fysiske lag

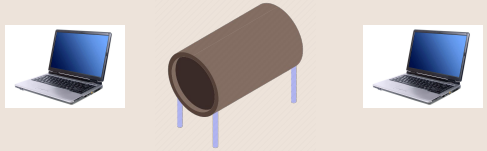
Secure Sockets Layer – (**https**) Kryptering for ende-til-ende Applikasjoner – f.eks. nettbank eller butikker.

VPN (IPSEC etc.) – Kobler to nettverk sammen så det fungerer som ett LAN selv om de er fysisk adskilt

WPA – WiFi Protected Access - Kryptering på trådløse nettverk, krypterer forbindelsen mellom deg og aksesspunkt/ruter.

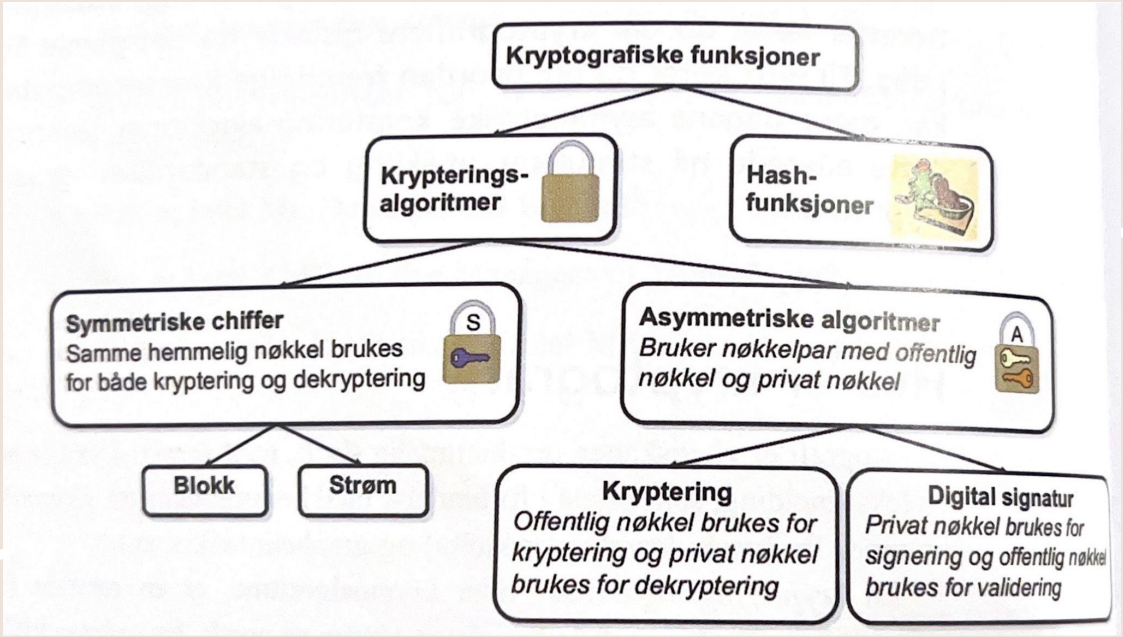
Kryptering på flere lag gjør det vanskeligere for uvedkomne å lytte til kommunikasjonen. Adressen (avsender / mottakeren) er vanskelig å kryptere, da router må vite hvor pakken skal leveres.

VPN /IPSEC -> krypterte forbindelser gjennom åpne nett (internettet)



Kryptert forbindelse

Kryptografi = skjule betydningen av en tekst



Kryptere: gjøre hemmelig

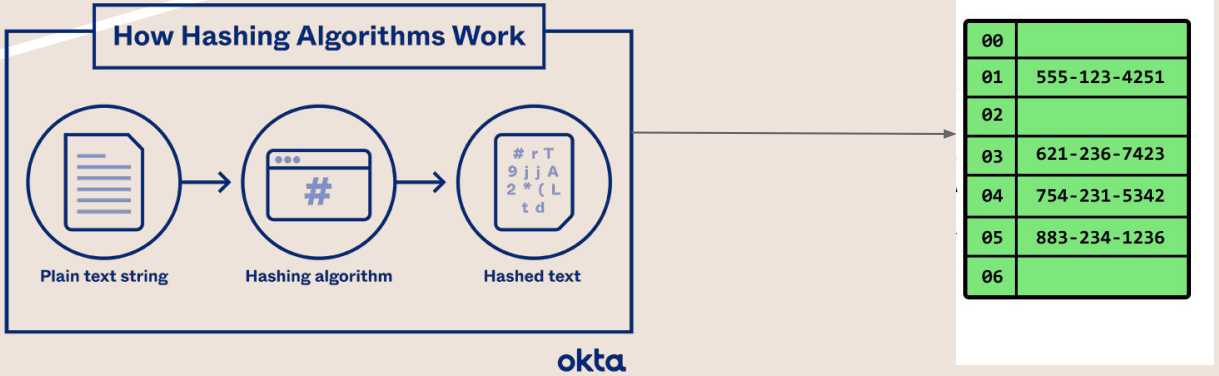
Dekryptere: Gjøre synlig

(*Chiffer = Krypteringsalgoritme*)

Hash-funksjoner

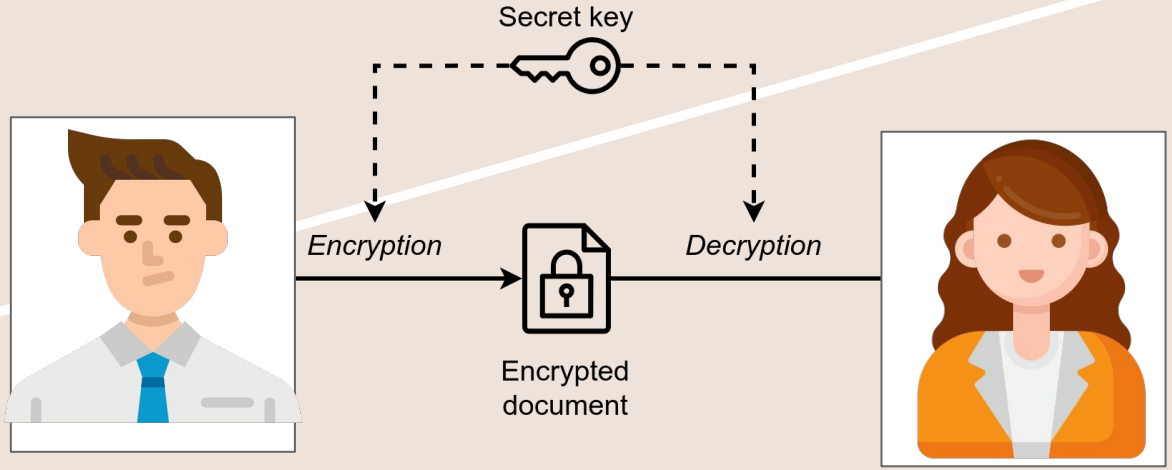
Enveis identifikasjon – Ingen nøkkel

- Konverterer data av en størrelse til en hash-verdi av fast størrelse.
- Samme melding skal alltid produsere samme hash-verdi



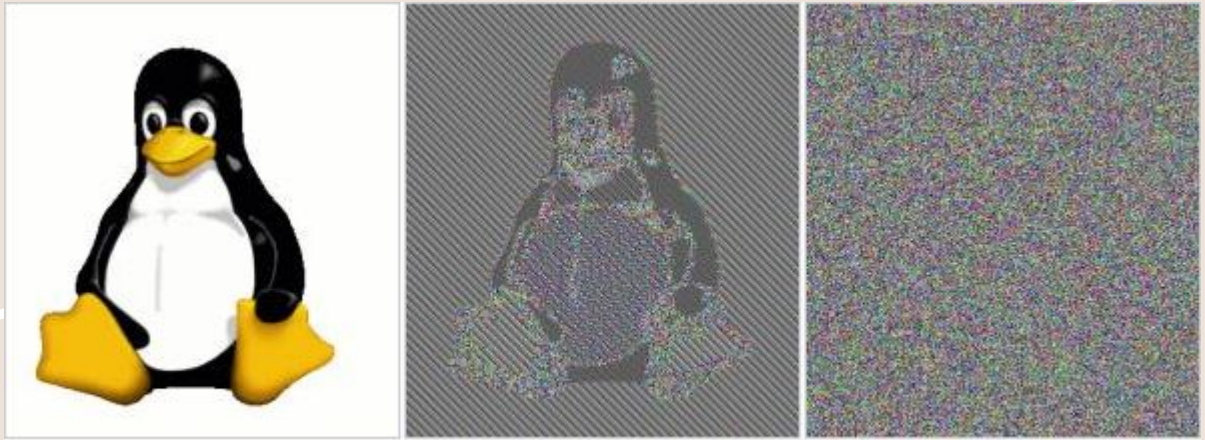
Symmetrisk kryptering (Blokk)

- Samme nøkkel benyttes for både kryptering og dekryptering
- AES mest brukte blokkchiffer, tre størrelser 128, 192 eller 256 bits



Blokk-kryptering transformasjon av en blokk med et visst antall bits

- ECB (litt usikke)



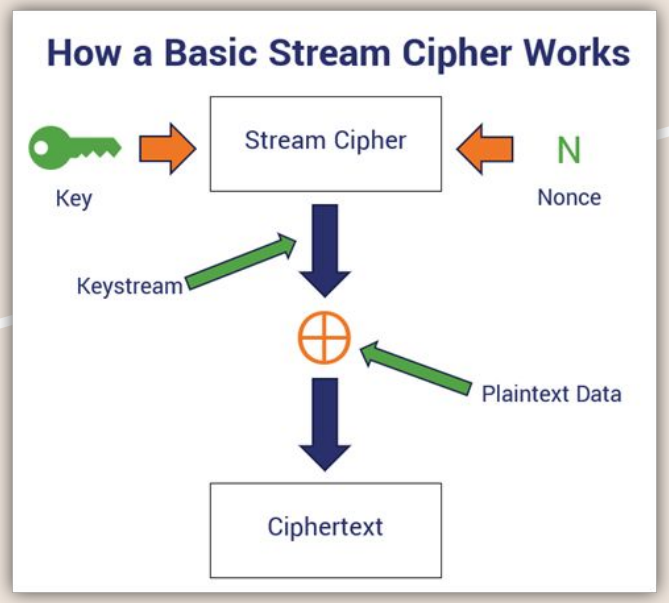
Original image

Encrypted using ECB mode

Modes other than ECB result in pseudo-randomness

Symmetrisk kryptering – Strøm

- Bruker strøm for å kryptere



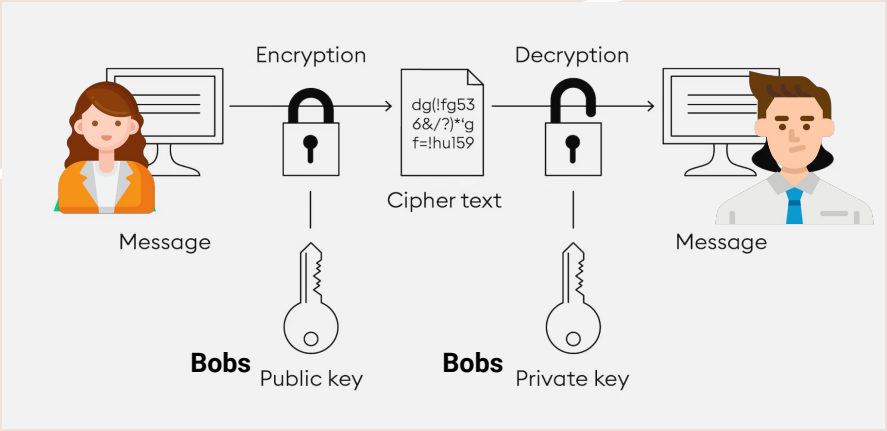
Asymmetrisk kryptering

- *Her benytter man seg av mottakerens nøkler*

1. Alice sender melding til Bob
2. Alice **genererer** hemmelig nøkkel og bruker **symmetrisk kryptering** for å kryptere meldingen
3. Alice bruker **asymmetrisk krypterering** på hemmelig nøkkel med Bobs offentlig nøkkel
4. Alice sender krypterte chiffertekstene og den hemmelige nøkkelen til Bob
5. Bob dekrypterer hemmelig nøkkelen med sin egen (Bobs) private nøkke
6. Bob dekrypterer meldingen med symmetrisk kryptering



Alice:
Privat og public





Bob:
Privat og public

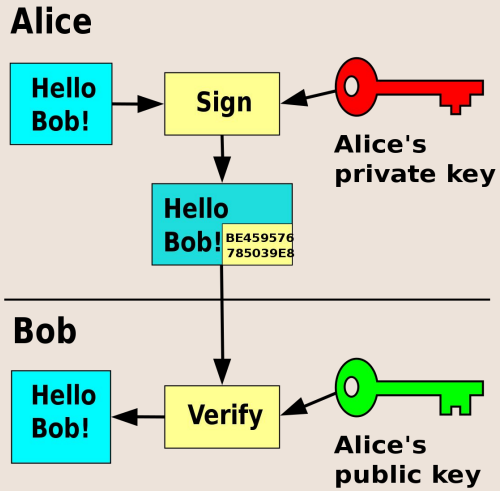
Digital signatur

Her benytter man seg av avsenderens nøkler

- **Privat nøkkel:** Din hemmelige nøkkel. Alice bruker den for å "låse" eller signere et dokument.
- **Offentlig nøkkel:** En nøkkel alle kan se. Den brukes for å sjekke at det Alice signerte virkelig er ditt.

Hvordan dette fungerer: Alice sender melding til Bob

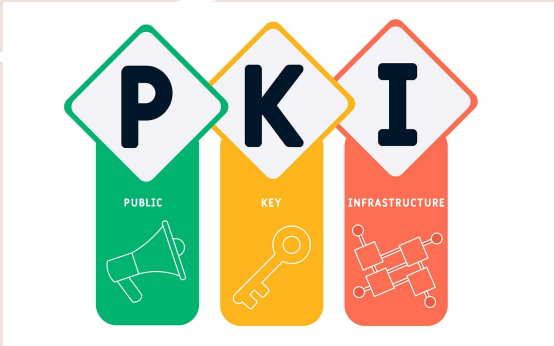
- **Signere**: Alice bruker sin private nøkkel til å lage en spesiell kode på dokumentet.
- **Sjekke**: Bob bruker Alice sin offentlige nøkkel til å se at koden passer og at dokumentet er ekte.



PKI

- Alice “genererer” hemmelig nøkkel
- PKI, eller Offentlig-nøkkel infrastruktur, er et system designet for å sikre og administrere digitale nøkler og **sertifikater**.
- Hovedformål er å bekrefte offentlige nøkler, sikre trygg distribusjon av disse nøklene, og etablere tillit gjennom strenge prosedyrer, og retningslinjer.

Eksempel : BankID, Feide -> hvor enn man logger inn med asymmetrisk kryptering



3.5 Symmetrisk kryptering

Symmetrisk kryptering er en av flere kategorier kryptering som benyttes innen databasert kryptografi.

Hvilke påstander om symmetrisk kryptering er sanne og hvilke er usanne?

	Usant	Sant
Kan brukes for å sikre uavviselighet.	○	○
Benyttes til såkalt digital signatur.	○	○
Kan brukes for å sikre konfidensialitet for data.	○	○
Baserer seg på bruk av et nøkkelpar bestående av en privat og en offentlig kryptografisk nøkkel.	○	○
Symmetrisk kryptering ødelegger meldingen slik at den aldri kan dekrypteres	○	○
Benyttes til kryptering av hemmelige meldinger.	○	○
Trygg utveksling av den hemmelige kryptografiske nøkkelen er en sikkerhetsutfordring.	○	○
Sender og mottager deler én felles, hemmelig kryptografisk nøkkel.	○	○

Maks poeng: 4

3.5 Symmetrisk kryptering

Symmetrisk kryptering er en av flere kategorier kryptering som benyttes innen databasert kryptografi.

Hvilke påstander om symmetrisk kryptering er sanne og hvilke er usanne?

	Sant	Usant
Benyttes til kryptering av hemmelige meldinger.	✔	
Baserer seg på bruk av et nøkkelpar bestående av en privat og en offentlig kryptografisk nøkkel.		✔
Symmetrisk kryptering ødelegger meldingen slik at den aldri kan dekrypteres		✔
Benyttes til såkalt digital signatur.		✔
Sender og mottager deler én felles, hemmelig kryptografisk nøkkel.	✔	
Trygg utveksling av den hemmelige kryptografiske nøkkelen er en sikkerhetsutfordring.	✔	
Kan brukes for å sikre konfidensialitet for data.	✔	
Kan brukes for å sikre uavviselighet.		✔

Maks poeng: 4

Ukesoppgaver:)