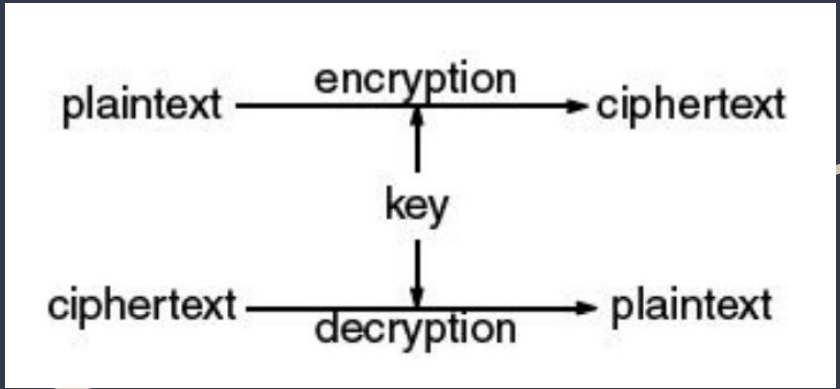
IN1020 gruppetime nr 4

- Kryptering, PKI og sertifikater
- Tjenester i internet

Hva er kryptografi?



“Kunsten å skjule budskap”

Algoritme -> oppskrift

Nøkkel -> hemmelighet

Viktige begreper:

“plaintext, ciphertext, kryptering, dekryptering.”

Hvorfor trenger vi kryptografi?

Digital kommunikasjon er sårbar → noen kan lytte, endre eller utgi seg for å være andre.

Kryptografi beskytter:

- **Konfidensialitet** – holde hemmelig
- I**ntegritet** – oppdage endringer
- **Autentisering** – vite hvem som snakker
- **Uavviselighet** – hindre benektelse i etterkant (signaturer).

Forskjellige typer kryptering

Symmetrisk kryptering

1 nøkkel, deles mellom sender og mottaker

Brukes til litt obskure ting (IPsec, OpenVPN osv)

Hash-algoritmer

Sikre integritet, eller data må lagres i en form som ikke kan reverseres

Lagring av passord

Sjekksum algoritmer

Asymmetrisk kryptering

Bruker **to nøkler,** en offentlig og en privat.

Digital signatur

Symmetrisk kryptering

“Hva kan konsekvensene være hvis en hemmelig nøkkel kommer på avveie?”

Hashing

“Hva er styrken til hash-algoritmer, og hvorfor kan de ikke brukes til kryptering?”

SYMMETRISK		ASYMMETRISK
Kan bruke åpne kanaler for nøkkeldistribusjon	Ødelegger data slik at de ikke kan dekrypteres	Kan sikre uavviselighet
Benyttes for digital signering	Sender og mottager deler en felles hemmelig nøkkel	Brukes for HTTPS alene
Trygg nøkkelutveksling er utfordrende	Raskere og mer effektiv enn den andre	Nyttig for å kryptere store mengder data
Kan sikre autentisk dataopprinnelse	Nøkkelfri kryptering	Kan sikre autentisk dataopprinnelse

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.	○	○

PKI

Public Key Infrastructure

Et system for å administrere offentlige og private nøkler

-> Skal knytte offentlig nøkkel til en identitet

Hvorfor: Vi må kunne stole på at en offentlig nøkkel virkelig tilhører den den utgir seg for å være.

Digitale sertifikater

Et **sertifikat** er som et digitalt pass eller førerkort for en nøkkel.

Inneholder:

- Offentlig nøkkel
- Informasjon om eieren (f.eks. www.uio.no)
- Gyldighetsperiode

  Signatur fra en **tillitsinstans** (Certificate Authority – CA).

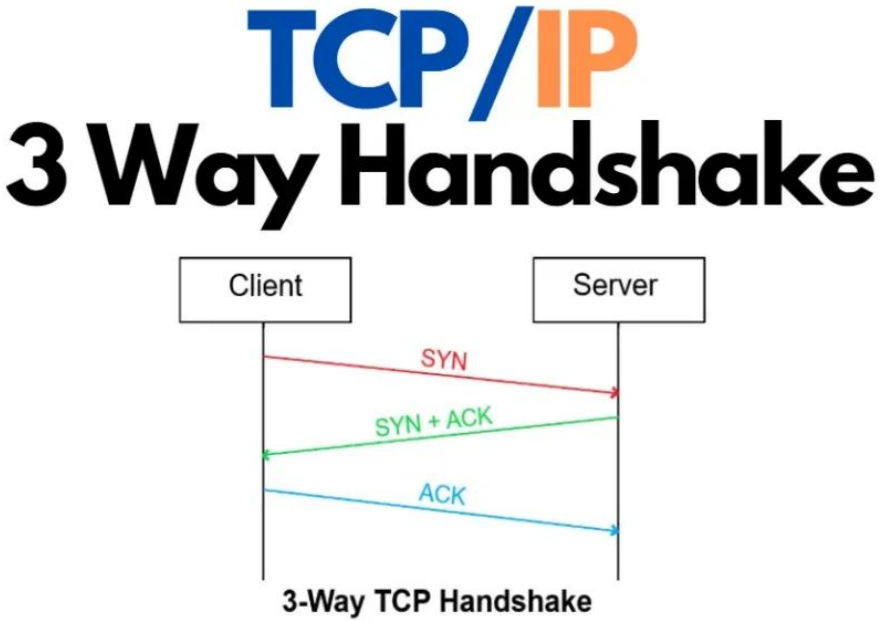
  - Passkontor for nøkler

Transportlaget

TCP

Transmission Control Protocol

Transportlaget



Transmission Control Protocol

Transportlaget

Flytkontroll:

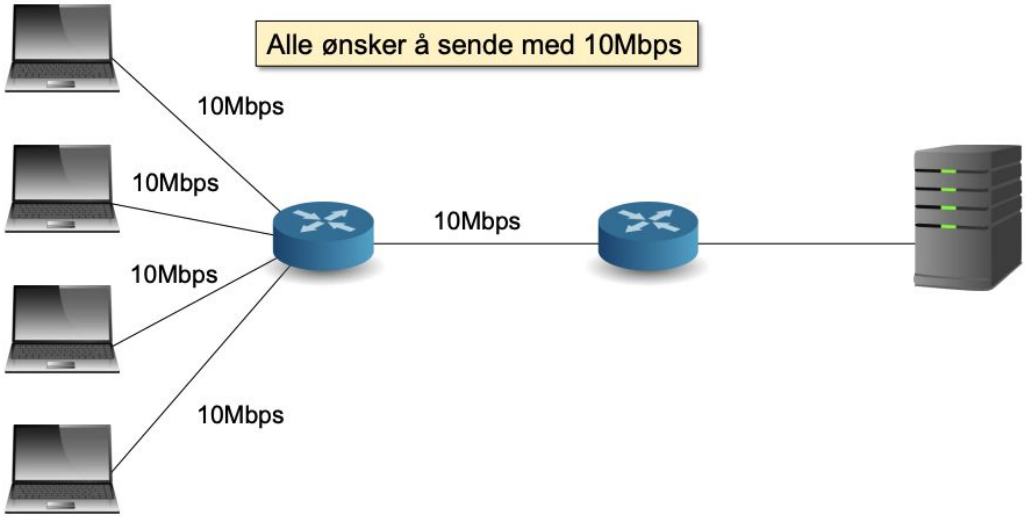
“Ikke overbelaste mottaker”

Transmission Control Protocol

Transportlaget

Metningskontroll:

“Ikke overbelaste nettverket”

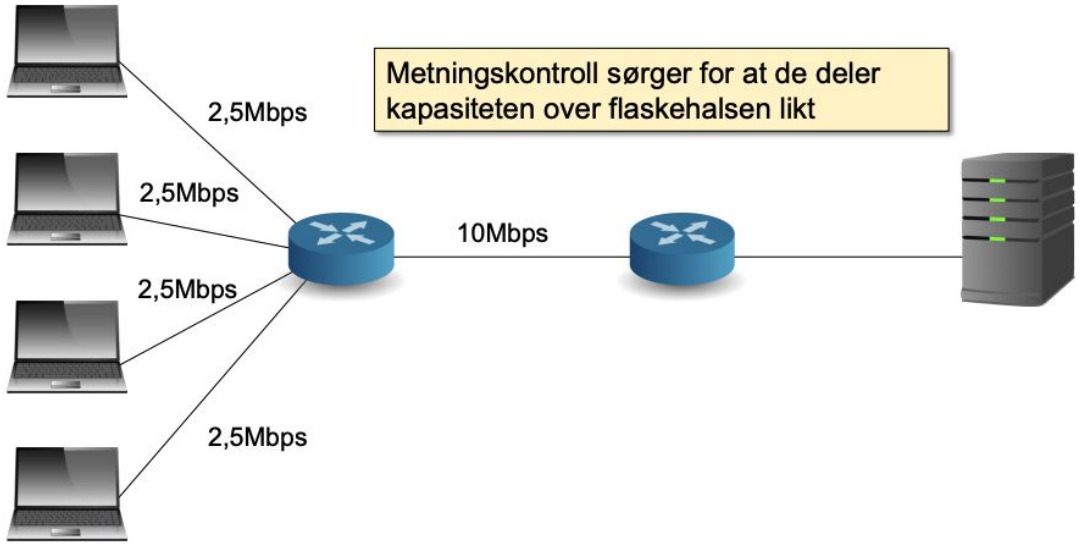


Transmission Control Protocol

Transportlaget

Metningskontroll:

“Ikke overbelaste nettverket”

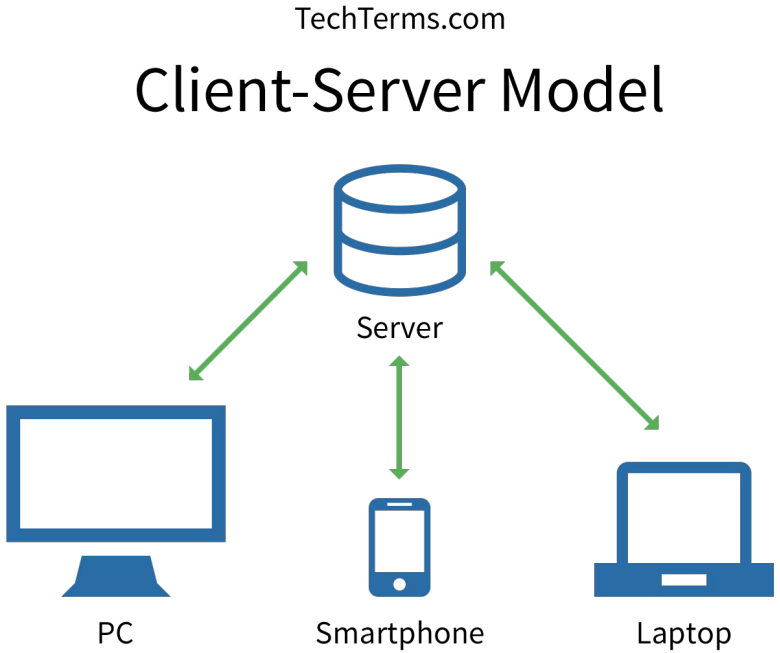


Nyttige nettverksverktøy

Verktøy	
ping	Måler forsinkelsen mellom din maskin og en annen på internett
traceroute	Gir informasjon om hvert hopp en datapakke er innom på vei til målet.
tracepath	Samme som traceroute, men trenger ikke superusertilgang
netstat	Gir informasjon om nettverksforbindelser på din maskin
dig	Gjøre DNS-oppslag og se hva som returneres.
whois	Slå opp hvem som eier/disponerer en IP-adresse
tcpdump / wireshark	Logge pakker som går inn og ut av maskinen, samt utføre analyse

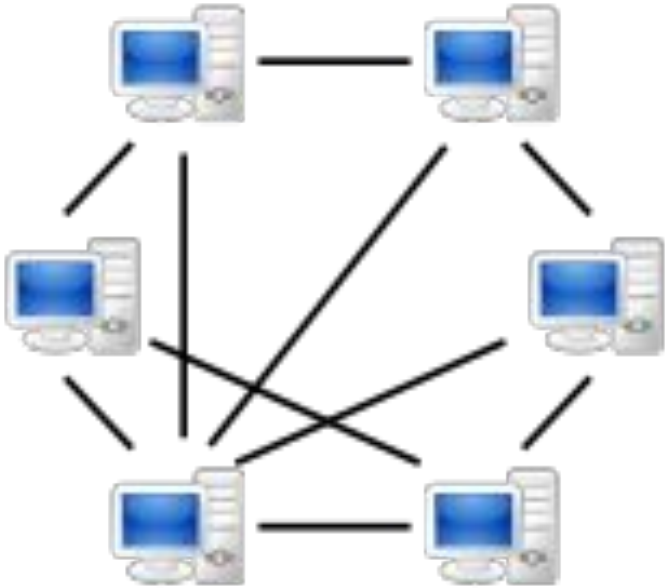
Aksessmodeller

Klient - Tjener



Aksessmodeller

Peer 2 Peer



4.1 Klient-tjener

Hva kjennetegner aksessmodellen klient-tjener?
Velg ett eller flere alternativer

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

CDN - Content Delivery Network

“Lagrer” populært innhold

Mange McDonalds restauranter, i stedet for 1

