

Datatransport og kryptografi

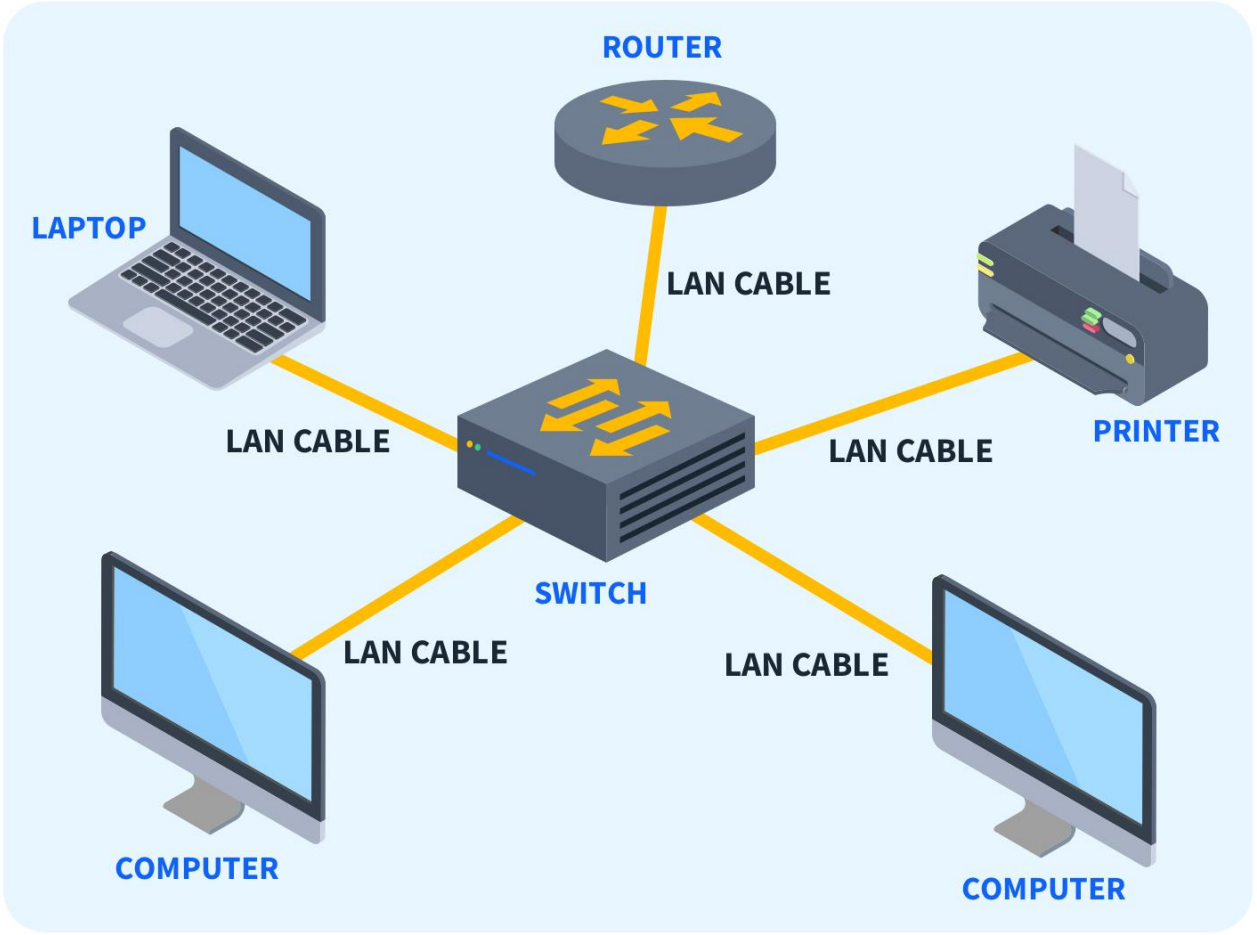
Gruppe 6 og 17

LAN og IP-adresse

- Adresser på internett
- F.eks. Ole Johan Dahls hus, Gaustadalléen 23B

- Internett er et sammenkobling av mindre, seperate nettverk
- Brukt med switch og HUB

- For å sende pakke utenfor LAN må den sendes til en router som vet hvor den skal videre



IPv4

192.168.1.5

11000000.10101000.00000001.00000101

IP-adresse

255.255.0.0

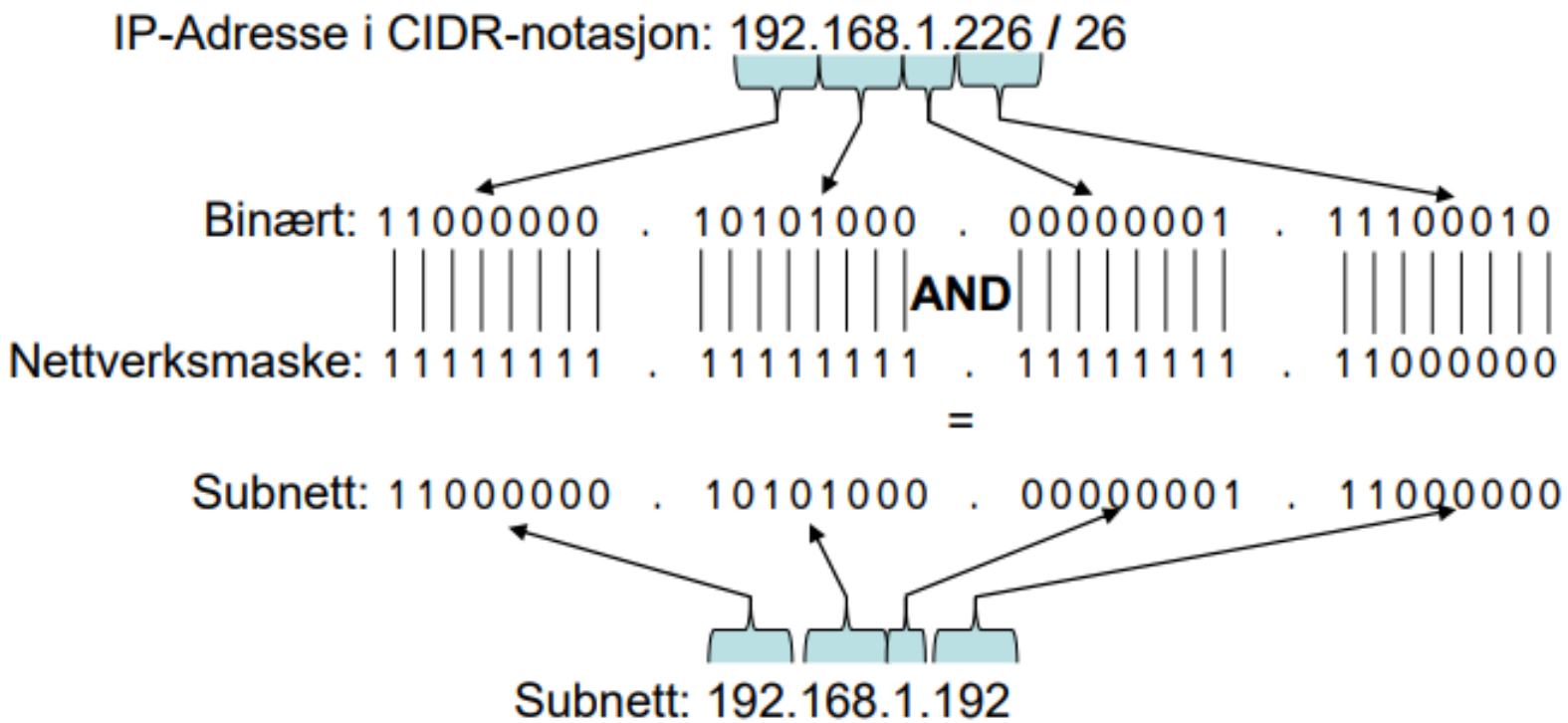
11111111.11111111.00000000.00000000

Nettverksmaske

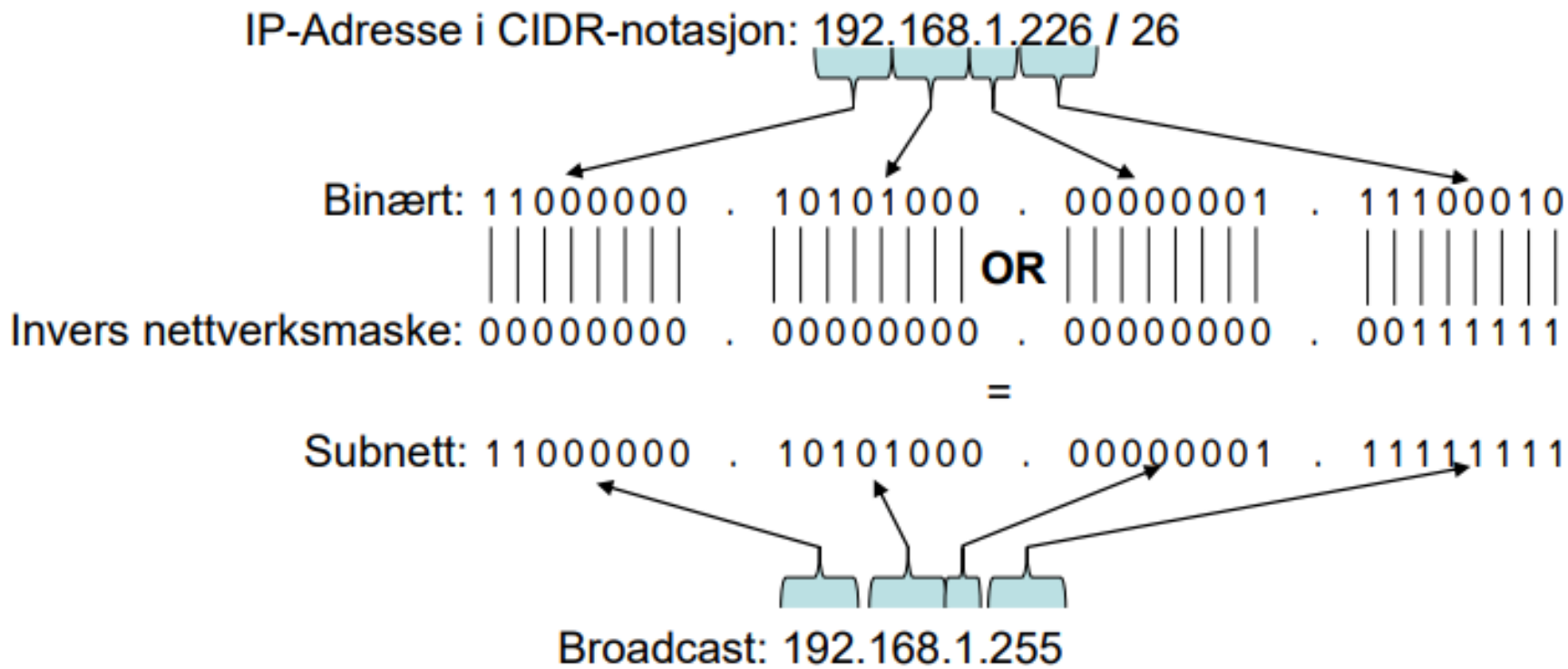
CIDR-notasjon:
Kan skrive 192.168.1.5/16 som viser både IP og nettverksmaske

Punktnotasjon

Eksempel: Subnettadresse fra IP / Nettverksmaske

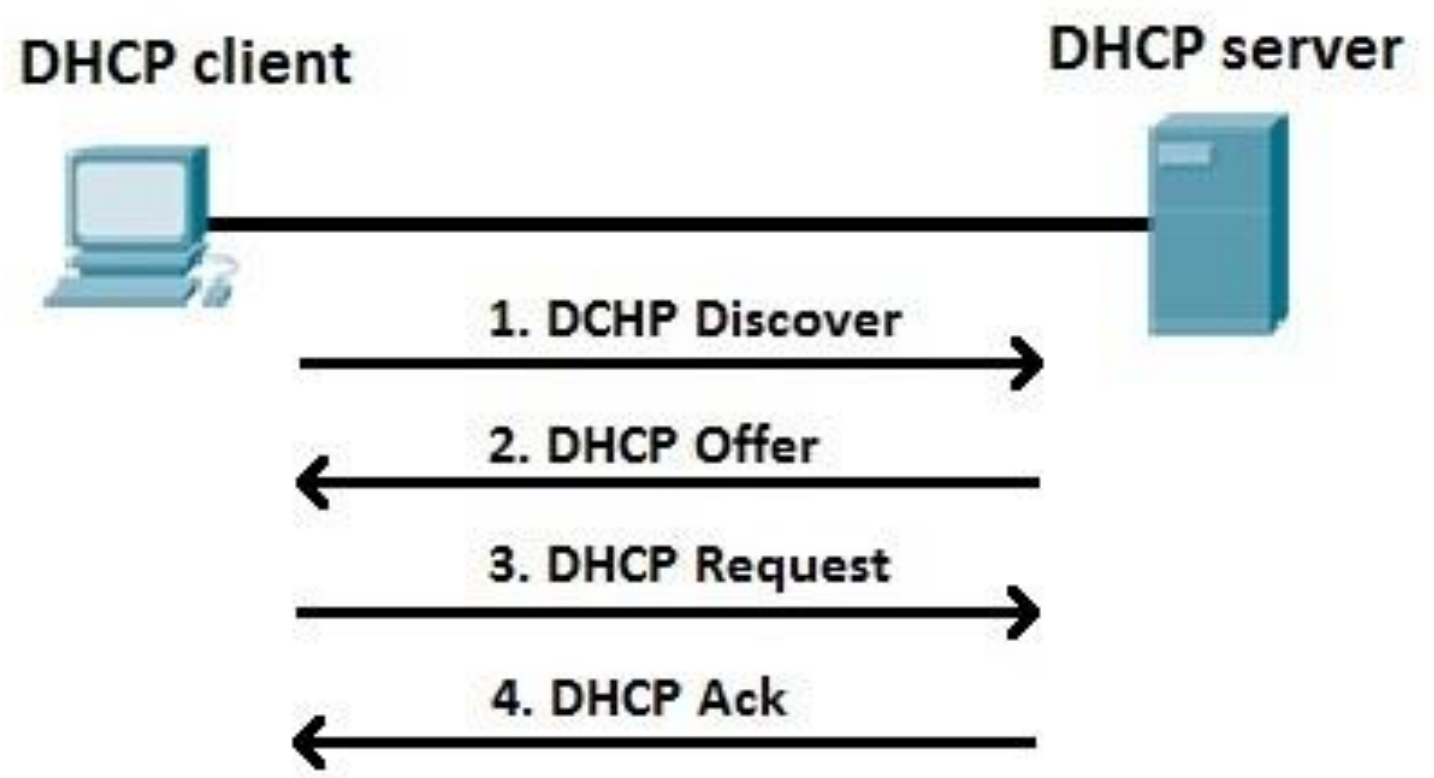


Eksempel: Kringkastingsadresse fra IP / Nettverksmaske



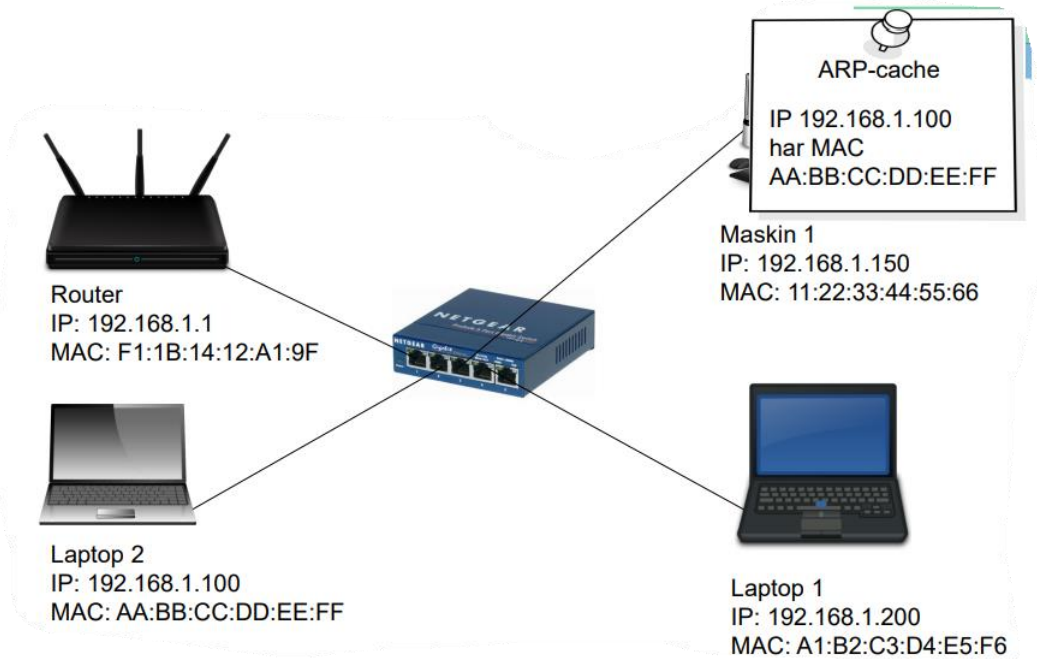
DHCP

- Automatisk utdeling av IP-adresser

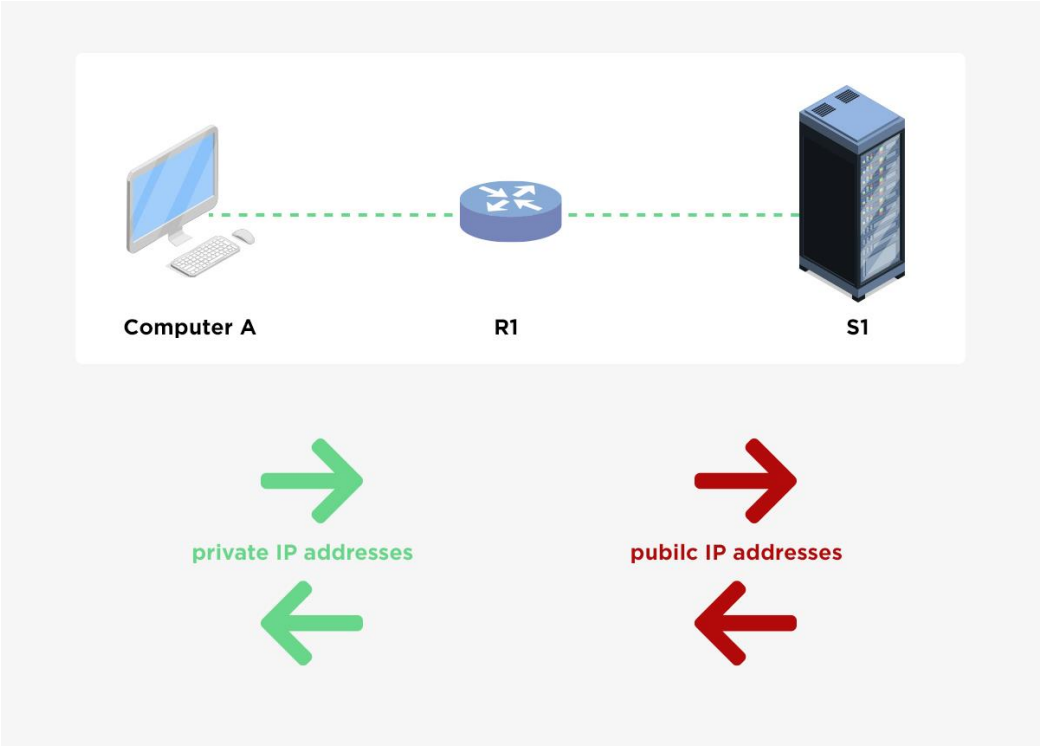


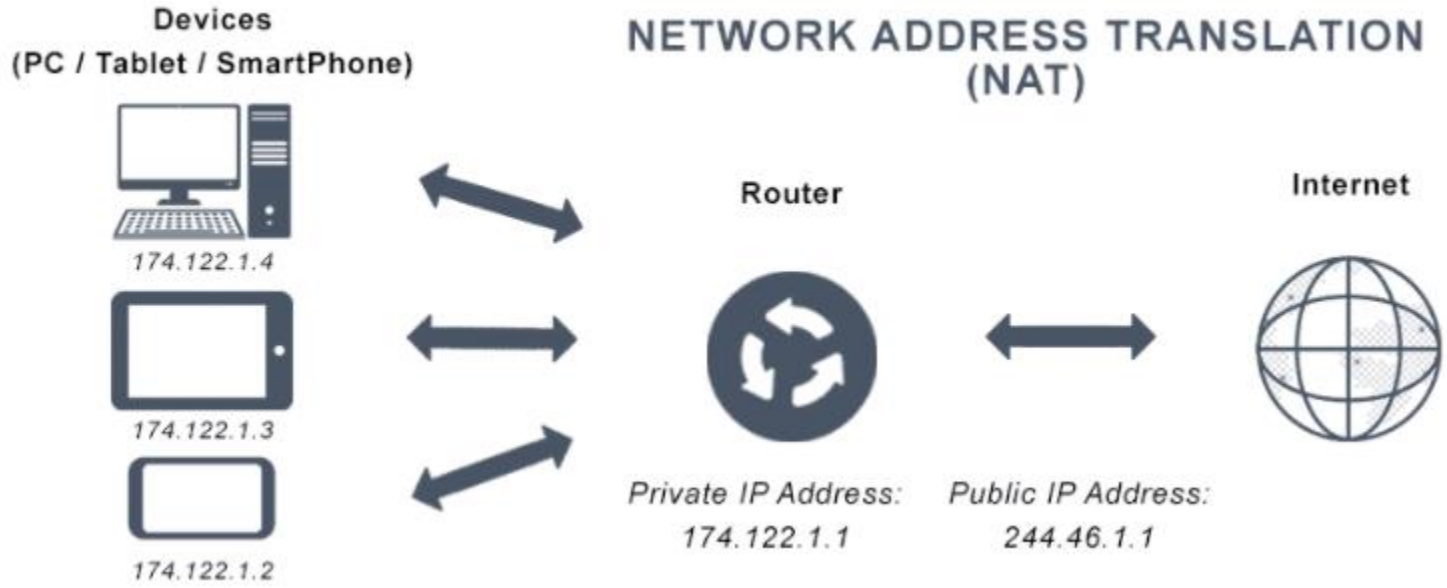
ARP-protokoll (Address Resolution Protocol)

- For å identifisere maskinene innenfor et nettverk må IP og MAC fungere for å vite hvor pakken sendes til
- Spør alle om den gitte IP-adressen
- En svarer og gir sin (6 byte)MAC –adresse
- Maskinen lagrer info til neste overføring
- Kan brukes for å finne dublikater



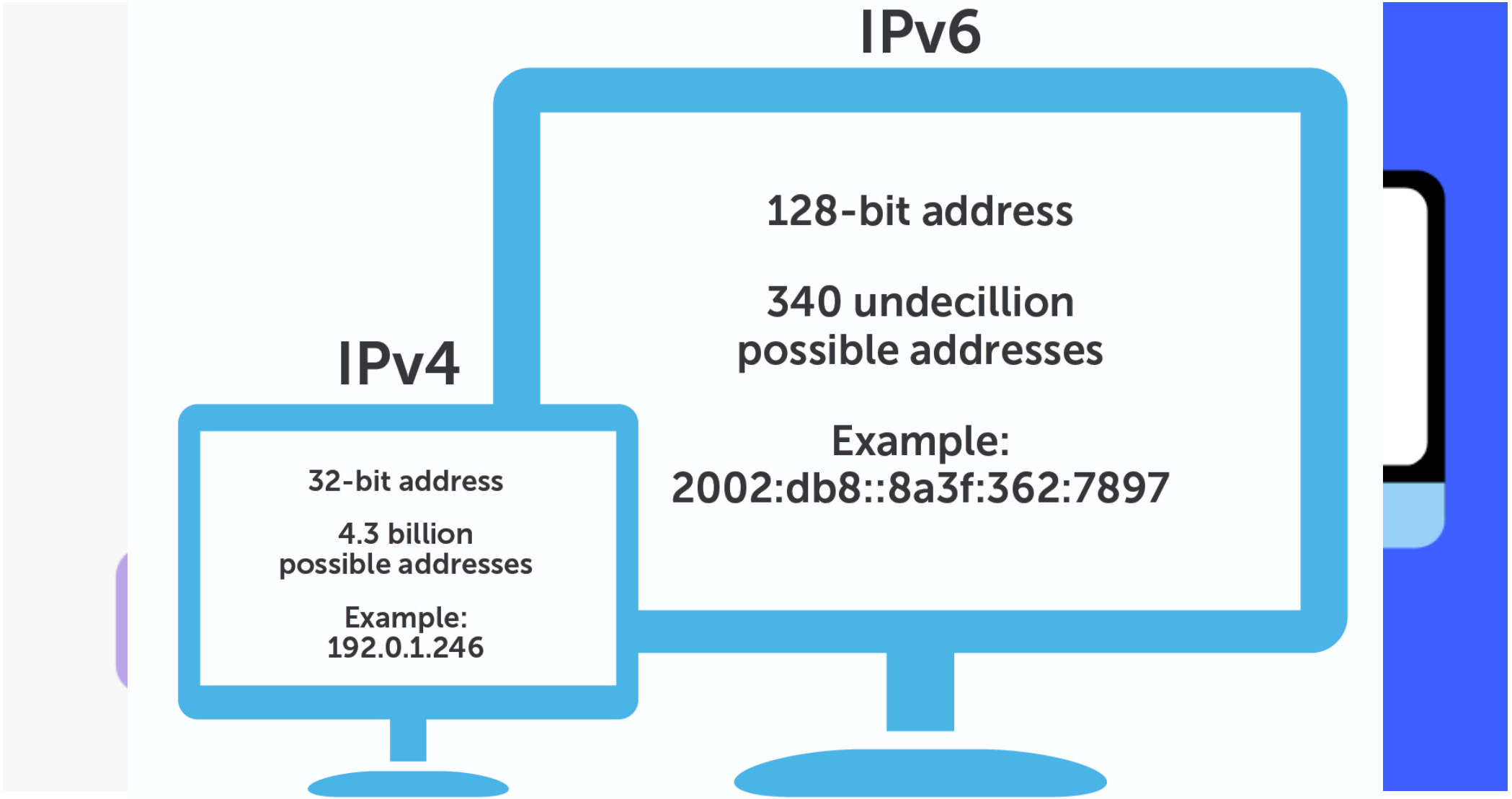
NAT - Network Address Translation





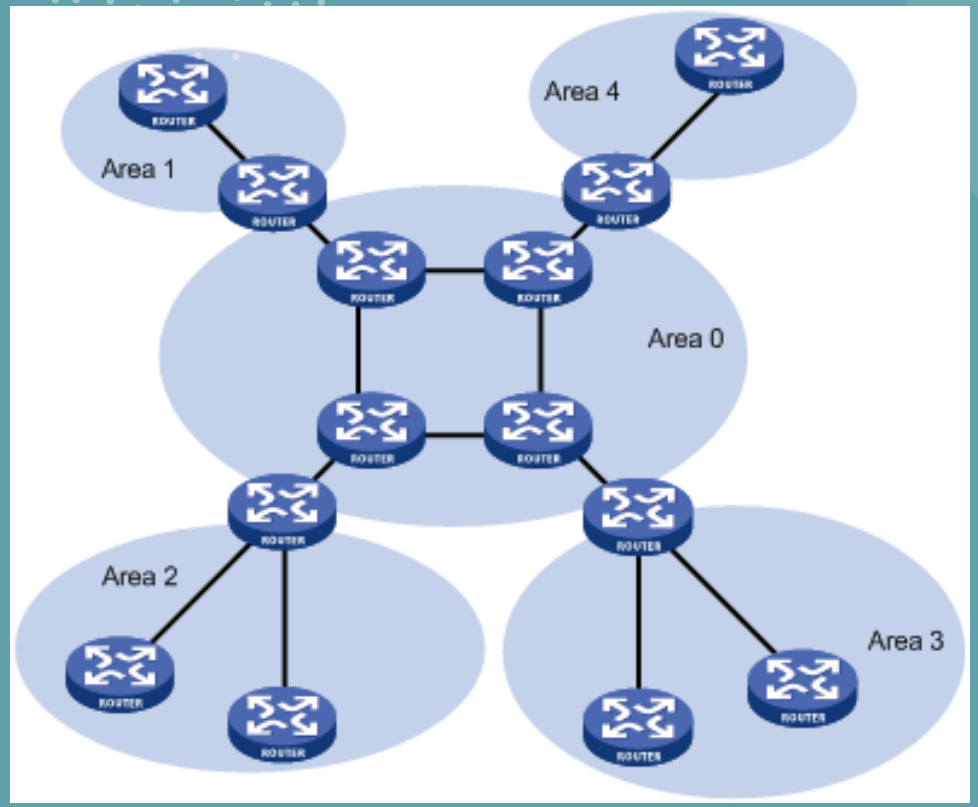
- Ekstra kompleksitet i nettet
- Routeren må bevare alle private IP-adressene og lage nye
- Vanskelig å koble utenifra til private IP-er

Fra IPv4 til IPv6



Router

- Målet er å videresende datapakke til adressen
- ISP – (Internet Service Provider) inngår avtaler og driver nettverket ved å videresende datatransport til andre ISPer og til sluttbrukeren
- BGP – (Border Gateway protocol) Rutingregler/protokoller som brukes mellom sending av datapakker



Transportlaget

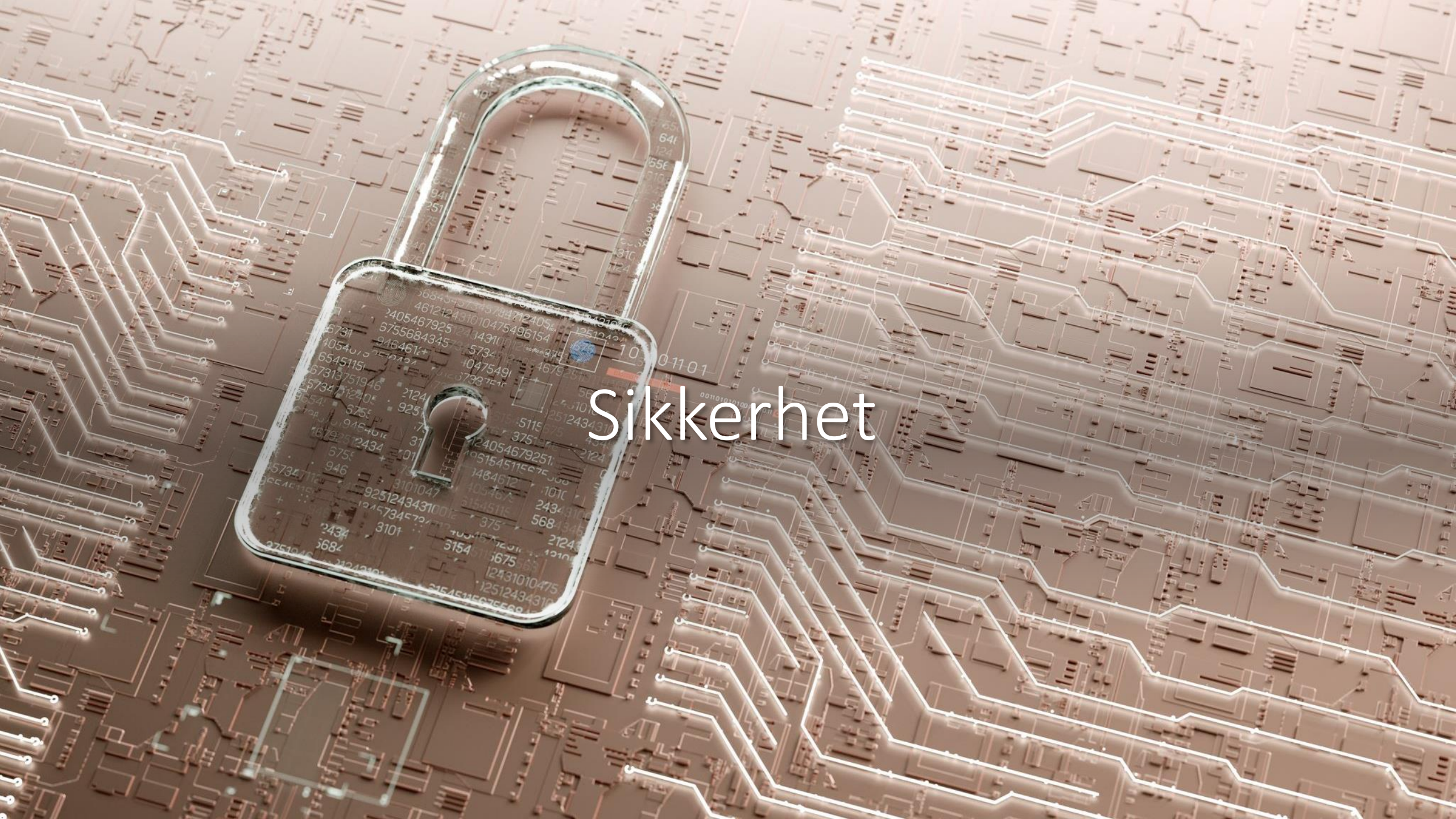
- En ruter er typisk FIFO kø. Hvis det oppstår mye trafikk over en gitt kø, vil det føre til stopp i trafikken. Dette kalles *congestion*. Blir det fullstopp kalles det *congestion collapse*
- Om dette skjer har vi en metningskontroll mekanisme som FIFO (fist-in-first-out) + begrenser mengde data per sekund.
- Metningskontroll sørger for at de deler kapasiteten likt på alle klientene *aktivt*
- Ressursene deles teoretisk likt mellom forbindelser
- Kan åpne flere forbindelser
- Per i dag finnes det ingen rettferdighet i internett

1000Mbps



10Mbps

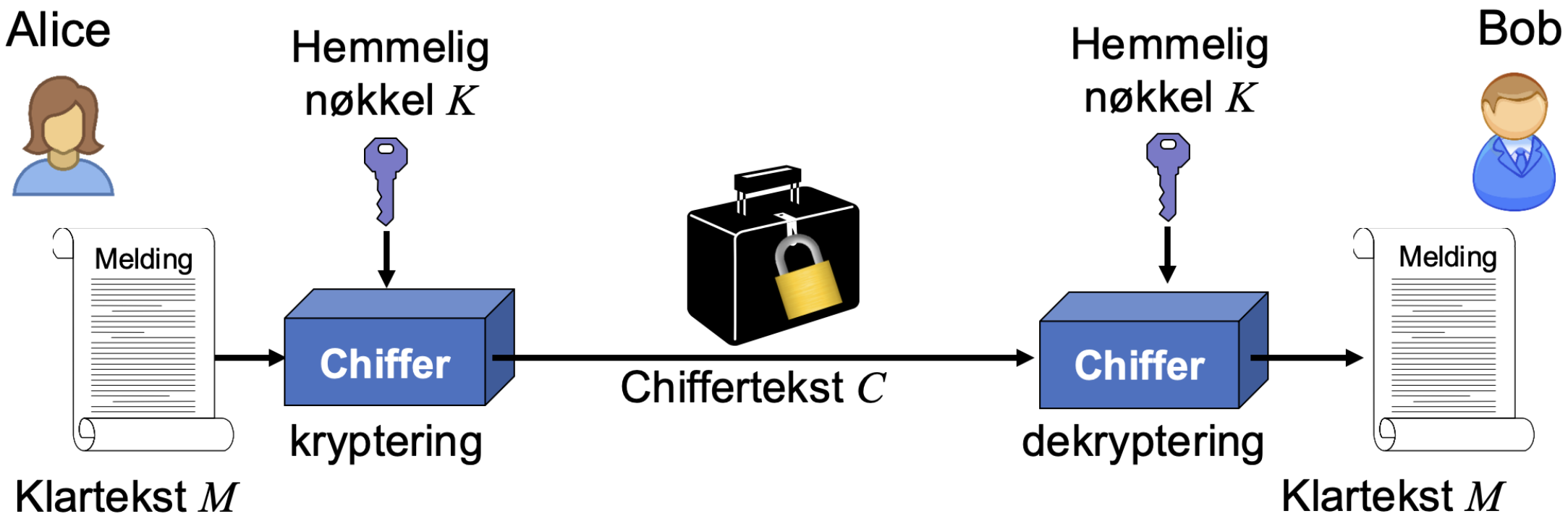
Verktøy	
ping	Måler forsinkelsen mellom din maskin og en annen på internett
traceroute	Gir informasjon om hvert hopp en datapakke er innom på vei til målet.
tracepath	Samme som traceroute, men trenger ikke superusertilgang
netstat	Gir informasjon om nettverksforbindelser på din maskin
dig	Gjøre DNS-oppslag 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


Sikkerhet

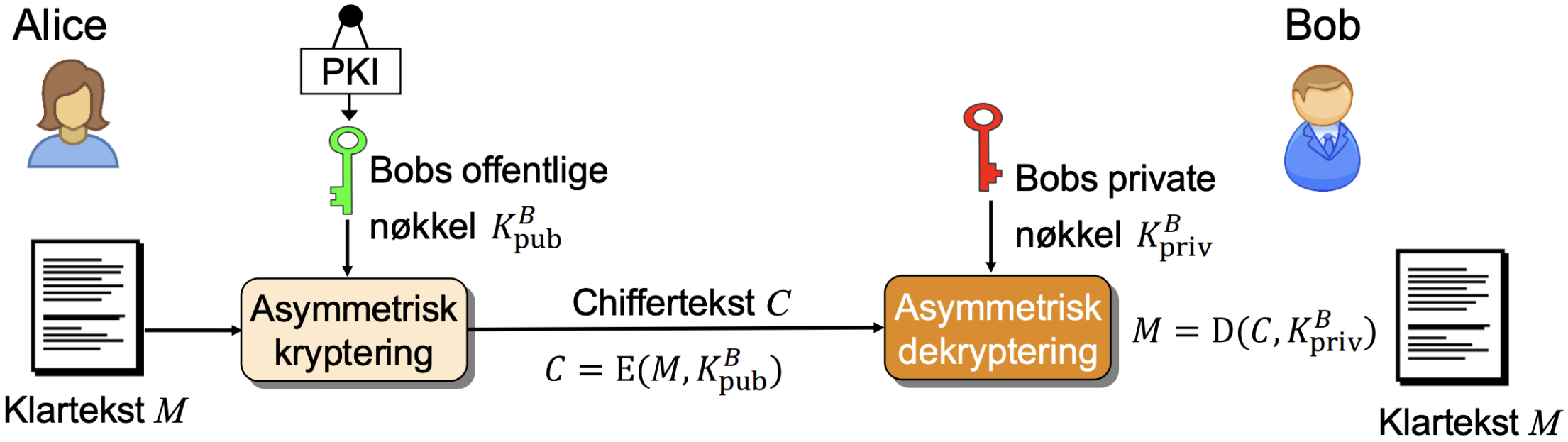


Hvorfor trenger vi kryptografi?

Symmetrisk kryptering

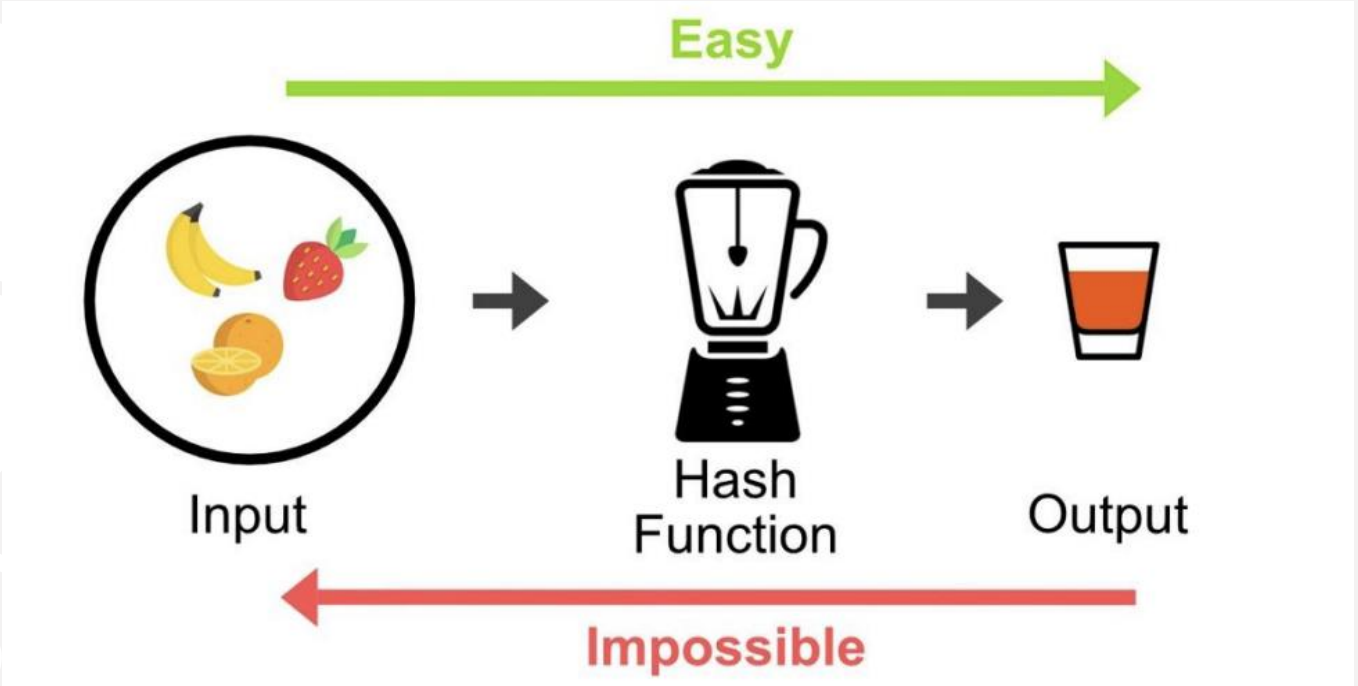


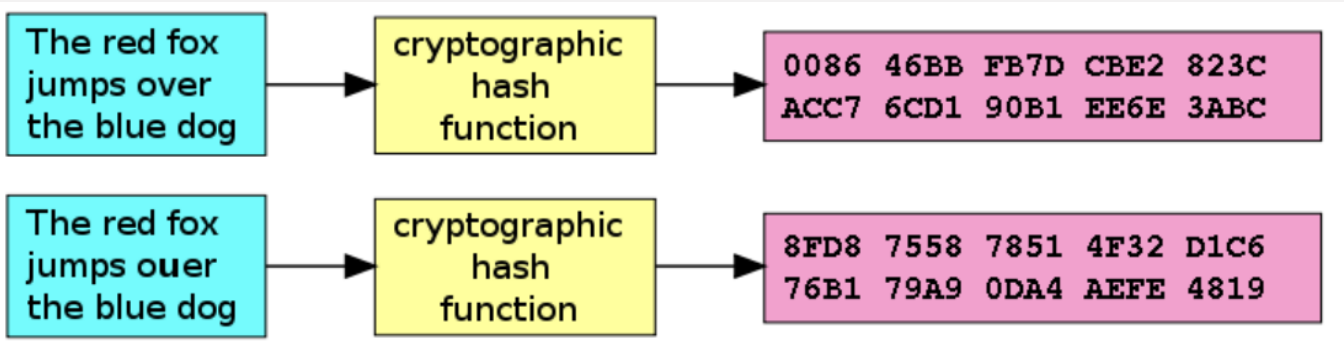
Asymmetrisk kryptering



Hash

- Beskyttelse av passord
- En liten endring, endrer hele sjekksummen
- Vanskelig å finne to ulike ord som skaper same sjekksum





Enkel eller ubenektelig meldingsautentisering

