

Institutt for Informatikk

IN1020

Uke 44

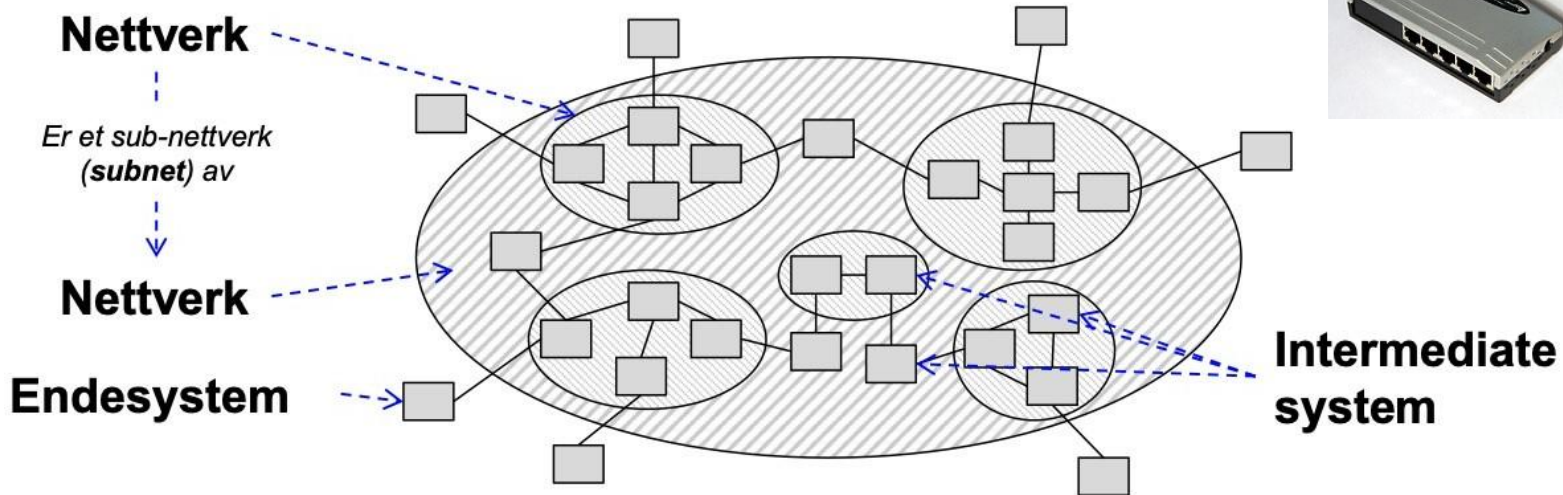
Datanettverk og kryptografi

01.11.22



UNIVERSITETET
I OSLO

Nettverkskomponenter



Aksesmodeller

I dette tilfelle
er datamaskin
= node

Aksesmodell: Måten man kommuniserer på

Klient-tjener modell

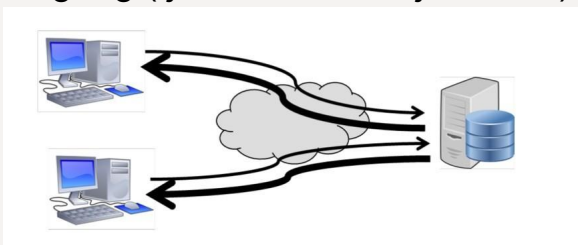
Klient ber om tjeneste → oppretter forbindelse

Tjenere leverer tjenesten

Eks: Innlogging i nettbank

Du logger inn på nettsiden med mobilen (klient ber om tjeneste)

Nettsiden sjekker innloggingsdetaljene, og du får tilgang (tjenere leverer tjenesten)



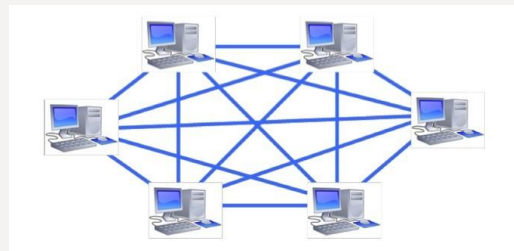
Peer-to-peer (P2P)

Alle noder likeverdige (node kan både være klient og tjener)

Alle noder kan nå hverandre

Eierskapet er distribuert

Eks: Windows-oppdateringer, Napster



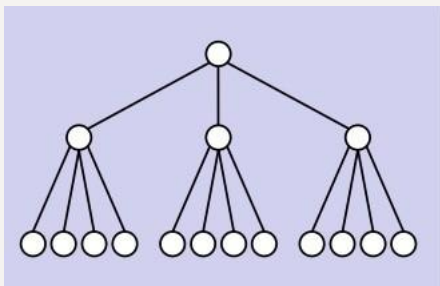
Nettverkstopologier: Punkt til punkt og broadcast nettverk

Nettverkstopologi: hvordan nettverket organisereres

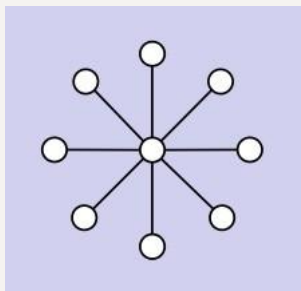
Punkt til punkt

- **Kablet** nettverk

- Stjernetopologi – der switchen er sentrum
- Kan utvides til tretopologi



Tre

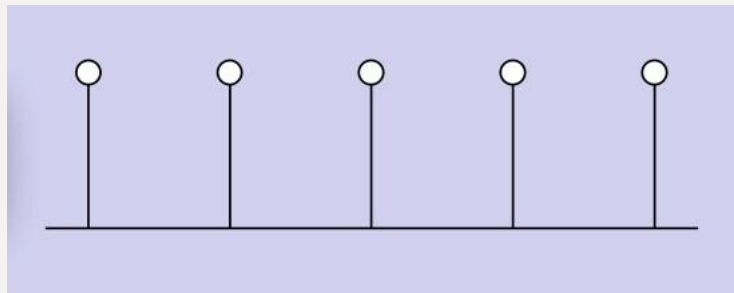


Stjern

Broadcast nettverk

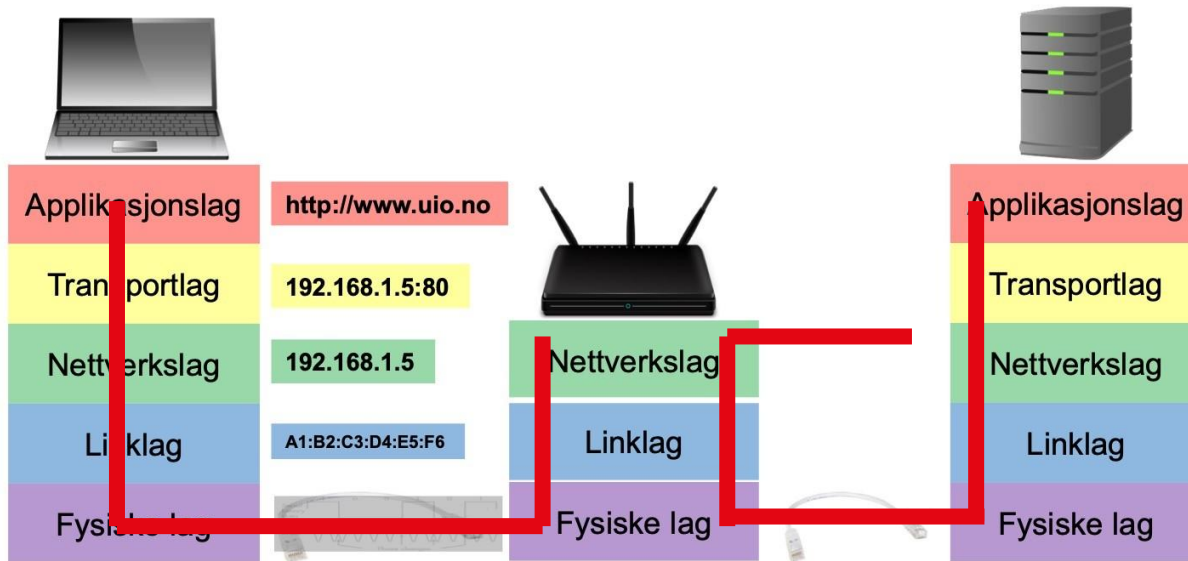
- **Radio**

- Wifi, 4G/5G
- Problem kan være at signalene går i veien for hverandre – støy i nettverket



TCP/IP-modellen

Lag		Funksjon
5	Applikasjon	Applikasjonsrelaterte tjenester
4	Transport	Kobler sammen systemene ende-til-ende (TCP/UDP)
3	Nettverk	Rute data fra ende-til-ende systemer (IP)
2	Link	Pålitelig overføring mellom to noder
1	Fysisk	Sender bit ut på mediet (kablet eller trådløst)



Komponenter i nettverk

- Tjener (server)

- Kjører programvaren (tjenesten) - applikasjonslaget

- Klient

- Kjører lokalt hos brukeren

Endesystem

- Switch

- Veldig primitiv (jobber på linklaget)

Intermediate system

- Router

- Mer avansert switch, trådløs i tillegg (jobber på nettverkslaget)

	Lag	Funksjon
5	Applikasjon	Applikasjonsrelaterte tjenester
4	Transport	Kobler sammen systemene ende-til-ende (TCP/UDP)
3	Nettverk	Rute data fra ende-til-ende systemer (IP)
2	Link	Pålitelig overføring mellom to noder
1	Fysisk	Sender bit ut på mediet (kablet eller trådløst)

TCP



TCP/IP EXPLAINED

Applikasjonslaget

DATA

<http://www.uio.no>



Transportlaget



192.168.1.5:80

TCP

- Forbindelsesorientert
 - 3 way handshake
- Flytkontroll
- Metningskontroll

UDP

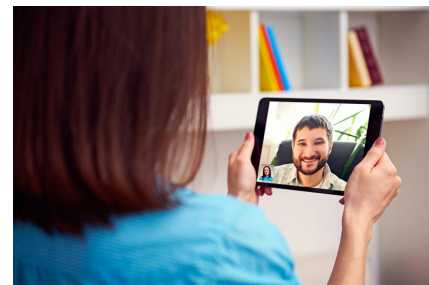
- Forbindelsesløst
- «Best effort»



NETFLIX



YouTube

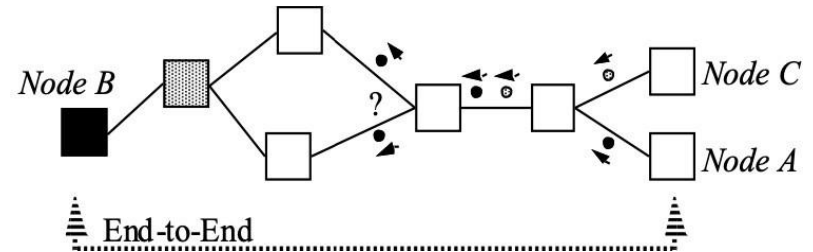


Nettverkslaget

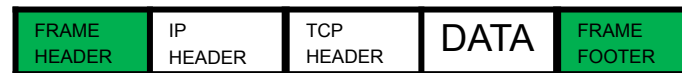


192.168.1.5

- IPv6 tar over for IPv4
 - 128 bit vs 32 bit adresser
 - Ruting av pakker over internett

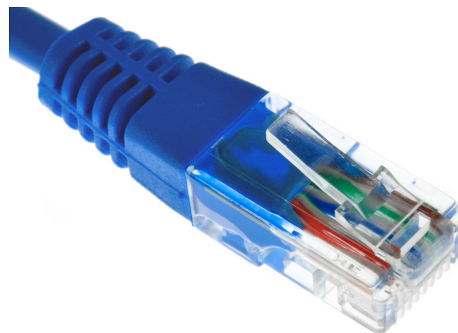


Linklaget



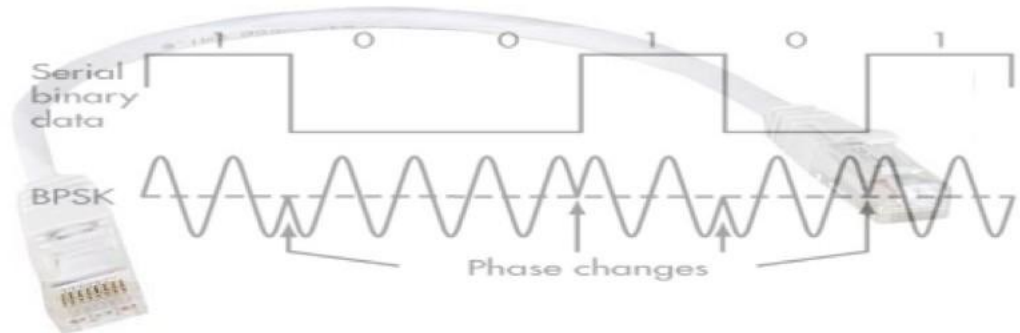
A1:B2:C3:D4:E5:F6

- Pålitelig overføring mellom to enheter.
 - Pakker som overføres i linklaget kalles «frames»
 - Feildeteksjon or retting innenfor en «frame»
-
- Ethernet og WiFi



Det fysiske laget

- Sørger for at bits blir overført korrekt



Regne ut nettverksmasken fra IP med CIDR notasjon

- Vi har gitt IP-adressen ved CIDR-notasjon: 192.168.0.30/24
- 192.168.0.165 \square binært = 11000000.10101000.00000000.00011110
- For å finne nettverksmasken ser vi at det er satt av 24 bit til nettverksdelen. Altså er det 8 bit igjen til vertsdelen. (32-24 = 8)
- Altså blir nettverksmasken: **11111111.11111111.11111111.00000000**
- Eller skrevet i 10-tallsystemet: 255.255.255.000

Regne ut subnettet fra en IP og nettverksmaske

- *En bitvis AND operasjon mellom IP-adressen og nettverksmasken*
- IP: 192.168.0.30
11000000.10101000.00000000.00011110
- Nettverksmaske: 11111111.11111111.11111111.00000000
- Resultat: **11000000.10101000.00000000.00000000**
- Subnettadresse i punknotasjon: 11000000.10101000.00000000.00000000
- Subnettadresse i CIDR-notasjon:
11000000.10101000.00000000.00000000/24
192.168.0.0/24

Hvor mange IP-adresser er det i vertsdelen av dette subnettet (fra forrige oppgave)?

- Som vi så tidligere er det 8 bit satt av til **vertdelen**. Altså skulle en tro at det blir $2^8=256$ adresser. Imidlertid er det **alltid**:
- En adresse til routeren
- En adresse til broadcast
- $256-2 = \underline{254}$
- Det er 254 adresser i vertsdelen av subnettet

Regne ut kringkastingsadressen til et subnett

- *En bitvis OR operasjon mellom maskinens **IP-adresse** og nettverksmasken **invers***
- IP: 192.168.0.30
11000000.10101000.00000000.00011110
- Nettverksmaske invers: 00000000.00000000.00000000.11111111
- Resultat: **11000000.10101000.00000000.11111111**
- Kringkastingsadresse til subnettet i punktnotasjon: 11000000.10101000.00000000.11111111
- Kringkastingsadresse til subnettet i CIDR-notasjon:
11000000.10101000.00000000.11111111/24 192.168.0.255/24

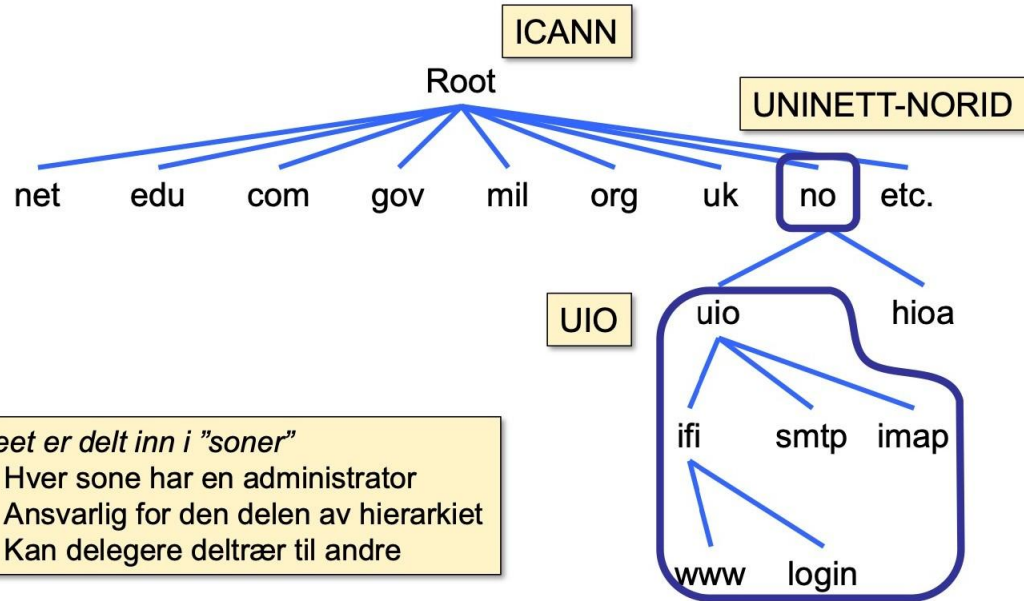
Private IP-adresser

RFC1918 name	IP address range	number of addresses	largest CIDR block (subnet mask)	host id size	mask bits
24-bit block	10.0.0.0 – 10.255.255.255	16,777,216	10.0.0.0/8 (255.0.0.0)	24 bits	8 bits
20-bit block	172.16.0.0 – 172.31.255.255	1,048,576	172.16.0.0/12 (255.240.0.0)	20 bits	12 bits
16-bit block	192.168.0.0 – 192.168.255.255	65,536	192.168.0.0/16 (255.255.0.0)	16 bits	16 bits

Disse IP-adressene skal ikke være direkte koblet mot internett

DNS

Domain Name
System



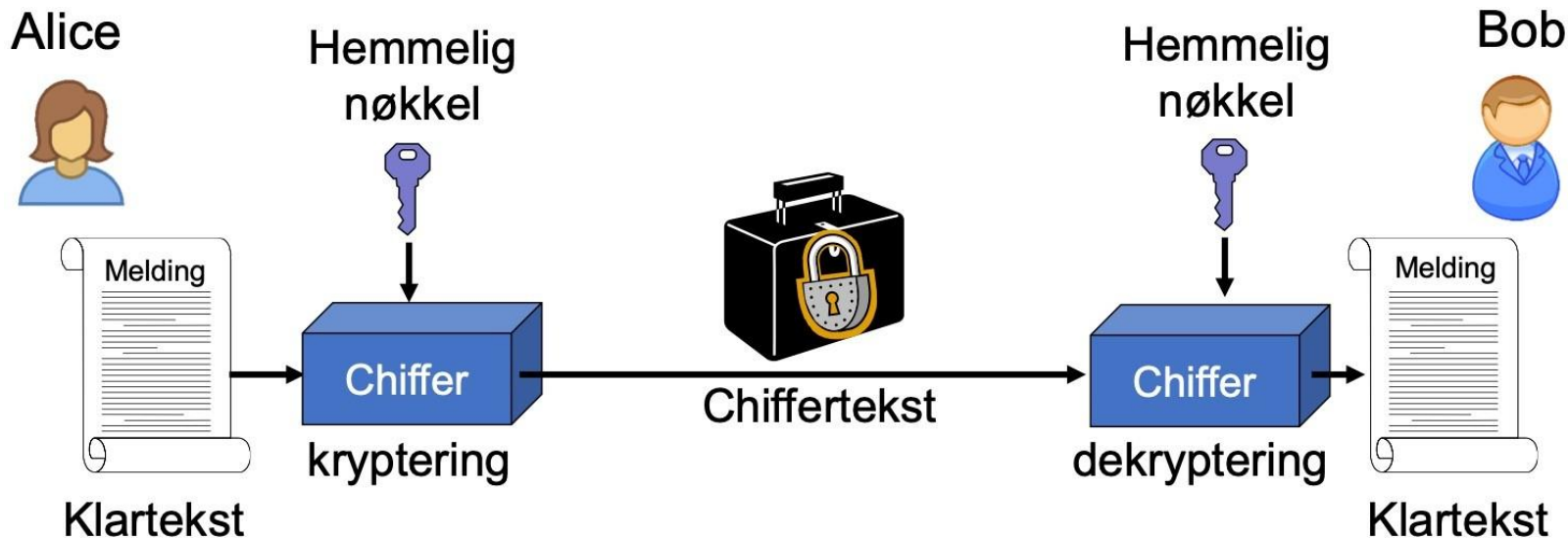
Kryptering

Kryptografi = vitenskapen om hemmelig skrift

- Krypteringsalgoritmer
 - Symmetrisk : Hemmelig nøkkelkryptering – En nøkkel: Men må deles mellom sender og mottaker
 - Asymmetrisk: – Offentlig nøkkelkryptering – To nøkler: a) Privat b) Offentlig
- Hash-funksjoner : Enveis identifikasjon – Ingen nøkkel
- Kryptering er ikke noe nytt – Cæsar-chifferet er et av de første formene for kryptering
- 2. verdenskrig: Enigma
- Sikkerhetsmål:
 - Konfidensialitet
 - Integritet
 - Autentisitet
 - Uavviselighet



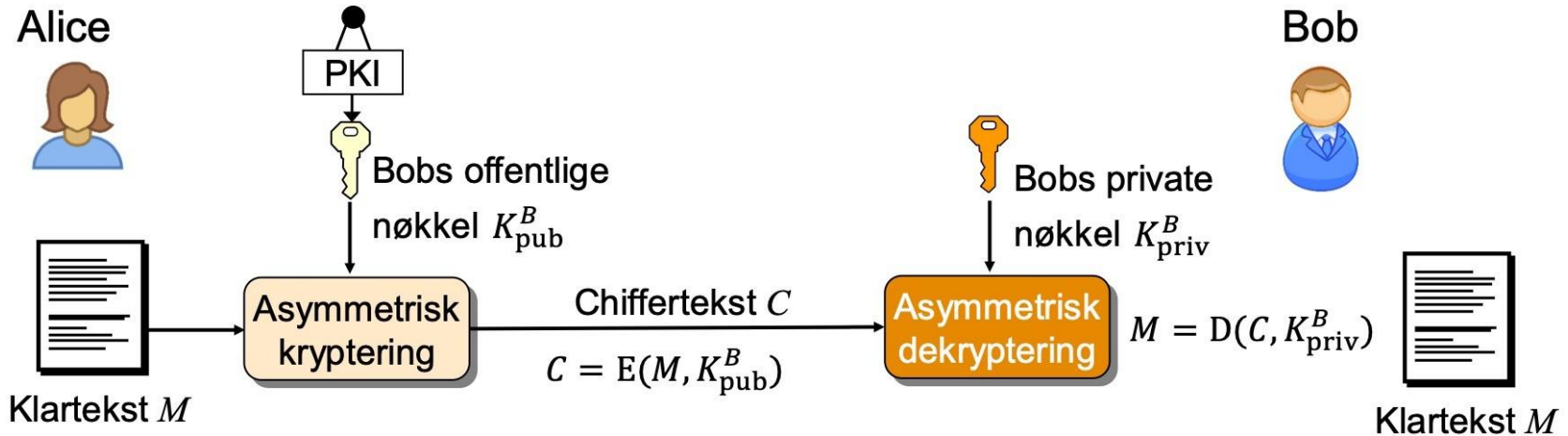
Symmetrisk kryptering



Gir autentisitet, men ikke uavviselighet

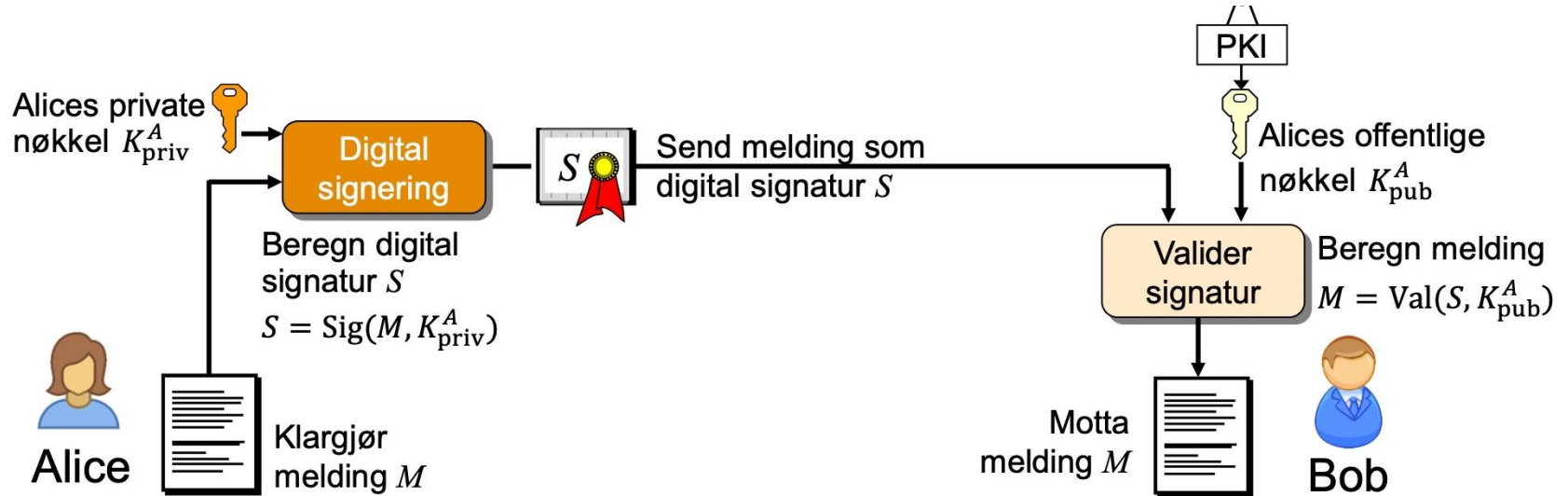
*Illustrasjon hentet fra IN2120
Informasjonssikkerhet*

Asymmetrisk kryptering



Digital signatur

Det motsatte av det vi så med vanlig asymmetrisk kryptering

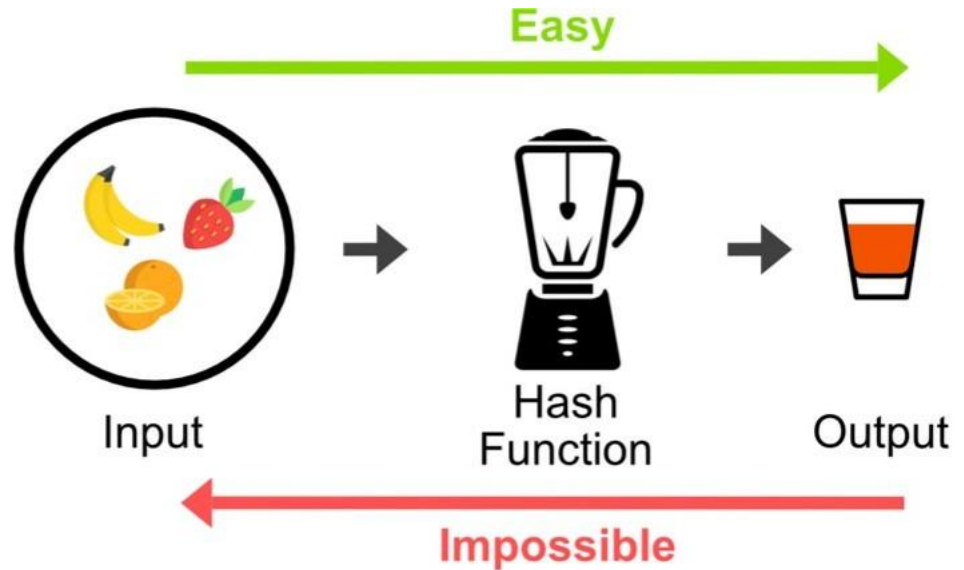


Gir uavviselighet
også

Illustrasjon hentet fra IN2120
Informasjonssikkerhet

Hashing

- En enveisfunksjon (ikke reverserbar)
- En «melding» gir alltid samme hashverdi (deterministisk)
- Brukes som sjekksumalgoritme – kan sjekke om en verdi er lik – de skal gi samme hashverdi
- Liten endring i «meldingen» endrer hashverdien omfattende



Meldingsautentisering

Kun ment som et eksempel for å vise hva hashing kan brukes til: (ikke pensum)

