Gruppetime 10 i IN1020

Datanettverk og kryptering

Cristina Tezec (cristite@ifi.uio.no)

My Hoang Duong(myhd@ifi.uio.no)

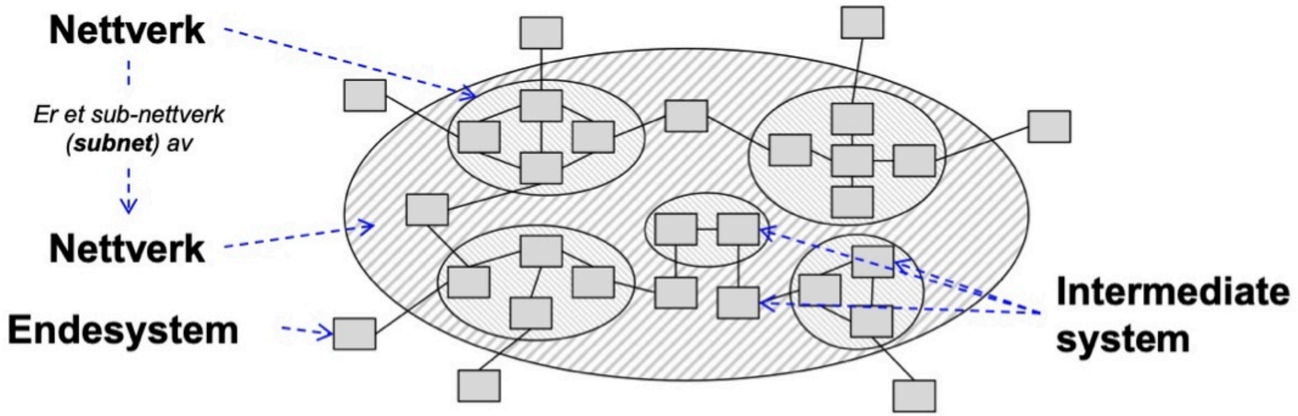
Plan for dagens gruppetime

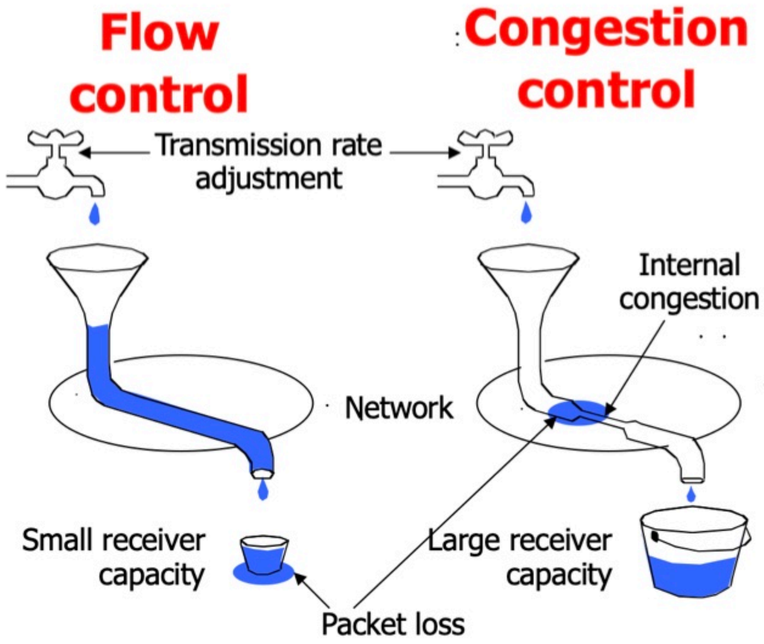
> TCP/IP modellen
> IP-adresserer og CIDR notasjon
> Hjelp med oblig 3

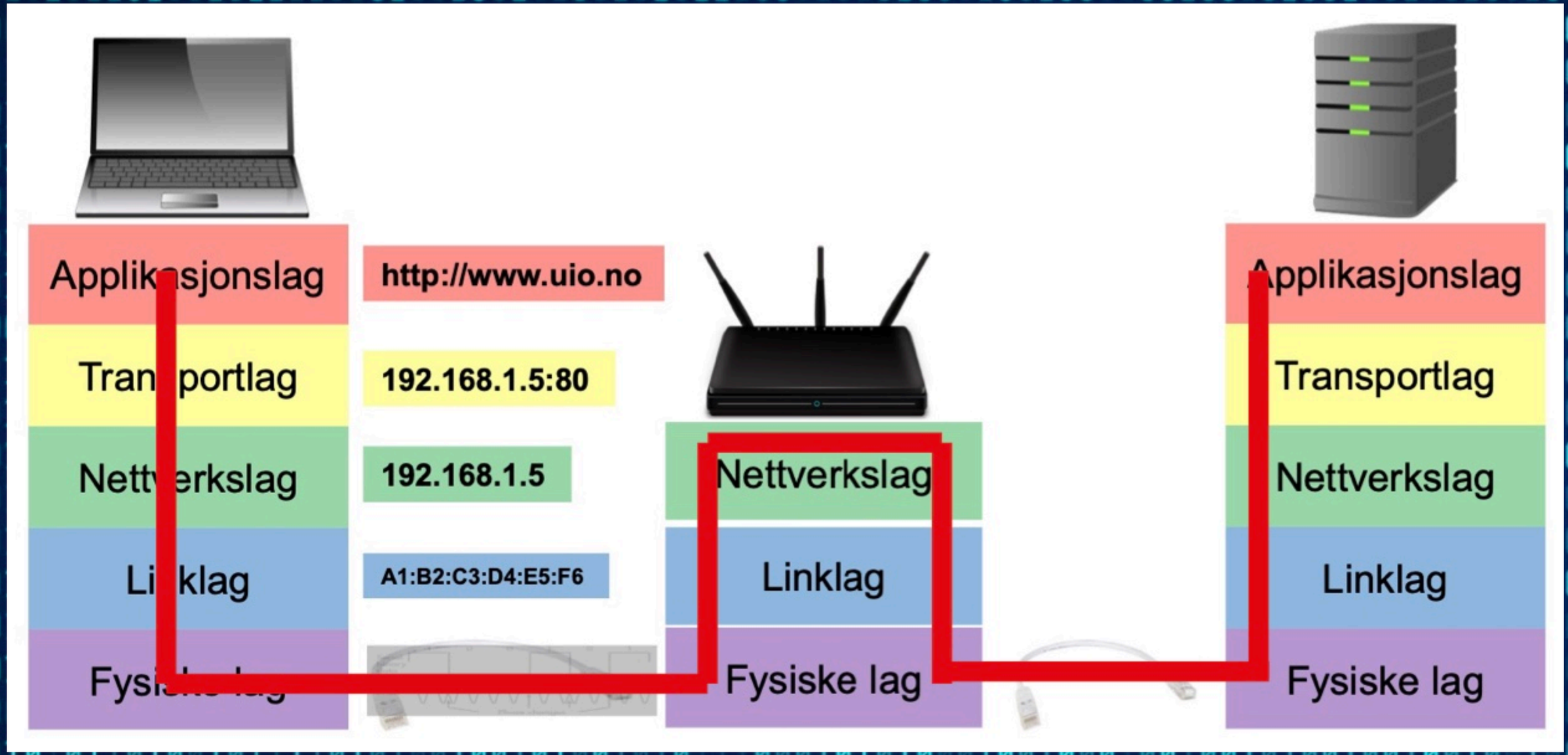
TCP/IP modellen

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)

Lagdeling brukes for retningskontroll og flyttkontroll






Applikasjonslag
Transportlag
Nettverkslag
Linklag
Fysiske lag
http://www.uio.no
192.168.1.5:80
192.168.1.5
A1:B2:C3:D4:E5:F6
Nettverkslag
Linklag
Fysiske lag
Applikasjonslag
Transportlag
Nettverkslag
Linklag
Fysiske lag

IP adresser

Det finnes IP adresser som består av 32 bits (IPv4) og 128 bits (IPv6). For eks. Er min IP adresse 192.168.0.110. I binært tallsystem skal IP adresse min se sånn ut: 11000000.10101000.00000000.01101110
Hver del av 8 bit kan ha verdier mellom 0 og opp til 255 (2^8 = 256).

Hva om jeg er en stor organisasjon?

Da deler vi nettverket inn i mindre subnett, slik at hele de første 28 bit (for eks) er felles, mens de siste 4 bit blir delt innen organisasjonen.

Felles IP: 192.2.9.x >>>>

1. enhet: 192.2.9.11, 2. enhet: 192.2.9.12, 3. enhet: 192.2.9..13

Nettverksmaske brukes for å finne hva den første adressen på subnettet er:

- 0 = vertsdel
- 1 = nettverksdel

255.255.0.0

11111111.11111111.00000000.00000000

- Punktnotasjon må ha med hele denne nettverksmasken
- CIDR-notasjon angir bare hvor mange hvor mange bits som er nettverksdelen

- Nettverksmaske brukes til å dele en IP-adresse i subnettverk. Spesifiserer hva som er tilgjengelig for verter

Nettverksmaske brukes for å finne hva den første adressen på subnettet er:

- *En bitvis AND operasjon mellom IP-adressen og nettverksmasken*
- Nettverksmaske: 11111111.11111111.11111111.00000000

IP	11000000	10101000	00000000	00011110
Nettverksmaske	11111111	11111111	11111111	00000000

AND

- Resultat: **11000000.10101000.00000000.00000000**
- Subnettadresse i punknotasjon (binært): 11000000.10101000.00000000.00000000
- Subnettadresse i punknotasjon (10-tallsystemet): 192.168.0.0
- Subnettadresse i CIDR-notasjon: 192.168.0.0/24

Hva om vi har flere enn 256 enheter å koble til nettverket?

Da bruker vi Broadcasting adress (Netflix for eks)

- *En bitvis OR operasjon mellom maskinens **IP-adresse** og nettverksmasken **invers***

IP	11000000	10101000	00000000	00011110
Nettverksmaske invers	00000000	00000000	00000000	11111111

- Resultat: **11000000.10101000.00000000.11111111**
- Kringkastingsadresse til subnettet i punktnotasjon (binært): 11000000.10101000.00000000.11111111
- Kringkastingsadresse til subnettet i punktnotasjon (10-tallsystemet): 192.168.0.256
- Kringkastingsadresse til subnettet i CIDR-notasjon: 192.168.0.256/24

- Du ønsker å laste ned en fil på 200 megabyte, og den maksimale nedlastingshastigheten på din Internettforbindelse er 20 megabit per sekund. Hva er den teoretisk korteste overføringstiden?

- 20 sekunder
- 80 sekunder
- 10 sekunder
- 5 sekunder
- 100 sekunder

$$v = \frac{s}{t} \longrightarrow t = \frac{s}{v}$$

$s = størrelse\ på\ filen$

$v = nedlastningshastighet$

$$t = \frac{200MB}{20Mbit/s} \longrightarrow t = \frac{200MB * 8bit/B}{20Mbit/s} \longrightarrow \underline{t = 80\ s}$$

DHCP

Dynamic Host Configuration Protocol

- Som oppgave å tildele IP-adresser til nye enheter
- Automatisk utdeling av IP-adresser
- Består av:
  - DHCP discover – ser etter en DHCP-tjener (broadcaster beskjeden)
  - DHCP offer – tilbyr en adresse
  - DHCP request – ber om å få bruke den gitte adressen
  - DHCP ack – gir IP-adressen enheten
- Som regel ruteren som står for utdeling av IP-adresser

ARP

Address Resolution Protocol

- Kobler internett og linklaget sammen
- Avsenderen må vite hvilken IP-adresse pakken skal sendes til
- En tabell, ARP cache, holder oversikt over korrelasjon mellom IP-adresser og MAC-adresser
- På mange måter likt hvordan DHCP fungerer, men på linklaget

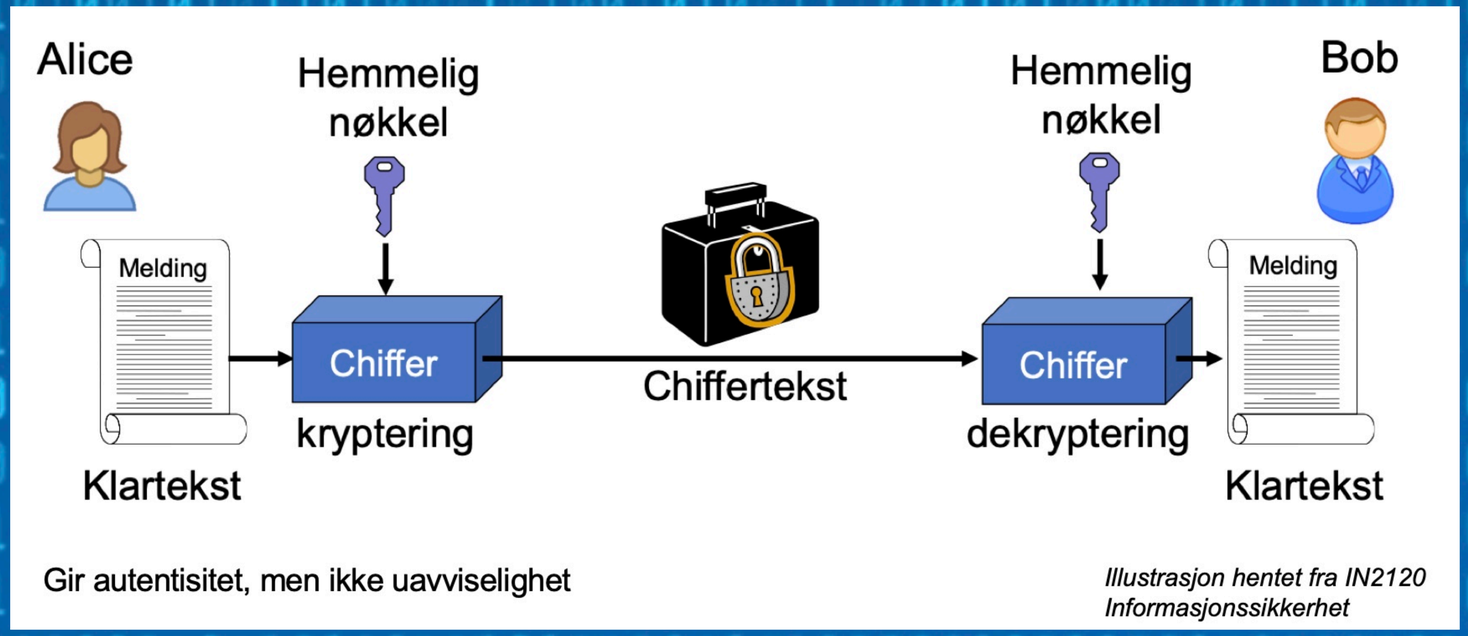
Porter

Port	Tjeneste
0	Reservert
1	tcpmux
…	
22	SSH
…	
80	HTTP
…	
1024-49151	Brukerporter
49152-65535	Dynamisk / privat

En IP-adresse kan ha ulike porter

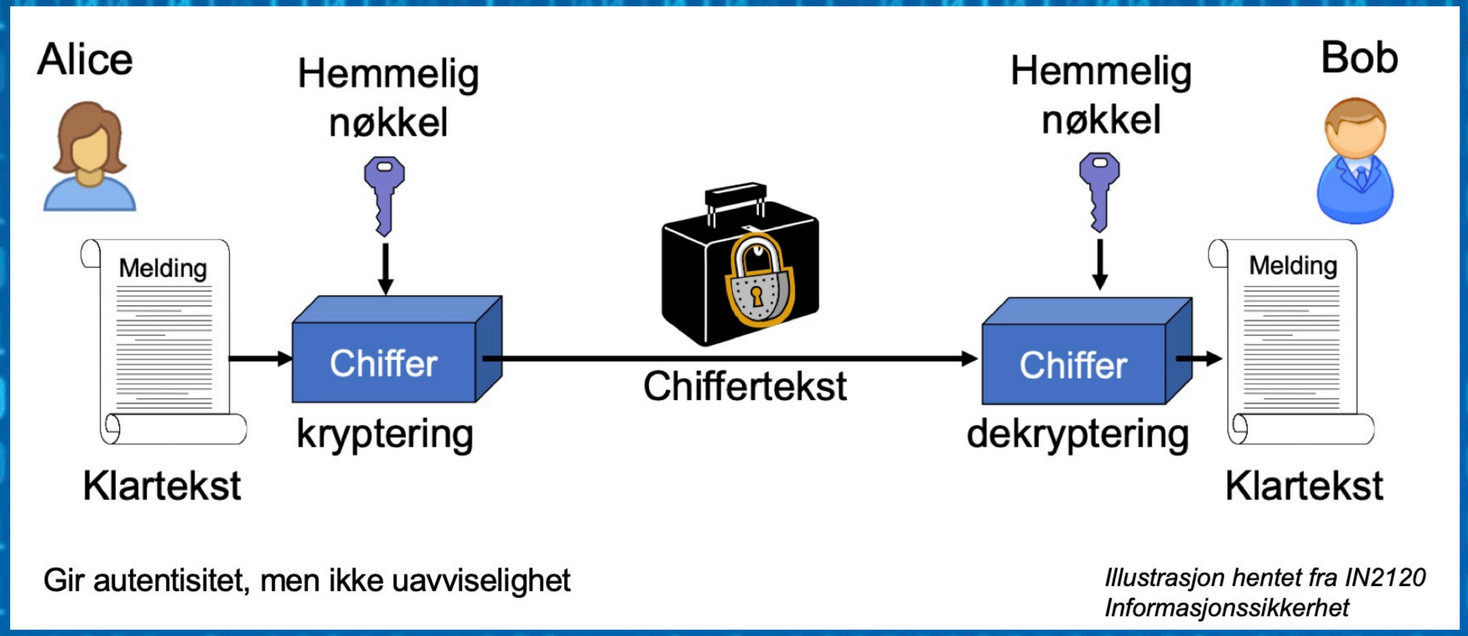
http://www.something.com:22/MyService

http://www.something.com:80/MyService



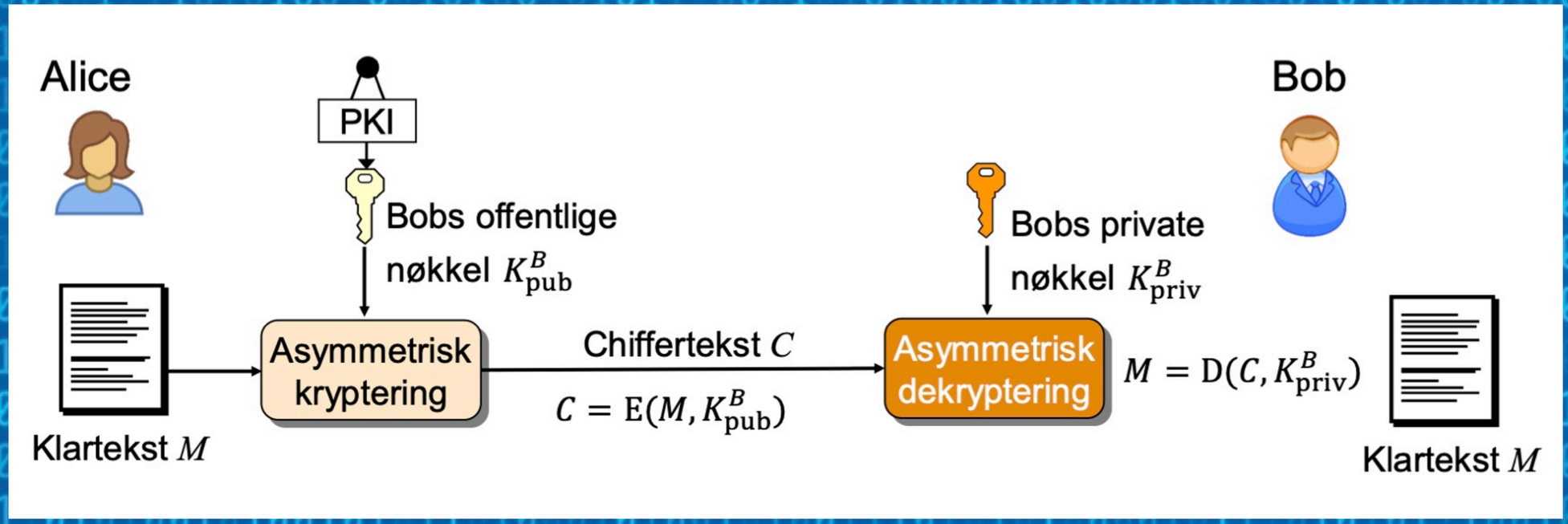
Gir autentisitet, men ikke uavviselighet

Illustrasjon hentet fra IN2120 Informasjonssikkerhet



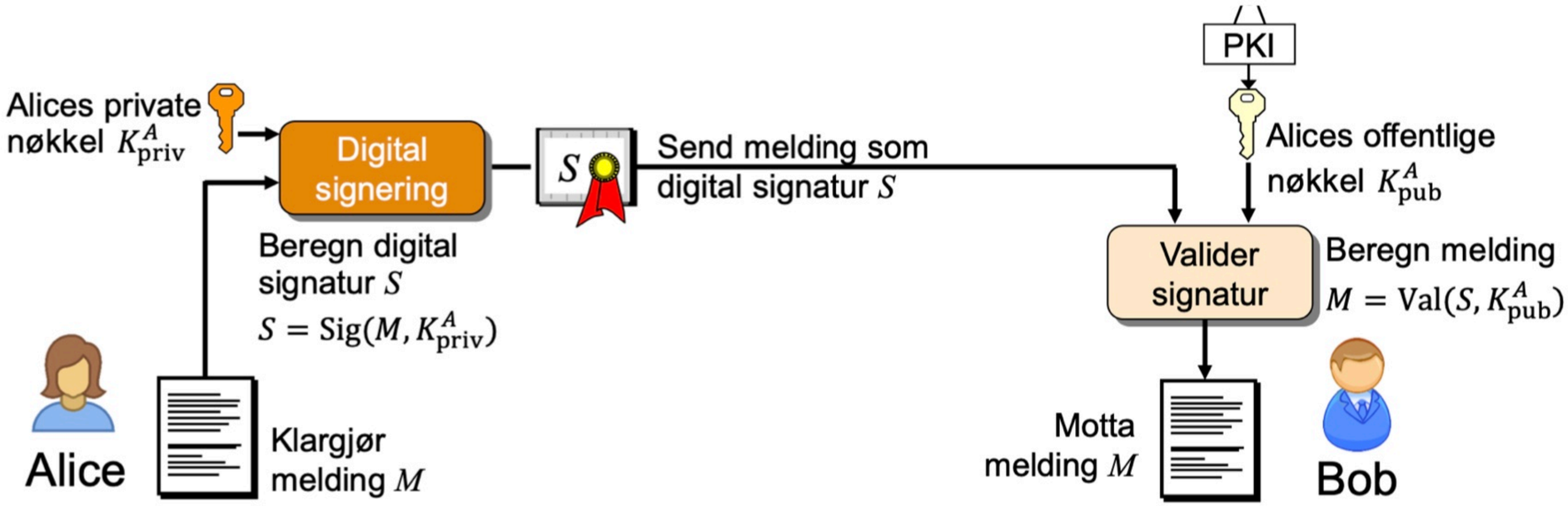
Gir autentisitet, men ikke uavviselighet

Illustrasjon hentet fra IN2120 Informasjonssikkerhet



Digital signatur

Det motsatte av det vi så med vanlig asymmetrisk kryptering



Gir uavviselighet også

Illustrasjon hentet fra IN2120 Informasjonssikkerhet

Sjekksumalgoritme (hash-funksjon)

1. a) Programmet sha256sum genererer en sjekksum av en fil basert på algoritmen SHA256. Lag en liten tekstfil med innhold, kall den f.eks. abc.txt. Kjør så programmet sha256sum: [kritisk@vestur]>sha256sum abc.txt
   [6ee0c32c675ce6d3bd3f6e326c81e45b3d6675c29c0c9ced1398684a667804e9
   abc.txt
2. Gjør endringer i fila abc.txt, og kjør programmet en gang til. Er nøkkelen den samme?
3. b) Hvordan kan sjekksumalgoritmer bidra til å sikre dataintegritet?
4. c) Finn og diskuter situasjoner/eksempler hvor bruk av sjekksumalgoritme kan være nyttig for deg.