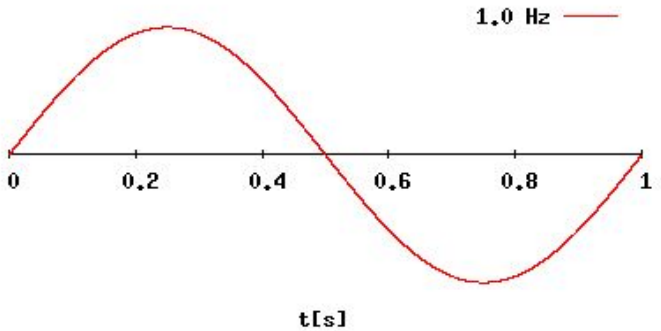
# Frekvens, synkronisering og masse bra repetisjon



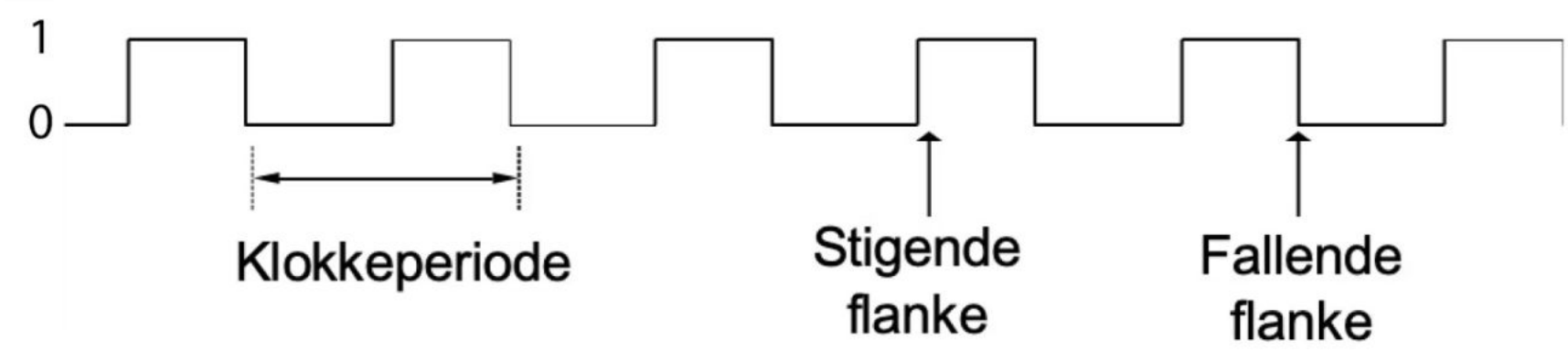

Aki, Birk og Sophie

# Mer om klokke



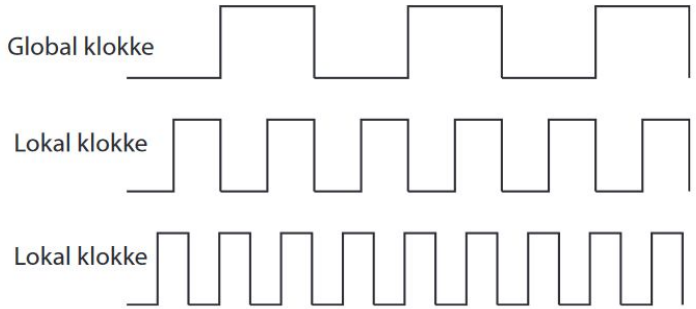
- Klokken veksler mellom 1 og 0.
- Når klokken tikker 1 utfører maskinen operasjoner.
- 0 er en pause mellom operasjoner

Hvorfor trenger vi pauser? Hvorfor ikke bare utføre operasjoner så fort som mulig?



# Klokke synkronisering og frekvens

- Maskiner opererer gjerne med flere klokker som må synkroniseres for å jobbe sammen.
- Klokkehastighet kalles også frekvens.




“ALU og CPU er en og samme enhet, men har ulik klokkehastighet” (Fra eksamen 2018)
Sant? Usant?

$$frekvens = \frac{1}{klokkeperioden}$$

# Oppgaver om Klokke fra ukeoppgavene

1) Diskuter fordeler og ulemper med å ha et klokkesignal som har en klokkeperiode som er 50% høy og 50% lav.

2) Diskuter fordeler og ulemper med å ha et klokkesignal som har en klokkeperiode som er 70% høy og 30% lav.

3) NØTT! Hva er frekvensen for en port (5ps delay) når klokkeperioden er som i oppgave 2.

# Fasit: Oppgaver om Klokke fra ukeoppgavene

1. Et klokkesignal som har en klokkeperiode som er 50% høy og 50% lav:
   - Er stabilt og lett å implementere
   - Men! Det sløser med tid å bruke like mye tid på pausene som operasjonene.

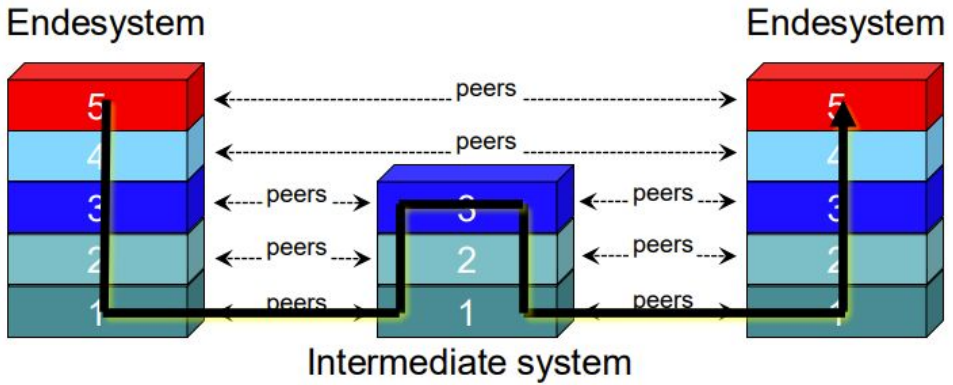
2. Et klokkesignal som har en klokkeperiode som er 70% høy og 30% lav er
   - Oppleves raskere, siden mer tid settes av til operasjoner enn pauser
   - Kan utføre mer komplekse operasjoner
   - Men! Er vanskeligere å lage og kan være ustabilt.

3. Frekvensen for en port (5ps delay) med klokkeperioden er 70% høy og 30% lav er:
   5ps / 70% ≈ 7.2ps , som fasit velger å runde opp til 8ps
   Dette gir en frekvens på: ⅛ = 0.125 = 125GHz


På tide med litt repetisjon!!!

# Nettverkslagene

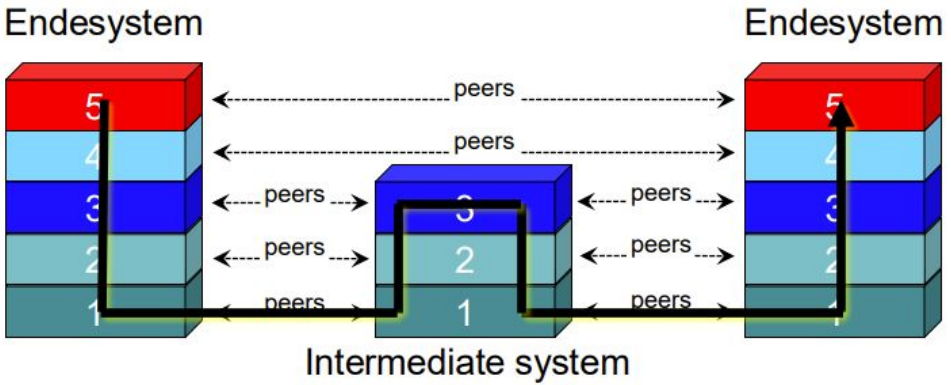
| Lag | | Funksjon |
|---|---|---|
| 5 | [redacted] | [redacted]relaterte tjenester (**HTTP**, **Mail**) |
| 4 | [redacted] | Kobler sammen systemene ende-til-ende ([redacted]) |
| 3 | [redacted] | Sende data fra ende-til-ende systemer[redacted] |
| 2 | [redacted] | Pålitelig overføring mellom to noder (**LAN/WiFi**) |
| 1 | [redacted] | Sender bit ut på mediet (kablet eller trådløst) |



# Nettverkslagene

- Separate lag med egne protokoller og oppgaver
- Applikasjonslaget
  - Selve dataen man vil sende
- Transportlaget
  - [redacted](diskuter i 1 min)
  - Flytkontroll
    - [redacted]
  - Metningskontroll
    - [redacted]
- Nettverkslaget
  - [redacted]-adresser
- Link-laget
  - [redacted]-adresser
- Fysiske laget
  - Overføring av bits

| Lag | | Funksjon |
|---|---|---|
| 5 | **Applikasjon** | Applikasjonsrelaterte tjenester (**HTTP**, **Mail**) |
| 4 | **Transport** | Kobler sammen systemene ende-til-ende ([redacted]) |
| 3 | **Nettverk** | Sende data fra ende-til-ende systemer [redacted] |
| 2 | **Link** | Pålitelig overføring mellom to noder (**LAN/WiFi**) |
| 1 | **Fysisk** | Sender bit ut på mediet (kablet eller trådløst) |

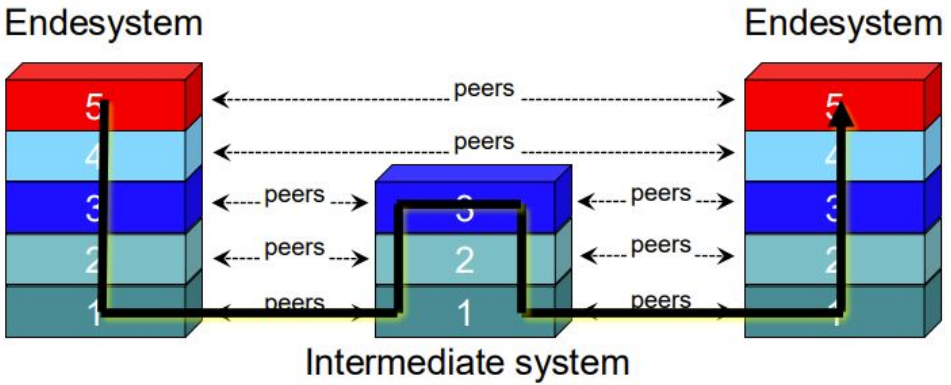


# Nettverkslagene

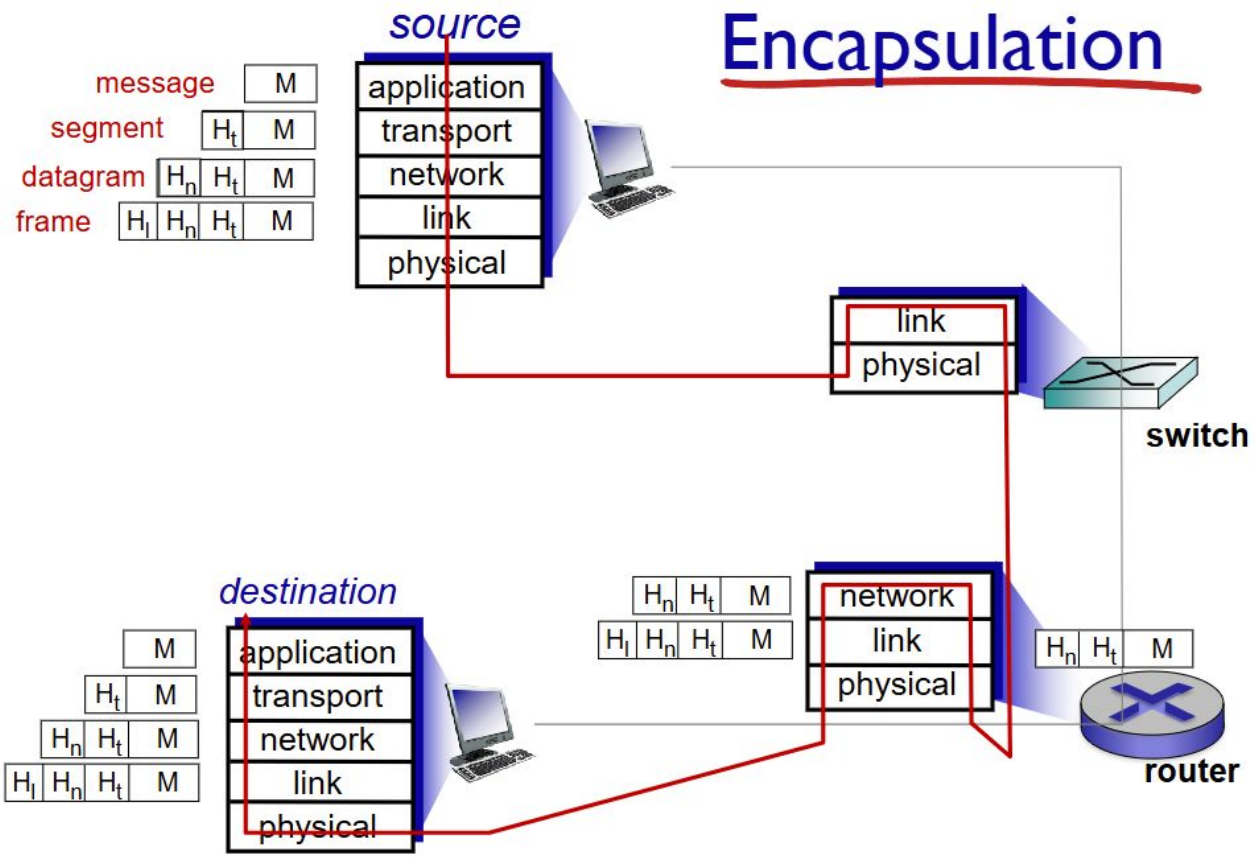
- Separate lag med egne protokoller og oppgaver

- Applikasjonslaget
  - Selve dataen man vil sende
- Transportlaget
  - TCP og UDP (diskuter i 1 min)
  - Flytkontroll
    - Sjekker hvor fort mottaker kan motta
  - Metningskontroll
    - Passer på at nettverket ikke blir overbelastet
- Nettverkslaget
  - IP-adresser
- Link-laget
  - MAC-adresser
- Fysiske laget
  - Overføring av bits

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



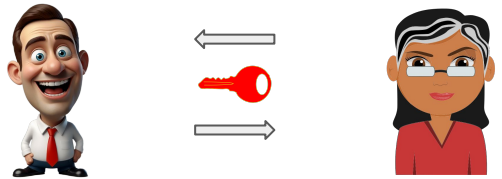
# Encapsulation



# Kryptering

[redacted] kryptering

- Én felles hemmelig nøkkel
- Samme nøkkel til kryptering og dekryptering
- Men hvordan skal de bli enige om denne nøkkelen uten at noen andre får tak i den?



Bob Alice

[redacted] kryptering

- Begge parter har to nøkler hver, en privat og en offentlig
  - [redacted] er for:
    - Kryptering
    - Verifisering av signatur
  - [redacted] er for:
    - Dekryptering
    - Signering

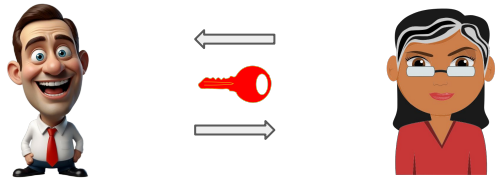


Bob Alice

# Kryptering

Symmetrisk kryptering

- Én felles hemmelig nøkkel
- Samme nøkkel til kryptering og dekryptering
- Men hvordan skal de bli enige om denne nøkkelen uten at noen andre får tak i den?



Bob Alice

Asymmetrisk kryptering

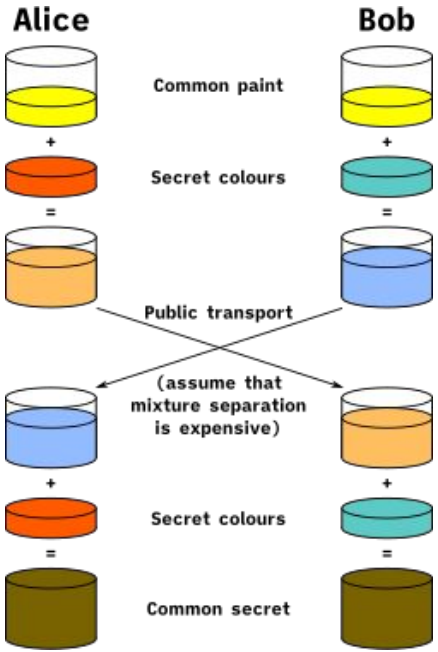
- Begge parter har to nøkler hver, en privat og en offentlig
  - Offentlig er for:
    - Kryptering
    - Verifisering av signatur
  - Privat er for:
    - Dekryptering
    - Signering



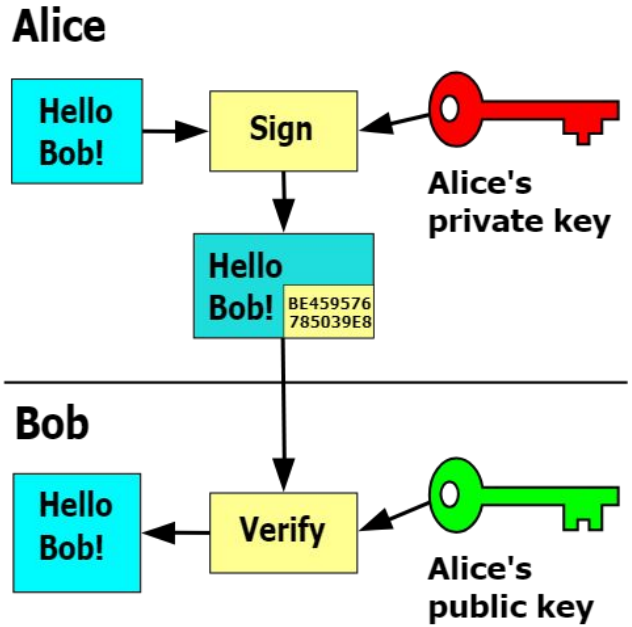
Bob Alice

# Bruksområder til asymmetrisk kryptering

Diffie-Hellman nøkkelutveksling




Digital Signatur



# LMC

```
          INP
          STA a
          INP
          BRZ print
          LDA a
          SUB b
          STA a
print     LDA a
          OTC
          HLT
a         DAT
b         DAT 32
```

Hva skrives ut når denne koden kjøres og bruker gir følgende inndata: **114** og **999**?

Det følgende programmet er skrevet i en tenkt utgave av LMC, som har en ekstra instruksjon AX2. Det denne instruksjonen gjør er å gange verdien i akkumulatoren med 2, og skrive resultatet tilbake til akkumulatoren.

Gitt dette LMC-programmet:

```
INP
STA 50
INP
STA 51
AX2
OUT
HLT
```

Gitt at brukeren skriver inn tallene 2 og 5 som input, hva vil skrives ut?

# LMC

```
        INP
        STA a
        INP
        BRZ print
        LDA a
        SUB b
        STA a
print   LDA a
        OTC
        HLT
a       DAT
b       DAT 32
```

Hva skrives ut når denne koden kjøres og bruker gir følgende inndata: **114** og **999**?

Det følgende programmet er skrevet i en tenkt utgave av LMC, som har en ekstra instruksjon AX2. Det denne instruksjonen gjør er å gange verdien i akkumulatoren med 2, og skrive resultatet tilbake til akkumulatoren.

Gitt dette LMC-programmet:

```
INP
STA 50
INP
STA 51
AX2
OUT
HLT
```

Gitt at brukeren skriver inn tallene 2 og 5 som input, hva vil skrives ut?

```
        INP
        STA a
        INP
        STA b
loop    LDA a
        INSTRUKSJON 1
        INSTRUKSJON 2
        INSTRUKSJON 3
        INSTRUKSJON 4
        LDA a
        SUB en
        STA a
        BRA loop
slutt   LDA res
        OUT
        HLT
res     DAT 0
a       DAT
b       DAT
en      DAT 1
```

Du lager et lite program for å gange sammen to tall **a** og **b**, slik at

res = a * b

Du har skrevet programmet over, men det mangler noen instruksjoner. Hvilke?

```
        INP
        STA a
        INP
        STA b
loop    LDA a
        INSTRUKSJON 1
        INSTRUKSJON 2
        INSTRUKSJON 3
        INSTRUKSJON 4
        LDA a
        SUB en
        STA a
        BRA loop
slutt   LDA res
        OUT
        HLT
res     DAT 0
a       DAT
b       DAT
en      DAT 1
```

1. BRZ slutt
2. LDA res
3. ADD b
4. STA res

Du lager et lite program for å gange sammen to tall **a** og **b**, slik at

res = a * b

Du har skrevet programmet over, men det mangler noen instruksjoner. Hvilke?

Vi skal kode et program som teller antall ganger bruker gir en input til LMC og printer summen av alle input 🧐

# Oblig eller ukesoppgaver