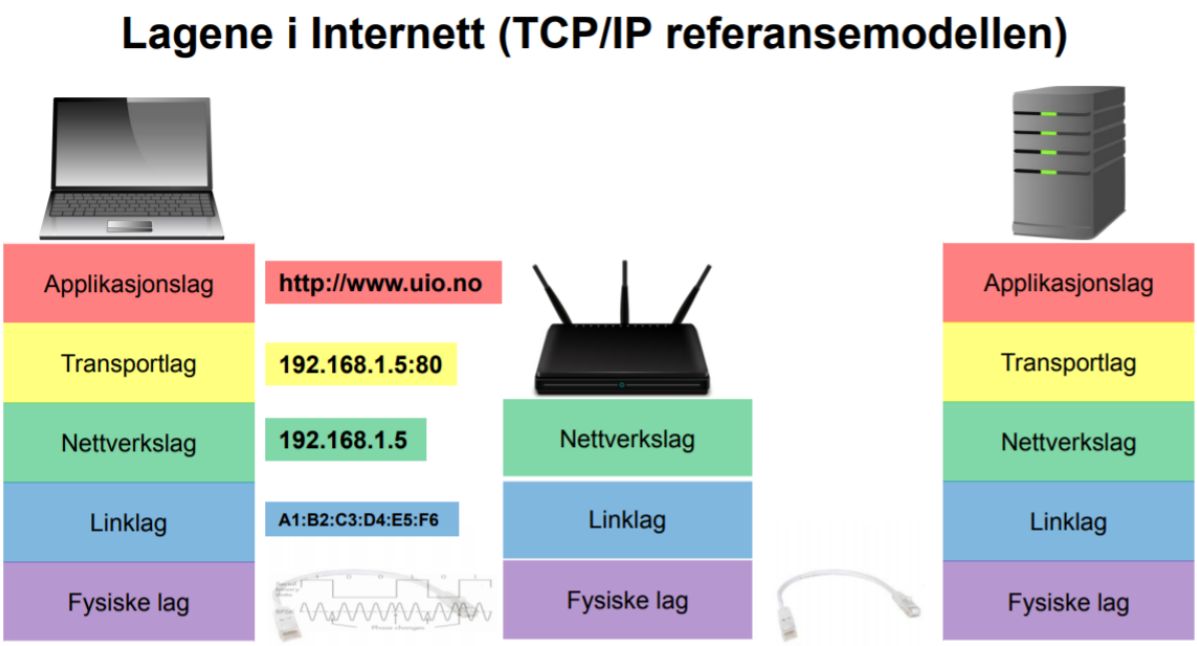
Seminar 10 (lagene spiller sammen + kryptering)

Pensum

https://s3-us-west-2.amazonaws.com/secure.notion-static.com/6c457fcc-2624-490e-bb5d-31081f30b6c9/uke-43-lagene-spiller-sammen.pdf

https://s3-us-west-2.amazonaws.com/secure.notion-static.com/e81f3d40-d118-46bb-83aa-fe3b627455ff/uke-43-kryptering.pdf

Lagene i TCP/IP-modellen

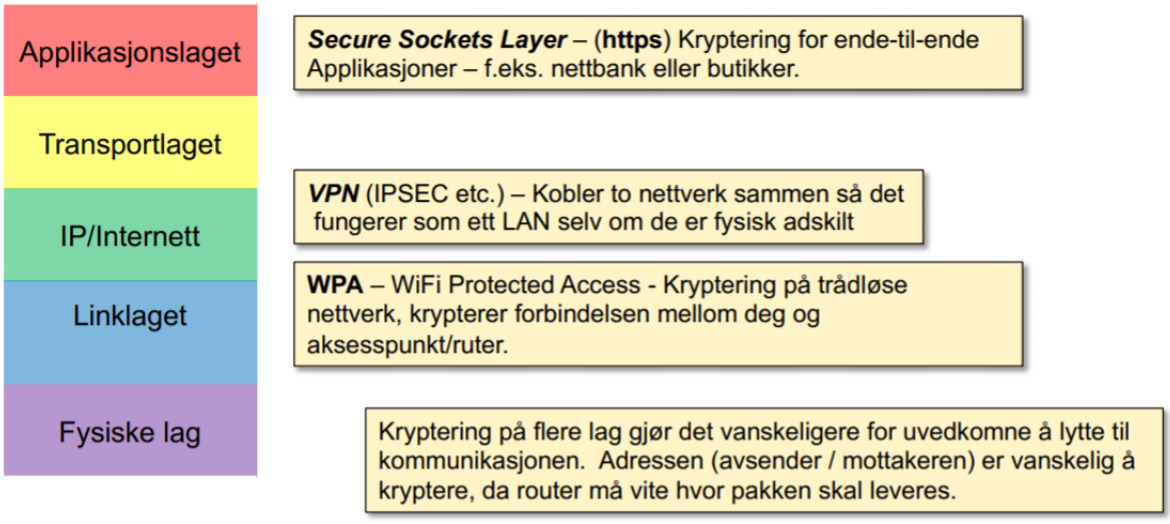


Jehan sin foilene:

https://s3-us-west-2.amazonaws.com/secure.notion-static.com/055cb854-278e-4980-861d-42f5a15f50cc/UKE10.pptx

Key Differences between the Switch & Router

Kryptering og sikkerhet i nettverket



Kryptografi



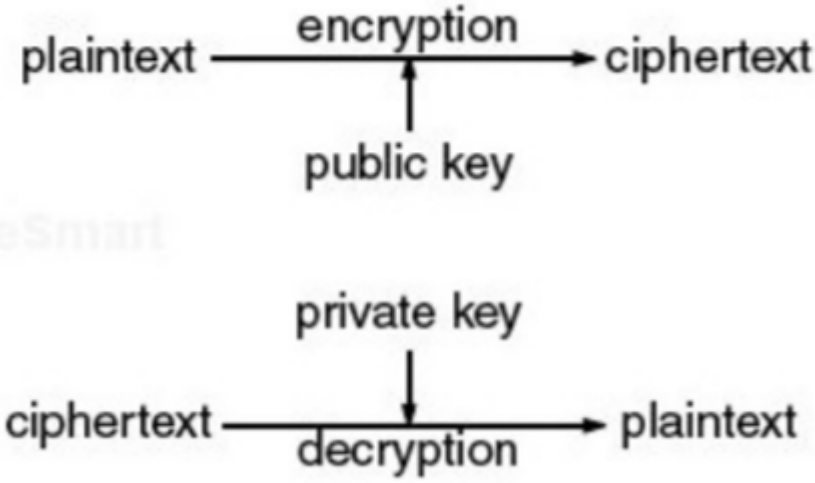
Forskjellige typer kryptering

Symmetrisk



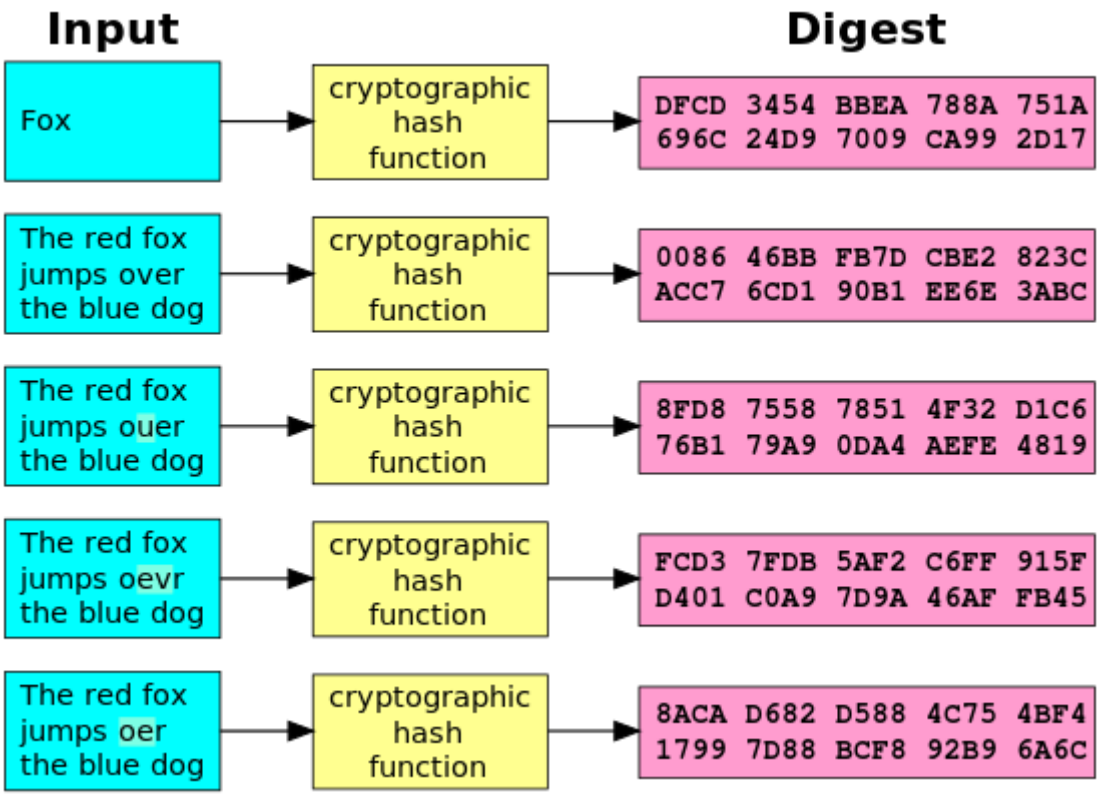
- En nøkkel - men må deles mellom sender og mottaker
- Nøkkel kun sendes gjennom en sikker kommunikasjonskanal
- To typer:
  - Block cipher (DES, 3DES, AES) (deler plaintext i blokker, vanligvis på 128 bits, og så krypterer)
  - Stream cipher (RC4) (krypterer enhver bit)

Asymmetrisk



- To nøkler: privat og offentlig
- Overførsel over usikker kanal
- Sikker lagring på utrygt media
- Mye treigere enn symmetrisk kryptering (kan løses med en hybrid-modell)
  - Offentlig nøkkel brukes for å bli enige om en midlertidig nøkkel.
  - Symmetrisk kryptering brukes under resten av kommunikasjonen

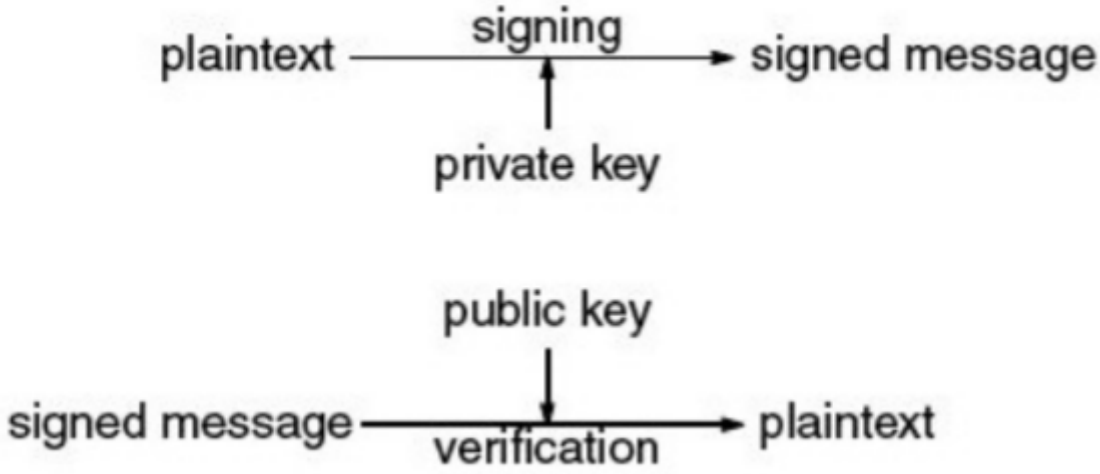
Hash-algoritmer



- Enveis identifikasjon
- Ingen nøkkel
- Generer et tilfeldig tall av et bestemt lengde fra plaintext (uavhengig av plaintext lengde)
  - Raskt å beregne
  - Kan ikke omgjøres: nesten umulig å generere opprinnelige plaintext fra en hash-verdi (kun ved brute-force)
  - Ingen to plaintext meldinger har samme hash-verdi
  - Avalanche-effect: små endringer i plaintext fører til drastiske endringer i hash-verdi
- Brukes til
  - Passord verifikasjon
  - Digital signatur opprettelse og verifikasjon
  - Verifikasjon av dataintegritet

- osv.

Digital signatur



- Genereres av eier (gjerne ved hjelp av hash-algoritmer)
- Verifiseres av mottakeren (egt alle som har offentlig nøkkel)
- En korrekt verifisert signatur bekrefter avsenderens **identitet**, og at meldingen Ikke ble **endret** fra sending til mottak.