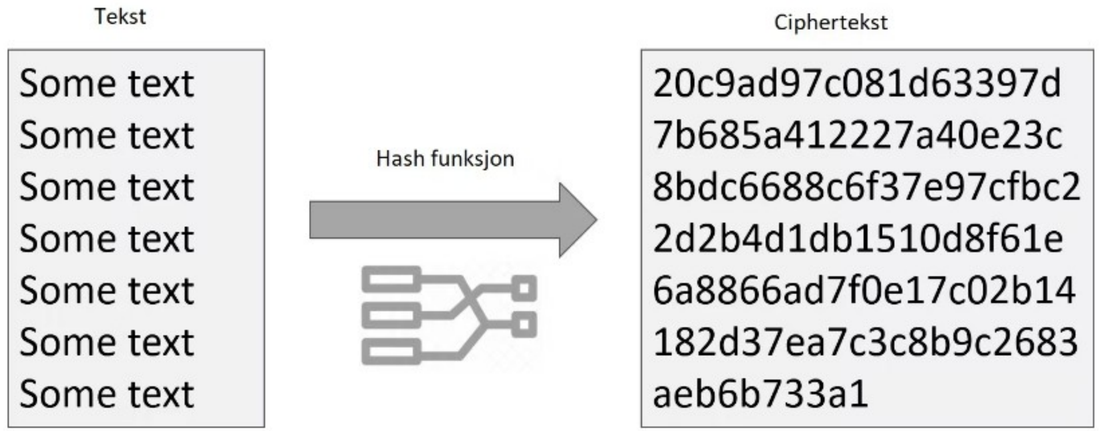
I dag: Kryptografi



Begreper

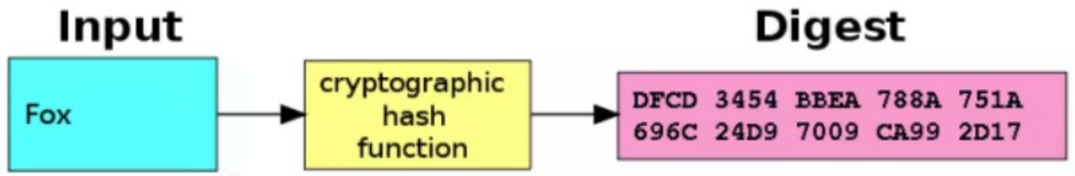
- Klartekst -> vanlig tekst
- Ciphertekst -> kryptert tekst
- Hashing / kryptering -> gjøre klartekst om til chipertekst
- Hashing- / krypteringsalgoritme -> funksjon som tar inn klartekst og returnerer chiphertekst.

Målet med kryptering

- Sikre konfidensialitet og/eller integritet
- Sikre autentisitet
- Autentisering av dataopprinnelse for å oppnå uavviselighet

Former for kryptering

- Hash algoritmer, enveis kryptering
- Symmetrisk kryptering, en hemmelig felles nøkkel
- Asymmetrisk kryptering, en offentlig og en privat nøkkel per person(nøkkelpar)

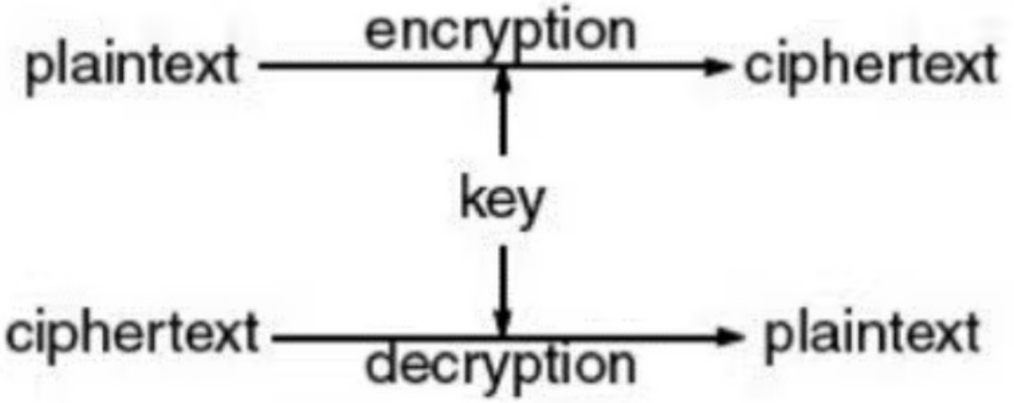


Hash-algoritmer

- Enveis funksjon
  - Man kan utføre krypteringen men man kan ikke dekryptere
- Brukes til:
  - Sjekksum (sjekksumalgoritmer) for å sjekke data integritet
  - For lagring av data. Feks lagring av passord. Dataen er ikke lagret i klartekst.
- Vi har gitt en hash-funksjon. Om en bruker skal logge inn så hasher vi passordet og sjekker om chipherteksten matcher det som er lagret i systemet.

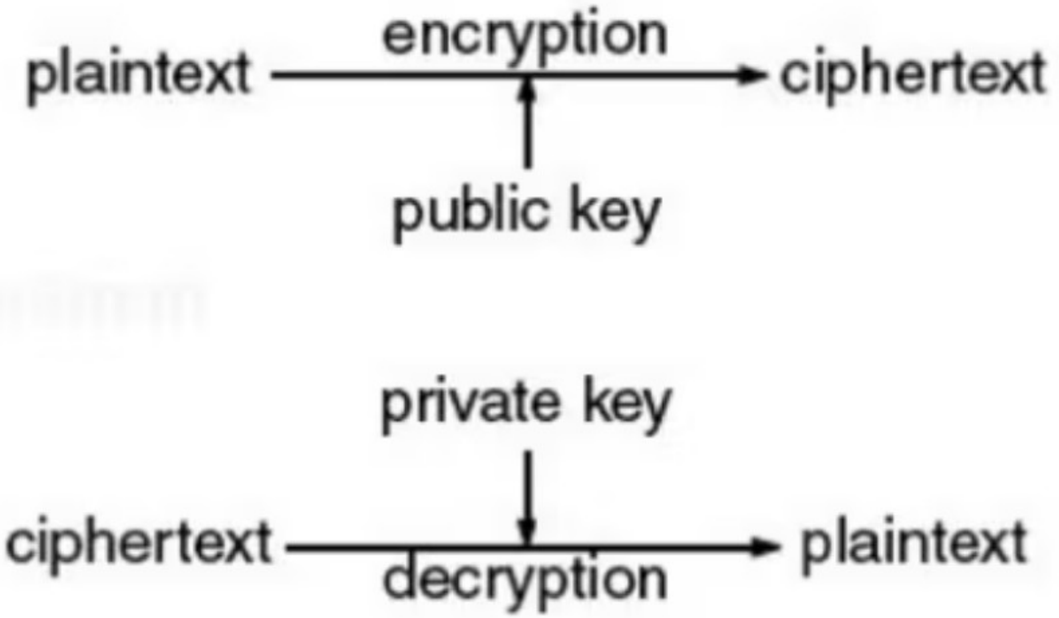
Symmetrisk kryptering

- En hemmelig felles nøkkel mellom sender og mottager
- Nøkkelen blir brukt for å kryptere og dekryptere



Asymmetrisk kryptering

- Hver person har sin offentlige og private nøkkel (et nøkkelpar)
  - Den offentlige nøkkel din er tigjengelig for alle
  - Den private nøkkelen er det bare du som har
- Sender krypterer melding med mottaker sin offentlige nøkkel
- Mottaker degrypterer meldingen med sin private nøkkel
- Da kan **bare** mottaker dekryptere meldingen, ingen andre



Hybrid modell

- → Asymmetrisk krypering går treigt
- → Så vi bruker en hybrid modell
- → Asymmetrisk kryptering for å bli enigje om en midlertidig felles nøkkel
- → Symetrisk krypering brukes under resten av kommunikasjonen

Digital signatur

- Får å oppnå uavviselighet
  - At vi har bevis for hvem som har sent en melding
- Alice skal sende en melding til bob
- Alice signerer meldingen med sin private nøkkel (som bare hun har)
- Bob mottar meldingen og verfiserer at meldingen er fra Alice med Alice sin offentlig nøkkel
- Vi vet at meldingen må være fra Alice fordi det er bare alice som har den private nøkelen sin
- Vi er også sikre på at nøkkelen ikke er falsk pga den er knyttet til sertifikat