IN1020 uke 8

GRUPPE 10

Plan for dagen

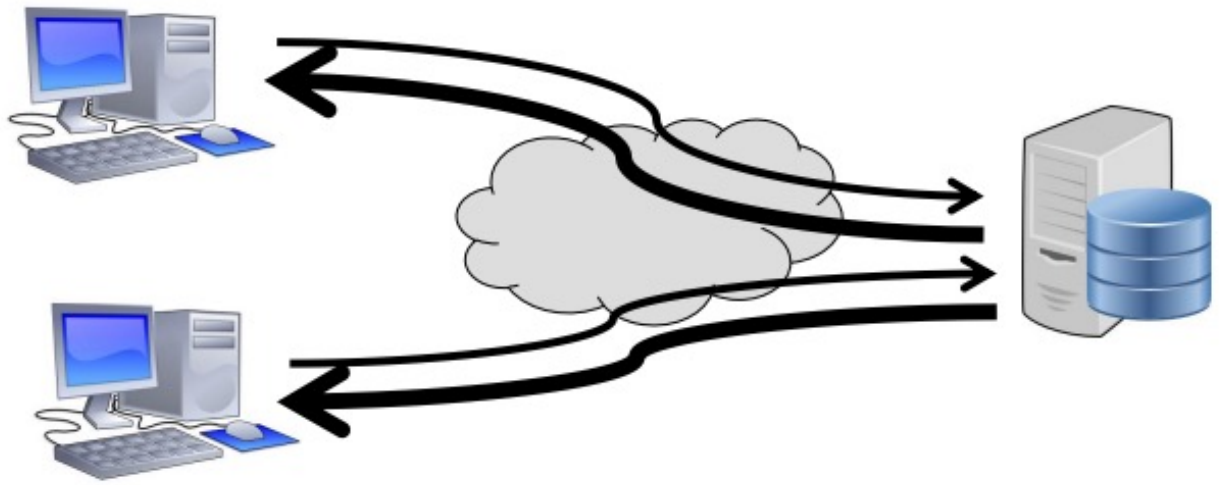
- Nettverk
- Kryptering
- Trygg lagring
- Nettverksikkerhet
- Lab

UiO : Institutt for informatikk
Det matematisk-naturvitenskapelige fakultet

Aksessmodeller: Klient-tjener

- Tradisjonell kommunikasjonsmodell, lettfattelig abstraksjon
  - Klienter ber om en tjeneste (oppretter en forbindelse)
  - Tjenere leverer tjenesten (svarer på forespørselen)

- Eksempler: Webklient (nettleser)/Webtjener, Mailklient/tjener, FTP

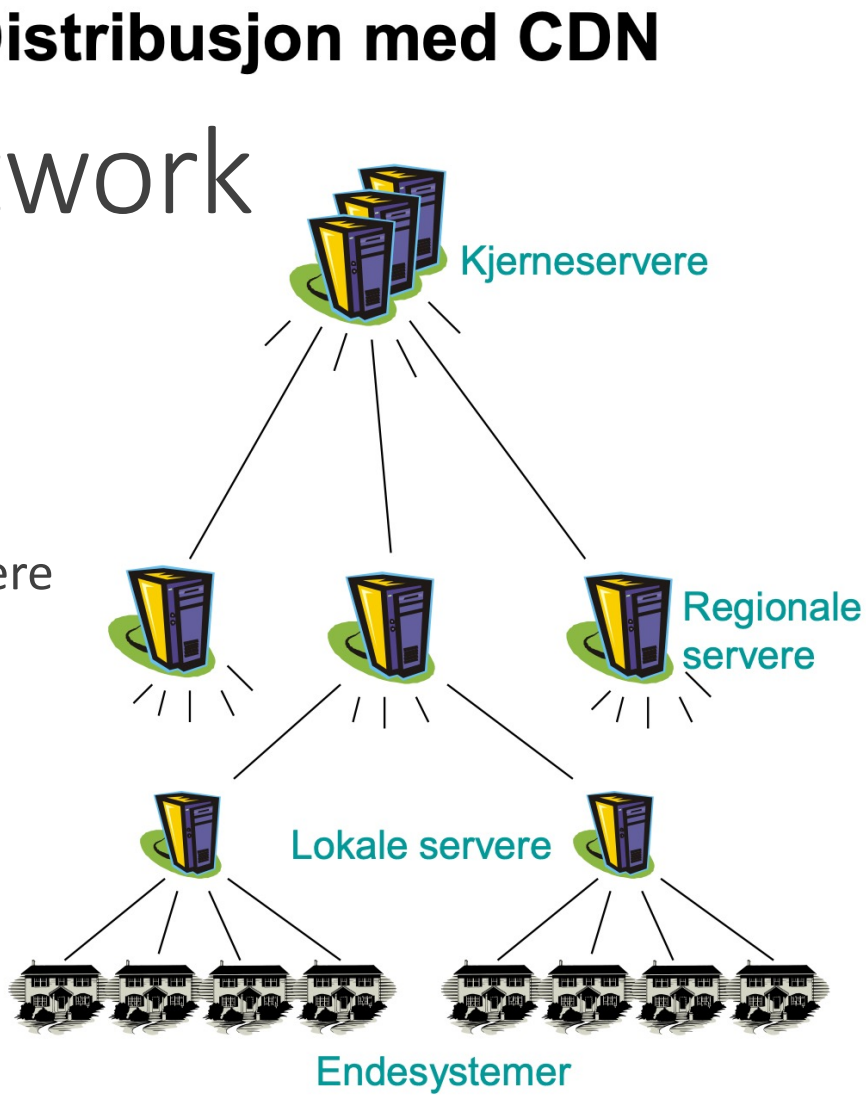


Forbindelsesstrategier

- **Pull:**
  - Klienten ber tjeneren oms en tjeneste
  - Tradisjonelt den vanligste metoden
- **Push:**
  - Tjeneren «dytter» en tjeneste til klienten
  - Krever at det er en forbindelse fra før, eller at klienten lytter
- **Publish-subscribe:**
  - Variant av «Push» der tjeneren dytter ut beskjeder til en gruppe av abonnenter

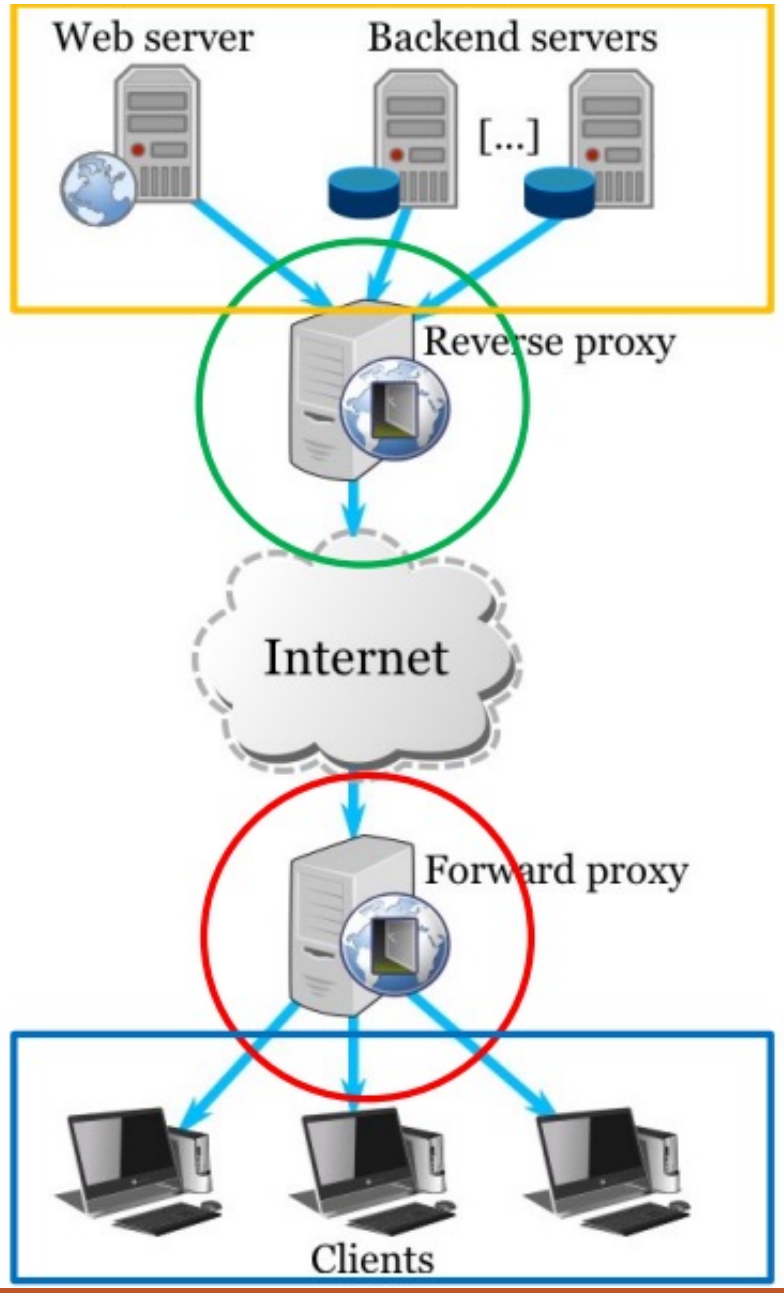
CDN – Content Delivery Network

- Hierkisystem:
  - Populært innhold blir prioritert, så de blir cachet
- Populære videoer blir lagret nærme sluttbrukerne
- Upopulære videoer blir enten lagret på eller nærme kjerneservere
- Brukes for å forbedre ytelse f.eks.:
  - Raskere innlasting av sider
  - Laster inn videoer fortere



Proxy-cache

- En forward proxy står nær klienten:
  - Og mellomlagrer data for klientene,
    slik at de ikke behøver å gå helt til kilden
- En «Reverse Proxy» står nær tjeneren:
  - Og mellomlagrer data fra en eller flere tjenere,
    slik at klienten slipper å gå helt til kilden
- Fordeler:
  - Lastbalansering
  - Sparer nettverkskapasitet
  - Lavere forsinkelse



Peer-to-Peer

- **På flere måter likt CDN:**
  - Endesystemer kan være både klient og tjener
  - Distribuert lagring
  - Innholdet nærmere sluttbruker
  - Begrenset lagring per endesystem

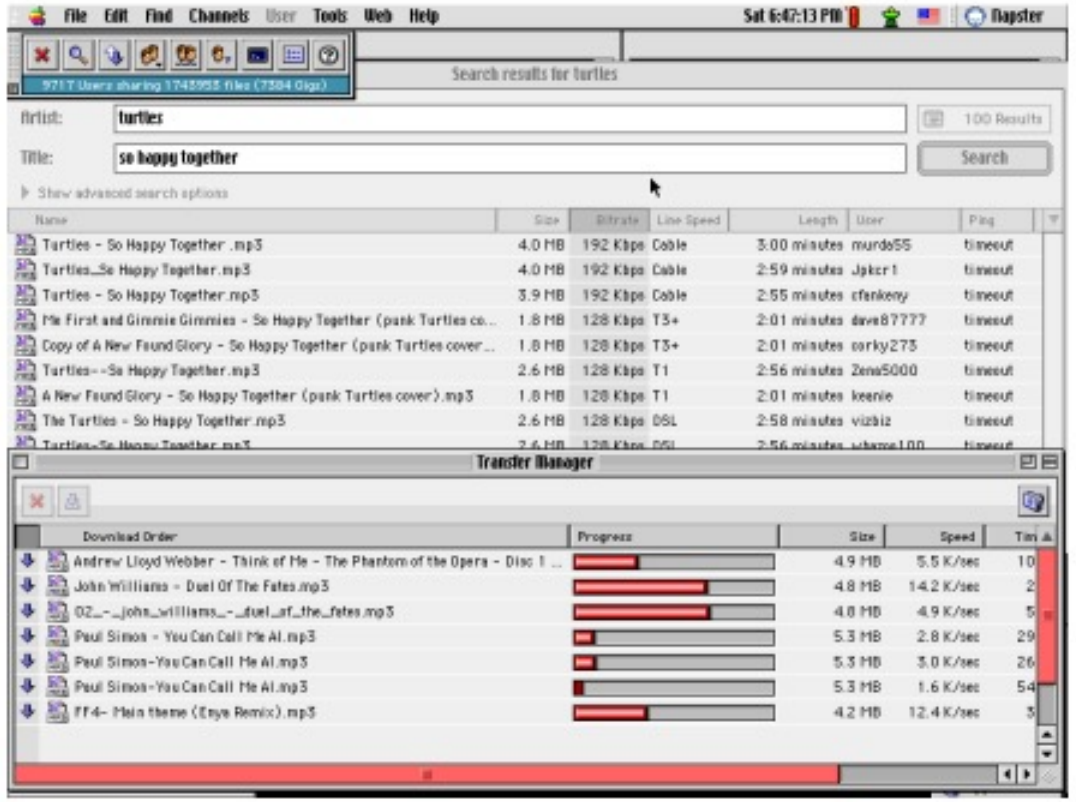
- **Men ulikt på noen punkter:**
  - Ingen klare roller på endesystemene
  - Ikke noe hierarkisk forhold
  - Klienter vet nødvendigvis ikke hvor innholdet er
    - Trenger protokoller for å «oppdage innhold»

Eksempel: Napster

- Program for deling av filer (musikk) over Internett

- Arkitektur
  - Sentralisert index (katalog)
  - Distribuert lagring og nedlastning
  - Alle filer lastet ned blir delt
  - Lansert i 1999

- P2P aspekter:
  - Endesystemene var også filtjenere



DNS – Domain name System

- DNS synker domenenavn med IP-adresser
- Gjør det enklere for mennesker å huske, mens maskinene på nettet bruker IP-adressene
- Når man skriver inn en webadresse/URL matcher DNS denne adressen med tilsvarende IP-adresse og kobler en til den nettsiden
- Bruker klient/tjener modellen:
  - UDP eller TCP port 53
  - Tjenere må bruke TCP seg i mellom (fra nylig)
  - Klienter som bruker TCP avvises ofte:
    - Reduserer lasten på DNS-tjeneren

HTTP – hypertext transfer protocol

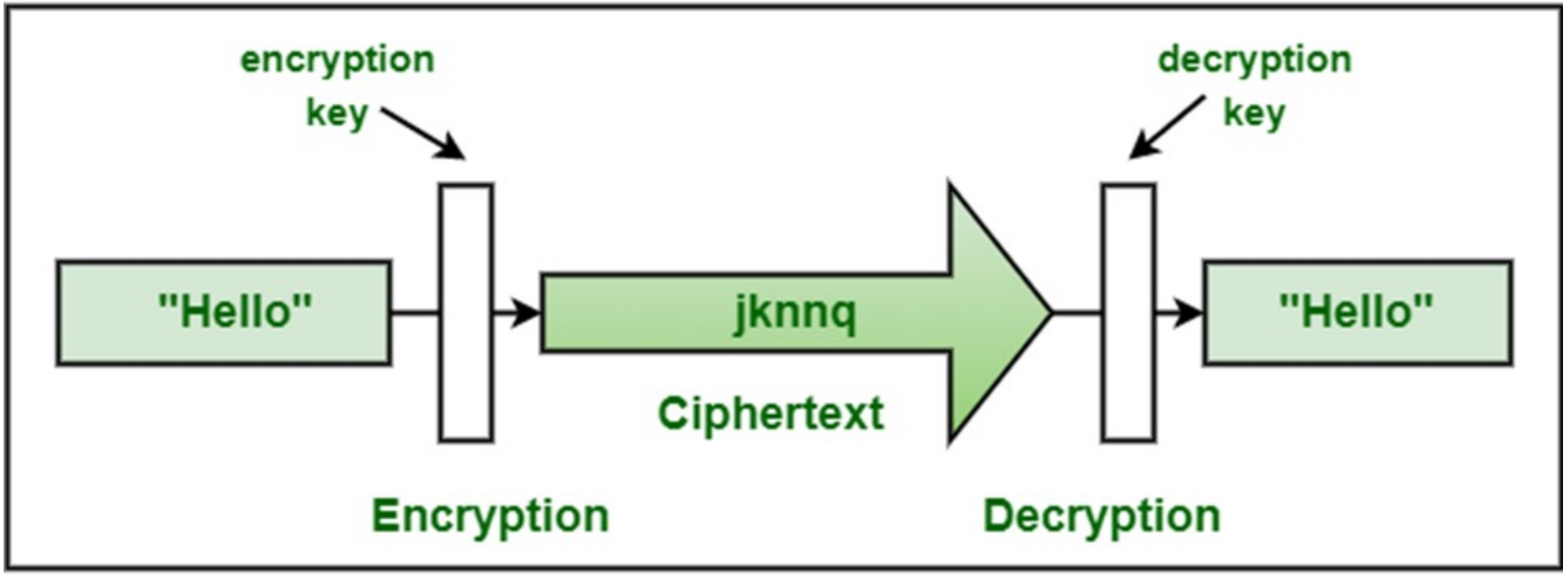
- Applikasjonslagsprotokollen for Web eller nettleser
- Bruker klient/tjenermodell:
  - Klient: nettleser som spør etter, får og viser webobjekter
  - Tjener: sender web-objekter som svar som forespørsler
- Port 80, reservert til web
- Bruker TCP som transport

HTTP-streaming

- Dynamisk, adaptive streaming over HTTPS (DASH)
- Bruker TCP og UDP som transportprotokoll
- Dele opp videoer opp i biter på ca. 2-10 sek
- Bitene er uavhengig og det er flere versjoner av biter med forskjellig kvalitet
- Videospiller fungere som en nettleser, der den spør serveren om den kan levere et segment og serveren sender segment med lavest kvalitet og mottaker mottar
- Dersom pakken, ikke ble mistet så sender serveren gradvis bedre og bedre kvalitet. Helt til optimal kvalitet er oppnådd

Kryptering

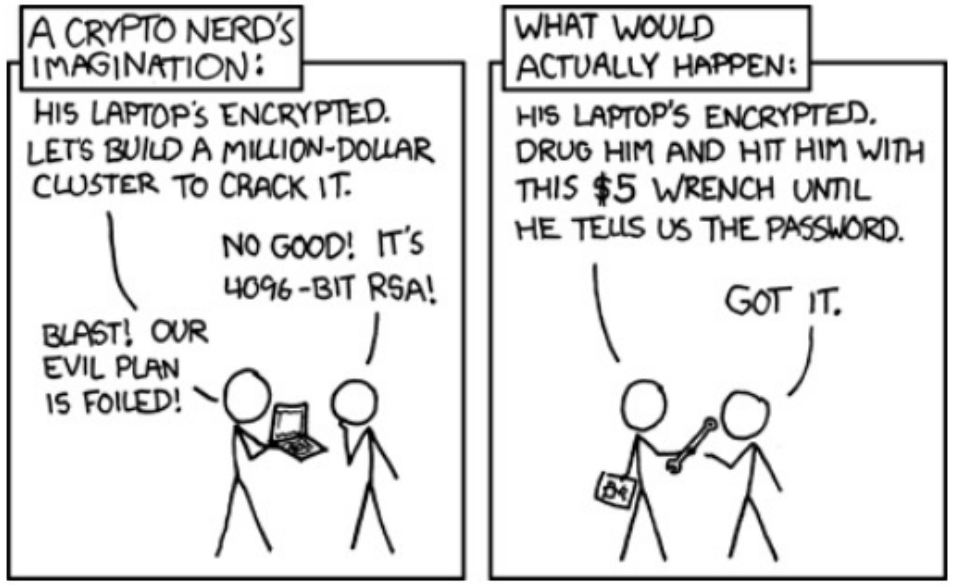
- *Kryptering* er en matematisk metode som sørger for *konfidensialitet* ved at informasjon ikke kan leses av uvedkommende. – datatilsynet
- Kryptografi: Viktige definisjoner
- Beskjeder:
  - Plaintext / klar tekst
  - Ciphertext / kryptert tekst
- Ingredienser:
  - Algoritmer
  - Nøkler



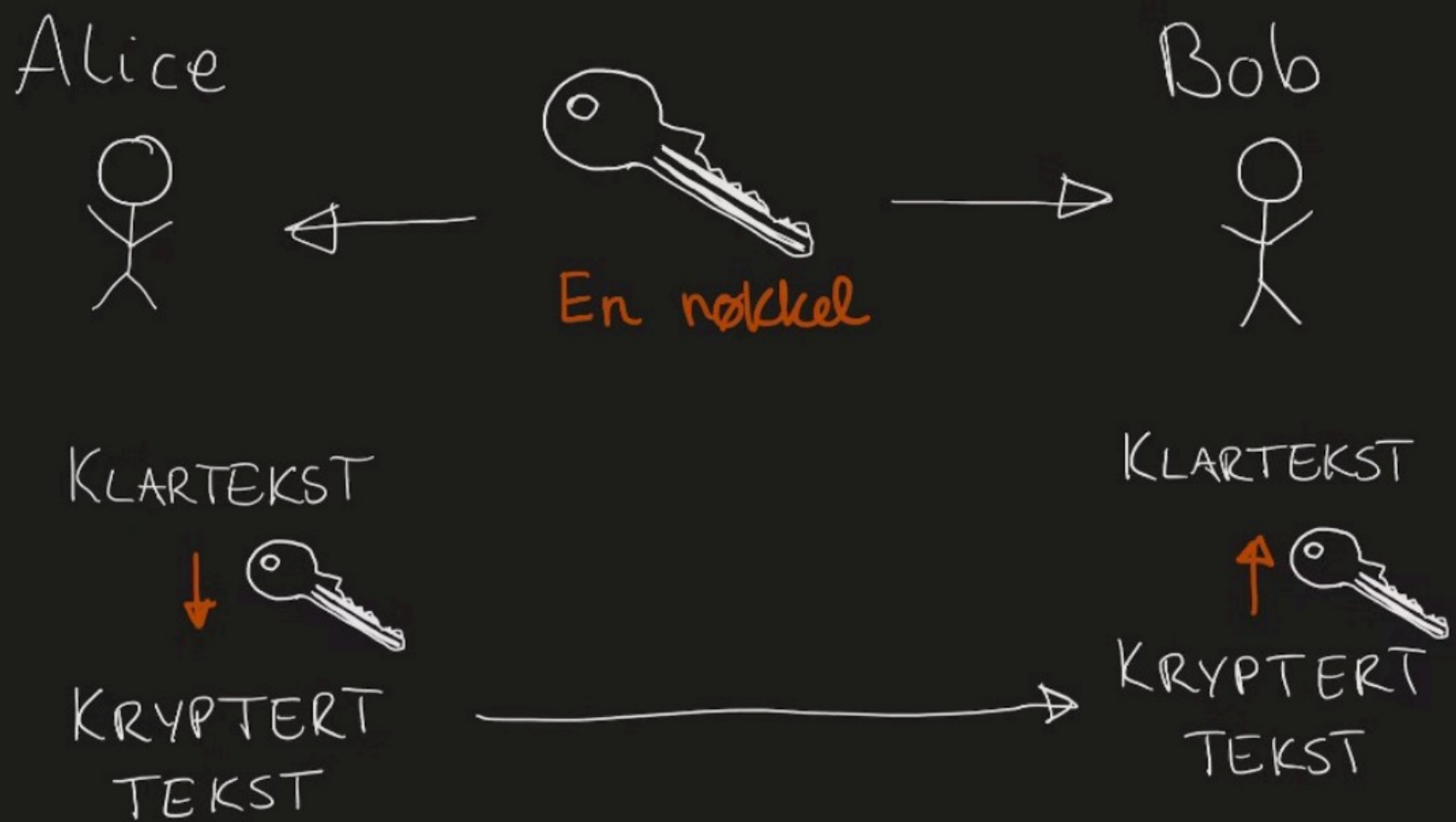
Cryptography

Forskjellige typer kryptering

- *Symmetrisk kryptering*
  - *Hemmelig nøkkelkryptering*
  - En nøkkel: Men må deles mellom sender og mottaker)
- *Hash-algoritmer*
  - Enveis identifikasjon
  - Ingen nøkkel
- *Asymmetrisk kryptering*
  - Offentlig nøkkelkryptering
  - To nøkler:
    - Privat
    - Offentlig



Symmetrisk Kryptering

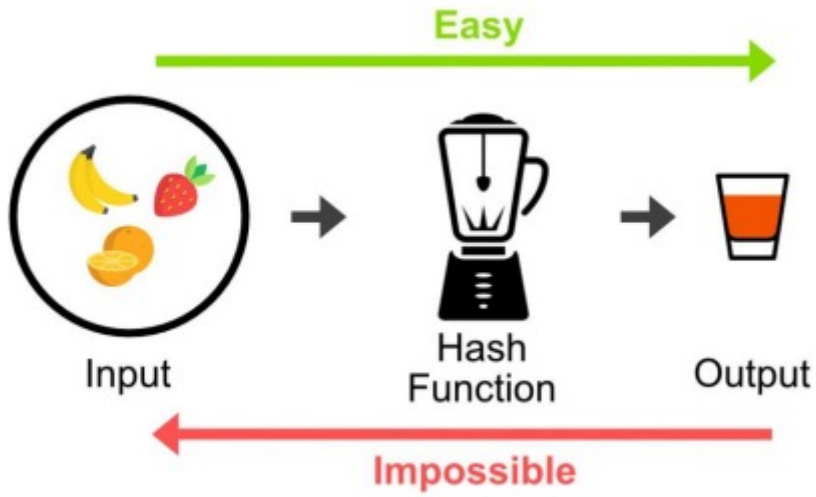


Anvendelse av symmetrisk kryptering

- Bruker **identisk nøkkel** til kryptering og dekryptering.
- Anvendelse: Kryptering av data, kryptering av meldinger
- **Hvilke sikkerhetsmål kan ivaretas?**
  - Konfidensialitet? **JA**
  - Integritet? I praksis **JA**
  - Autentisitet til dataopprinnelse? I praksis **JA**
  - Uavviselighet? **NEI**
- **Farer**: Nøkkel på avveie, nøkkel tapt

Kryptografisk enveisfunksjon (hash-funksjon)

- Sjekke dataintegritet
- Fungerer ved at man hasher klarteksten. Da får man en sjekksum så gjør vi en kryptering og sender cipher teksten til mottaker. Mottaker dekryptere cipher teksten og hasher den og får en sjekksum.
- Hvis sjekksummen er lik så vil det si at dataen er korrekt. Hvis ikke så har deler at dataen forvunnet eller så har noen endret på dataen
- Krav om at det skal være umulig å gå fra sjekksum til klartekst, altså umulig å gjette seg fram



Asymmetrisk Kryptering

Alice



To nøkler

Bob

KLARTEKST

BOB SIN OFFENTLIG NØKKEL

KRYPTERT TEKST

KLARTEKST

BOB SIN PRIVATE NØKKEL

KRYPTERT TEKST

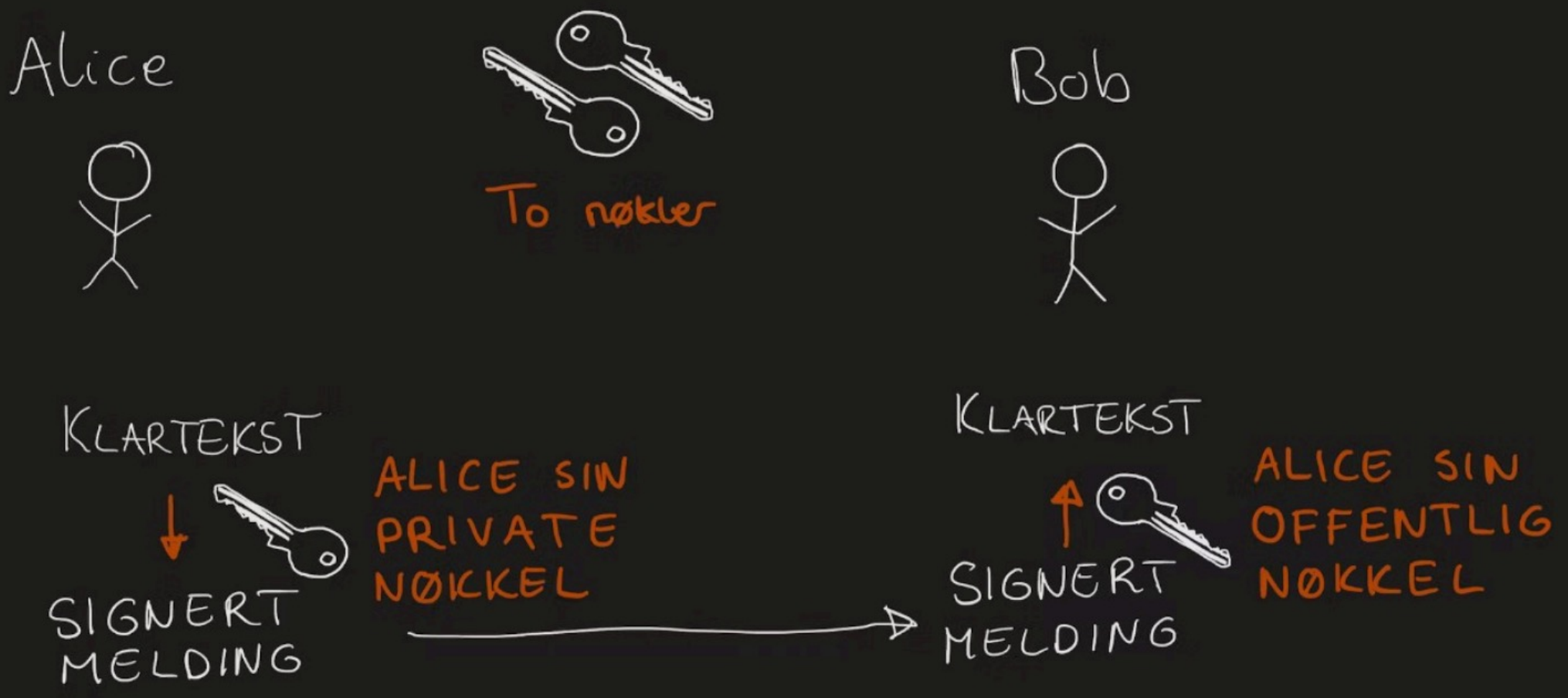
Asymmetrisk kryptering for meldingsutveksling:

- **Nøkkelpar**: Sender benytter mottagers offentlige nøkkel for å kryptere en melding, mottager benytter sin private nøkkel til å dekryptere meldingen.
- **Anvendelse**: Trygg overføring av data/melding, autentisering

- **Hvilke sikkerhetsmål kan ivaretas?**
  - Konfidensialitet? **JA**
  - Integritet? I praksis **JA**
  - Autentisitet til dataopprinnelse? **NEI**
  - Uavviselighet? **NEI**
  - Mottagers autentisitet **JA**

- Farer: Nøkkel på avveie, falske nøkler

DIGITAL SIGNATUR



Asymmetrisk kryptering for digital signering:

- **Nøkkelpar** Sender krypterer (og dermed signerer) en melding med sin private nøkkel. Mottager dekrypterer meldingen med senders offentlige nøkkel.
- **Anvendelse**: Ivareta tillitt til at meldinger kommer fra en hevdet avsender, autentisering.
- **Hvilke sikkerhetsmål kan ivaretas?**
  - Konfidensialitet? **NEI**
  - Integritet? I praksis **JA**
  - Autentisering av dataopprinnelse? **JA**
  - Uavviselighet? **JA**
- Farer: Nøkkel på avveie, falske nøkler

PKI – public key infrastructure

- Rammeverk for utstedelse, administrasjon og bruk av digitale sertifikater med offentlige nøkler
- Hovedmål: Sikre ektheten av offentlige nøkler, samt trygg og forsvarlig nøkkel-distribusjon
- En PKI må bestå av:
  - En policy for sertifikat-håndtering
  - Teknologi for å implementere policyen
  - Prosedyrer for hvordan håndtere og forvalte nøklene
  - Tillittsmodell for sertifikatene med offentlige nøkler

Trygg lagring

- Kryptering:
  - Gjør dataen uforståelig for uvedkommende
  - Å kryptere lagrede data er en strategi for å understøtte konfidensialitet og integritet
  - Sørge for at uvedkommende ikke får tak i data
  - Sørge for at hvis det blir gjort endringer så blir det oppdaget

- Sikkerhetskopiering:
  - Strategi for å ta vare på informasjon over tid
  - Bidra til økt tilgjengelighet ved å være i stand til å gjennomrette systemer og data ved uønskede hendelser som endrer eller sletter informasjon

Klassifisering av informasjon



PS: tatt fra forelesning

I noen sammenhenger så finnes det også svart data: kilde

Lagring og samarbeid

Hvor skal jeg lagre dokumentene mine?

På UiO kan du velge blant en rekke løsninger for lagring/oppbevaring og deling av dokumenter.

Hva er lov? Hva kan lagres hvor?

På UiO er informasjonssikkerhet viktig. For å gjøre det enklere å overholde lovverket deler vi inn informasjon i fire klasser og tildeler lagring etter informasjonens beskyttelsesbehov.

Hjelp! Jeg har mistet dokumentet mitt

Her finner du hjelp til å legge tilbake en backup, eller sikkerhetskopi, av en fil eller et dokument du har mistet.

Vis flere hjelpeartikler

Aktuelle tjenester

☑ Vis hva som er lovlig å lagre

Dropbox – UiO-Dropbox
Lagring og samarbeid
● ● Gule og grønne data

Hjemmeområdet – personlig fillagring for ansatte og studenter
Lagring og samarbeid
● ● Gule og grønne data

Aktuelle tjenester

Vis hva som er lovlig å lagre

Dropbox – UiO-Dropbox
Lagring og samarbeid
Gule og grønne data

Hjemmeområdet – personlig fillagring for ansatte og studenter
Lagring og samarbeid
Gule og grønne data

Fellesområder – lagring og deling av dokumenter
Lagring og samarbeid
Opptil røde data*

Tjenester for Sensitive Data (TSD)
Lagring og samarbeid. IT i forskning. Server- og driftstjenester
Opptil svarte data

Personlig lagringsområde til forskere
Lagring og samarbeid. IT i forskning
Opptil røde data

Sympa, e-postlister – én adresse til mange mottakere
E-post og kalender. Lagring og samarbeid

NRIS Betzy, for større parallelle beregninger
Lagring og samarbeid. IT i forskning
Gule og grønne data

Colossus: Tungregningsklynge for sensitive data
Lagring og samarbeid. IT i forskning
Opptil svarte data

Fox: Tungregningsklynge for brukere av Educloud Research
Lagring og samarbeid. IT i forskning
Opptil røde data

Nettverksikkerhet

- Trusler på nett:
  - Avlytting
  - Data modifisering. F.eks. «*Man in the middle angrep*»
  - Forfalskning
  - Tjenestenektangrep (DDoS): Gjøre ressurser utilgjengelig ved å overlaste serveren med trafikk
  - Uautorisert bruk: Misbruk av ressurser
- Sikkerhetstiltak:
  - Kryptering av nettverk
  - Brannmur
  - Innbruddsdeteksjon:
    - Datavirus
    - Tjenestenektangrep

Lab

- Se på oblig 2
- Midtveisevaluering
- Jobbe videre med oblig eller ukesoppgaver
- Send meg mail eller teamsmelding hvis dere lurer på noe eller trenger hjelp til oblig
- myhd@uio.no