Mentimeter

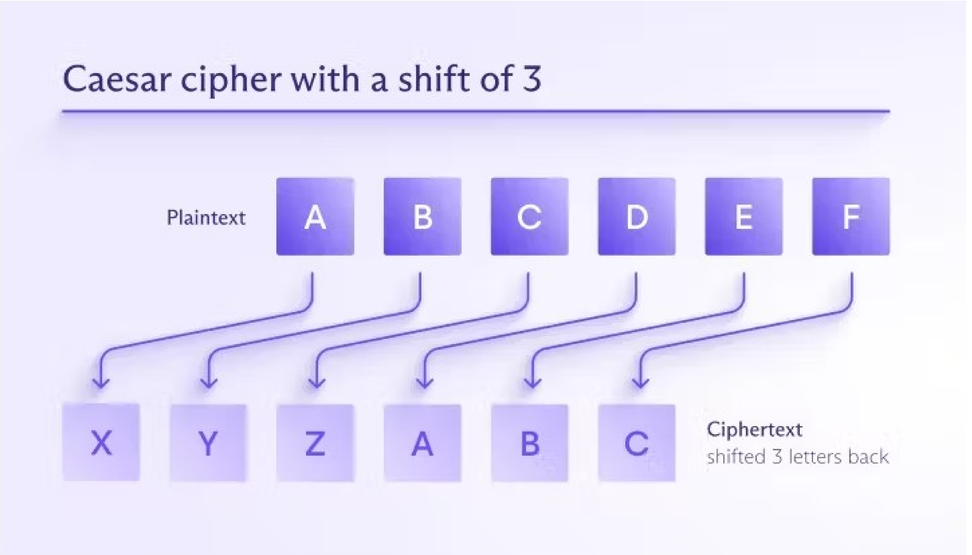
Kryptering og nettverk

Gruppe 16

Mentimeter

Hva er kryptering?

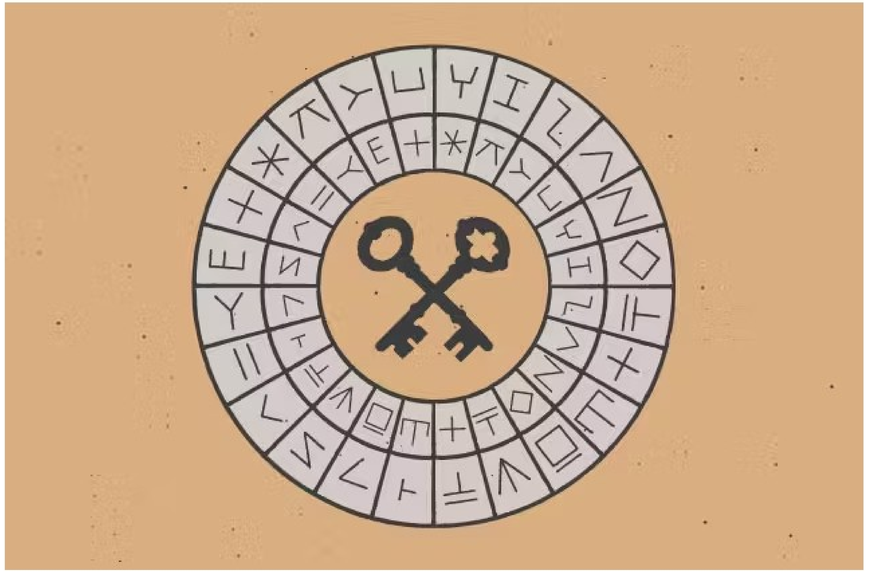
Plaintext -> Ciphertext



Mentimeter

Hvordan knekke kryptering?

- Brute force
- Kjente krypteringer og regler
- Frekvensanalyse



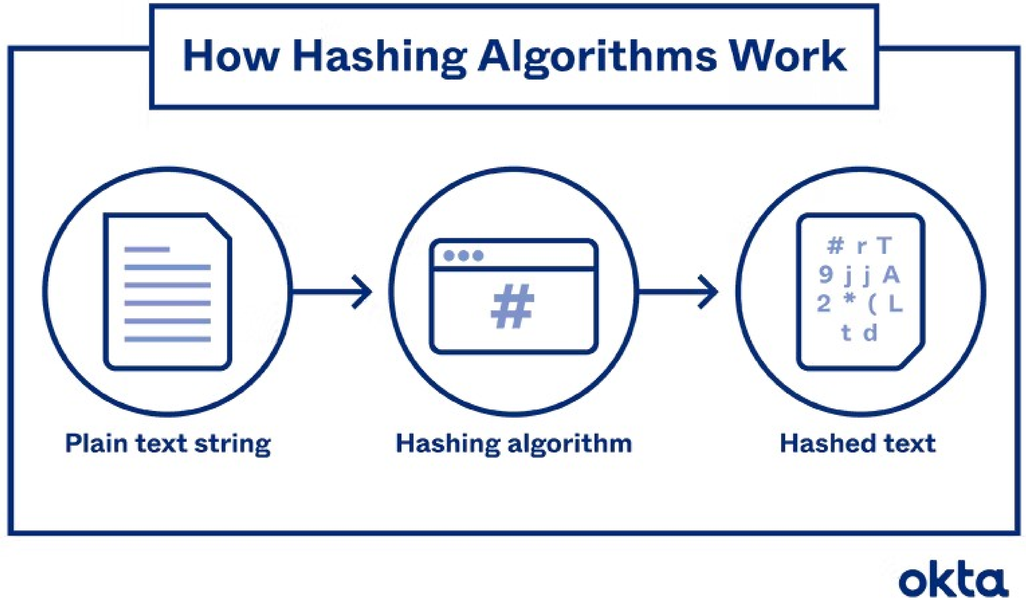
Mentimeter

Forskjellige typer kryptering

Mentimeter

Hash-algoritmer

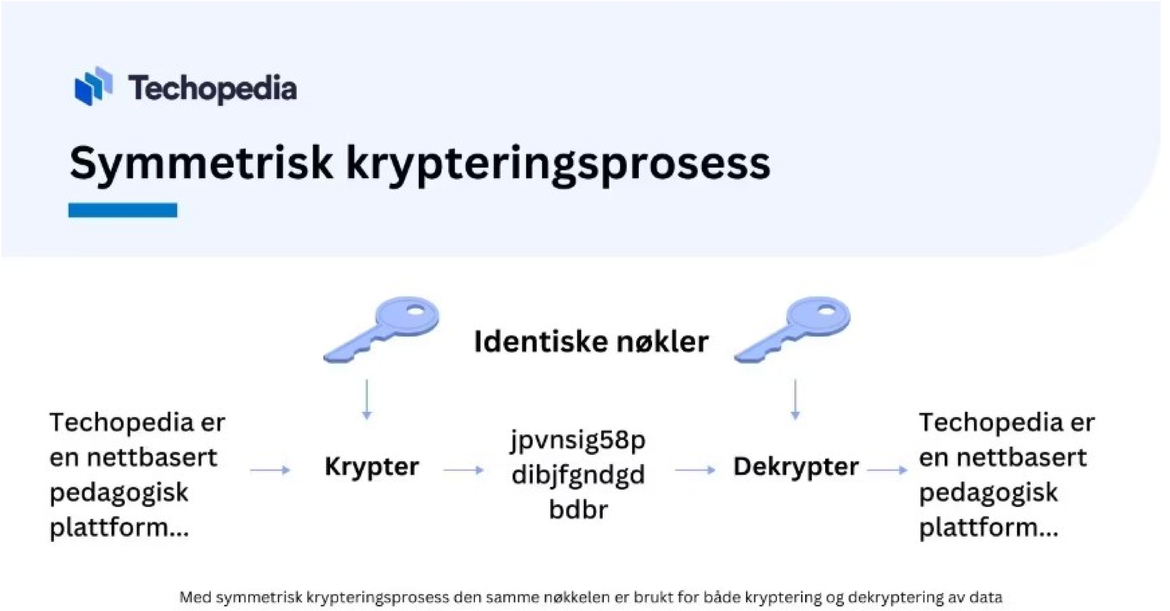
- Sjekksum
- Enveis algoritme



Mentimeter

Symmetrisk kryptering

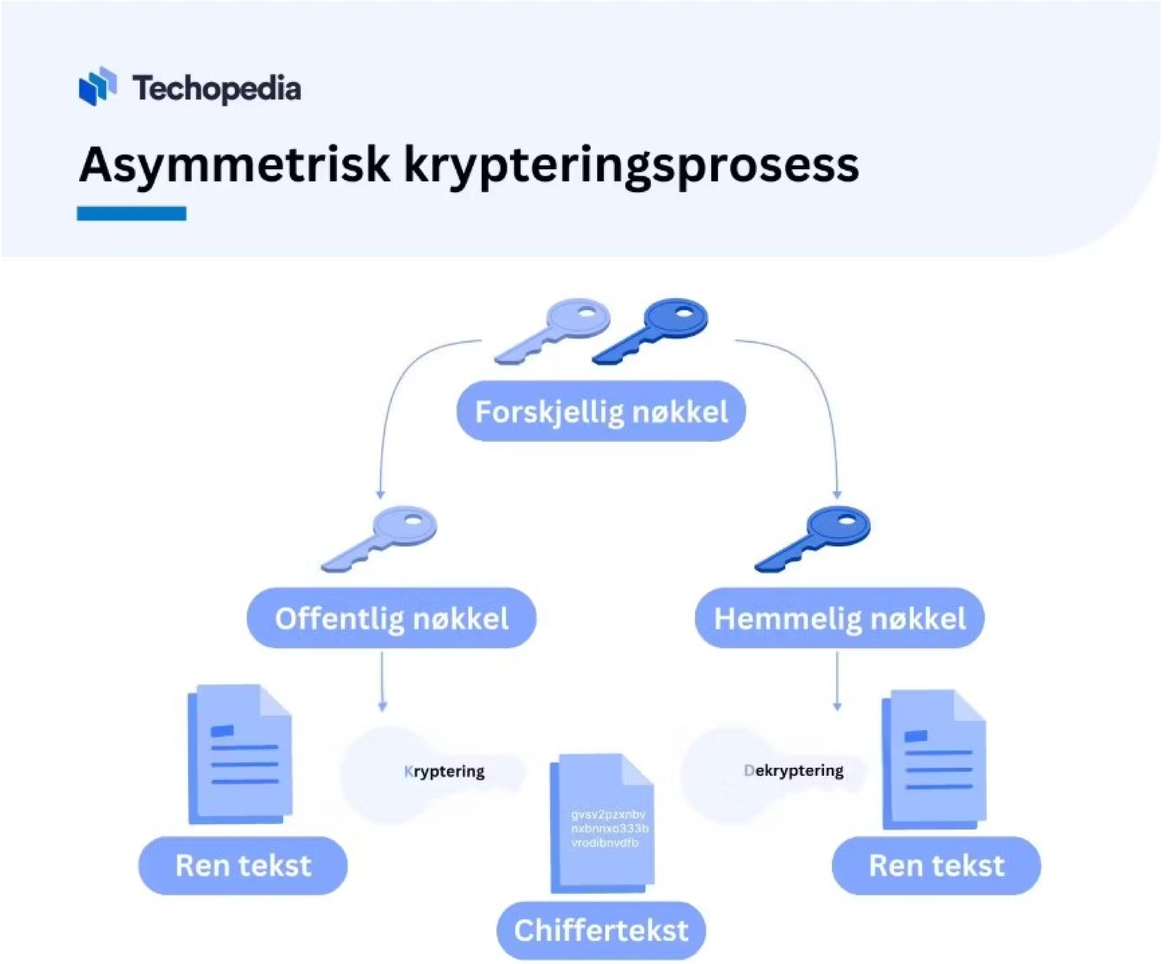
- Samme nøkkel for kryptering og dekryptering
- Block cipher



Mentimeter

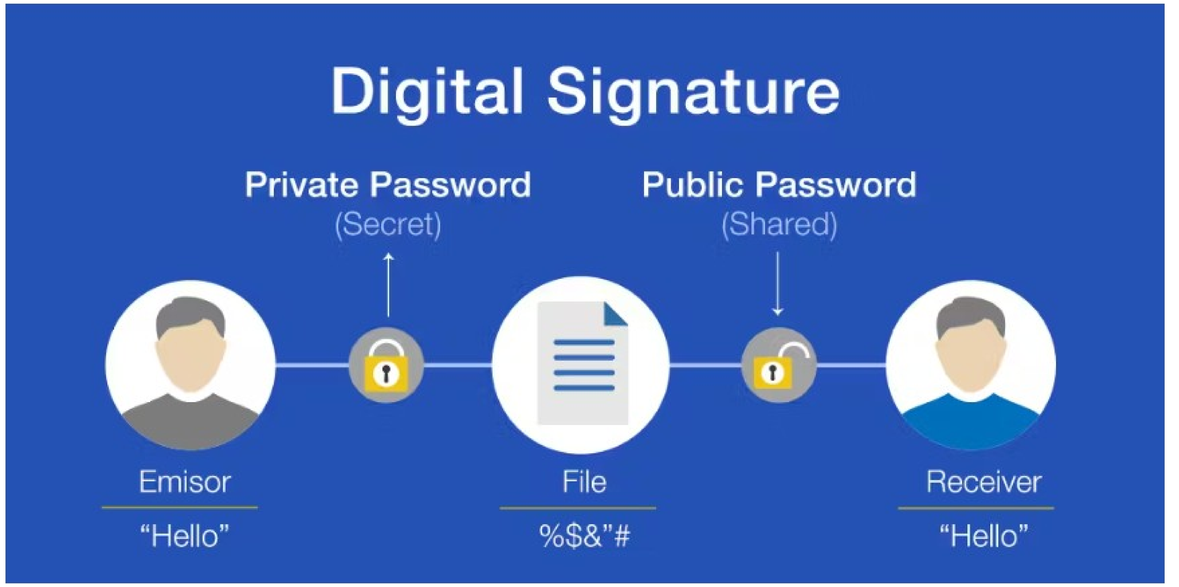
Asymetrisk kryptering

- En privat og en offentlig nøkkel
- Sende meldinge som bare en kan åpne

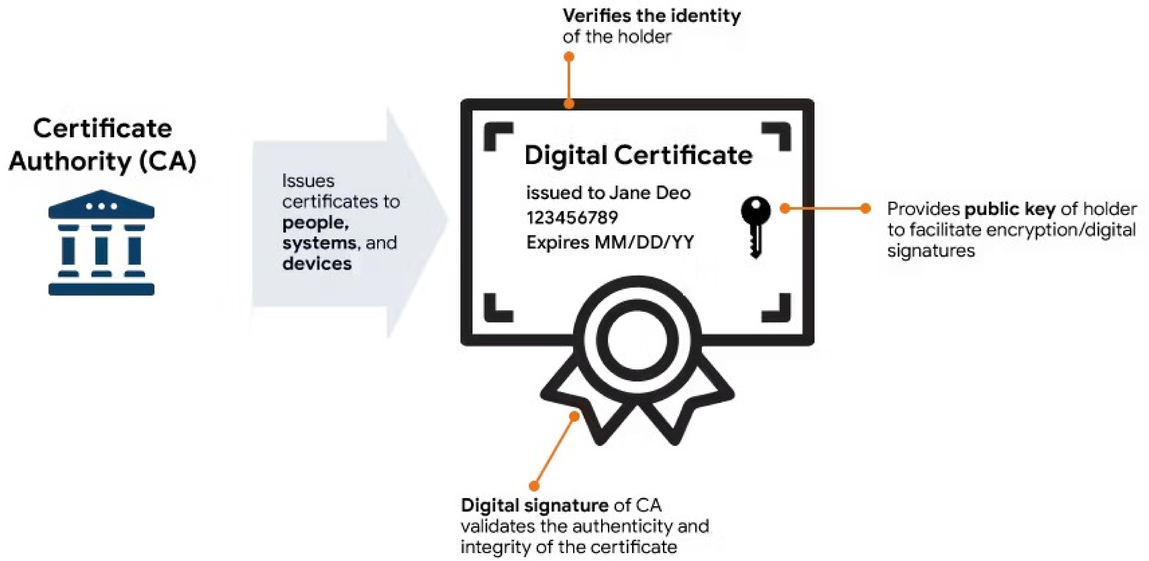


Mentimeter

Digital signatur



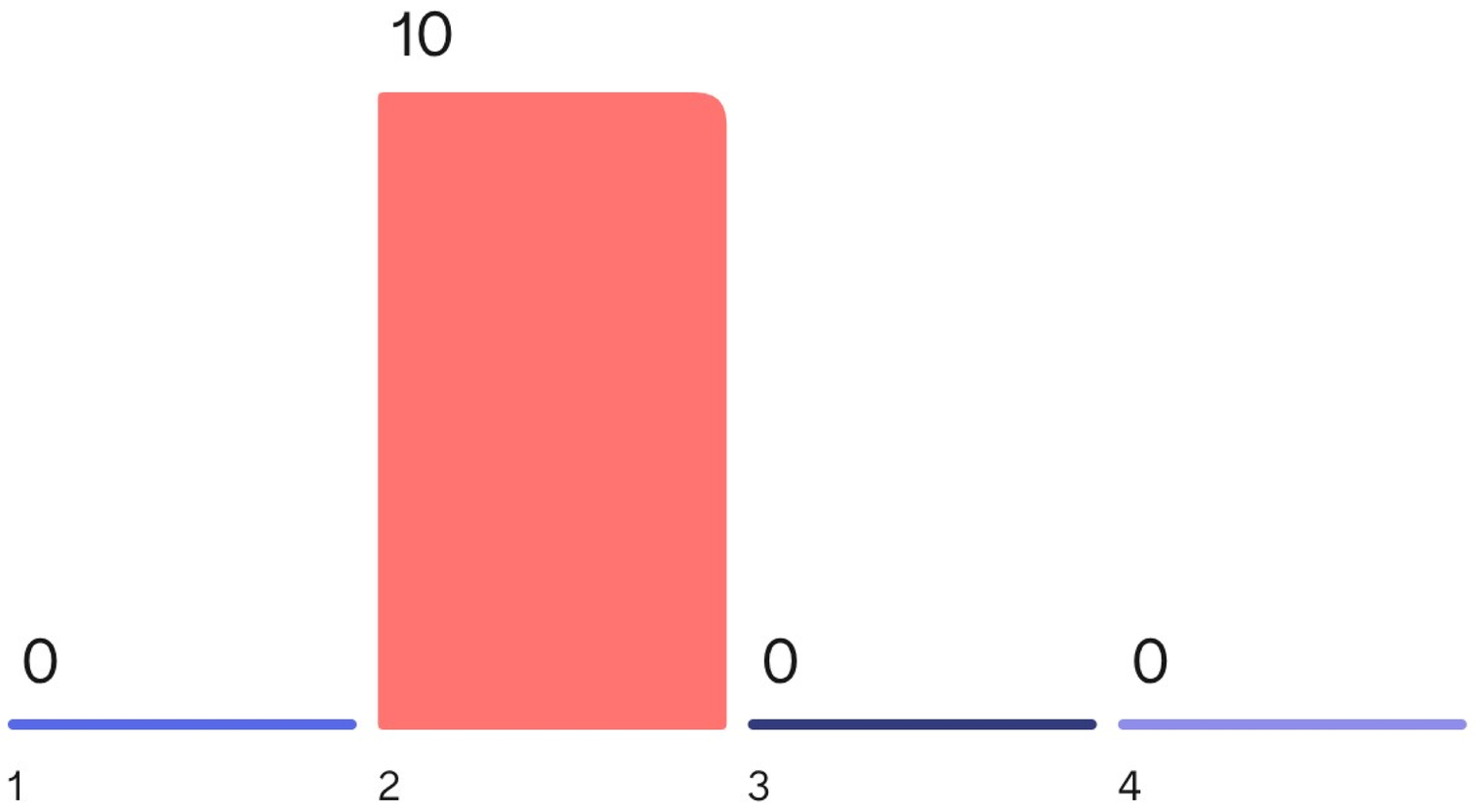
Sertifikater og PKI



Mentimeter

Hvilke påstander om symmetrisk kryptering er sanne og hvilke er usanne?

	Usant	Sant
Kan brukes for å sikre uavviselighet.	○	○
Benyttes til såkalt digital signatur.	○	○
Kan brukes for å sikre konfidensialitet for data.	○	○
Baserer seg på bruk av et nøkkelpar bestående av en privat og en offentlig kryptografisk nøkkel.	○	○
Symmetrisk kryptering ødelegger meldingen slik at den aldri kan dekrypteres	○	○
Benyttes til kryptering av hemmelige meldinger.	○	○
Trygg utveksling av den hemmelige kryptografiske nøkkelen er en sikkerhetsutfordring.	○	○
Sender og mottager deler én felles, hemmelig kryptografisk nøkkel.	○	○



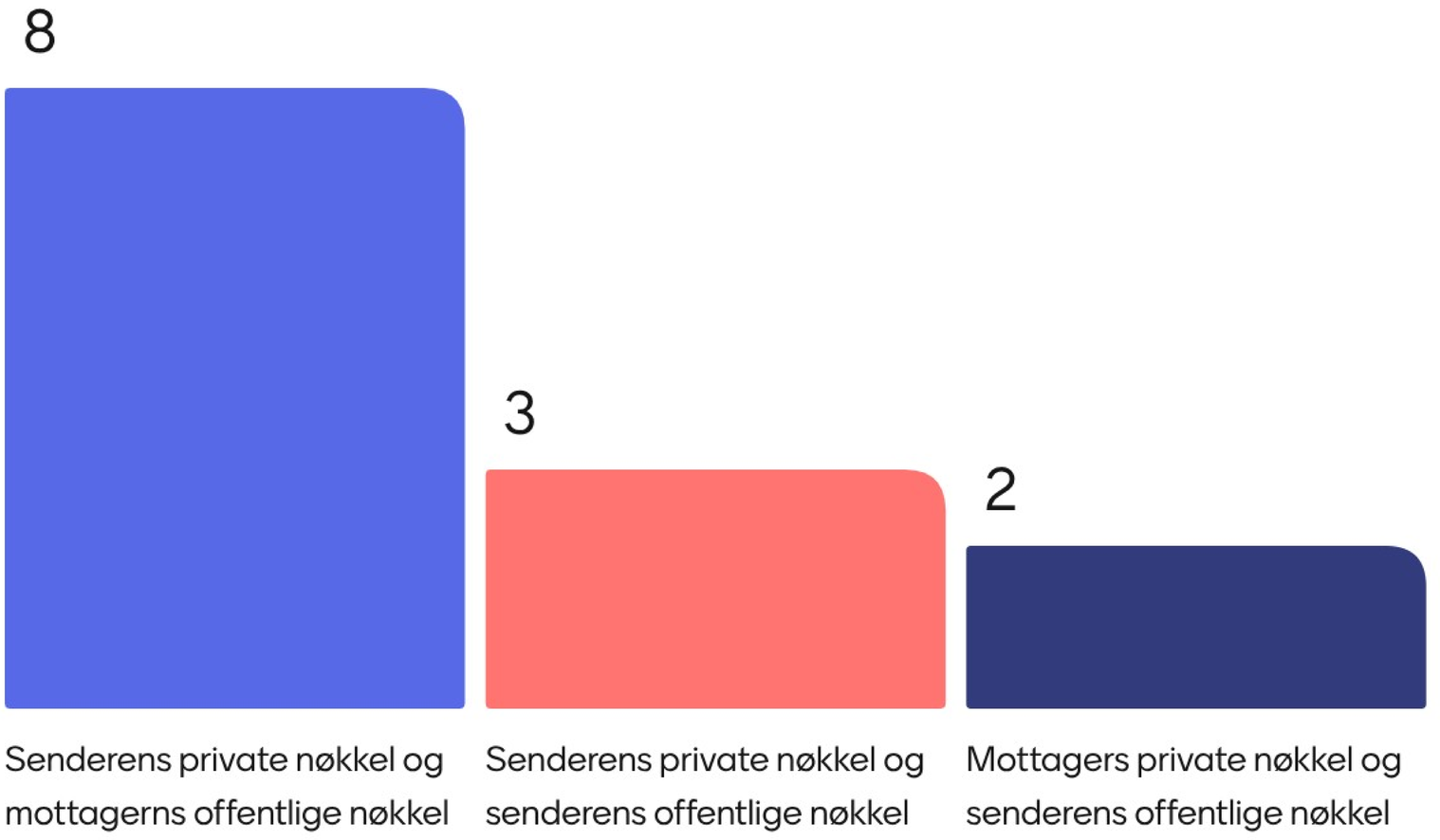
Kryptering: Hash-algoritmer

Anta at en melding har en sjekksum (hash-verdi). På hvilken måte beskytter denne sjekksummen meldingen under overføring i et datanettverk?

Velg et eller flere alternativer

- [ ] En sjekksum gjør det teknisk umulig å endre meldingen underveis i overføringen.
- [ ] Hvis meldingen er endret under overføring vil ikke lenger sjekksummen stemme, og mottager vil dermed vite at meldingen er endret.
- [ ] En hash-algoritme krypterer meldingen slik at kun eieren av nøkkelen kan dekryptere og lese meldingen.
- [ ] En hash-algoritme ødelegger meldingen slik at den ikke kan leses av uvedkommende.

10



b) Hvilke *kryptografiske nøkler* er involvert når *digital signatur* benyttes :
Velg ett eller flere alternativer

- [ ] Senderens offentlige nøkkel.
- [ ] Symmetrisk nøkkel generert av mottager.
- [ ] Mottagers private nøkkel.
- [ ] Symmetrisk nøkkel generert av sender.
- [ ] Senderens private nøkkel.
- [ ] Mottagers offentlige nøkkel.

Mentimeter

Tjenester i internett

1

Mentimeter

Tjenester i internett

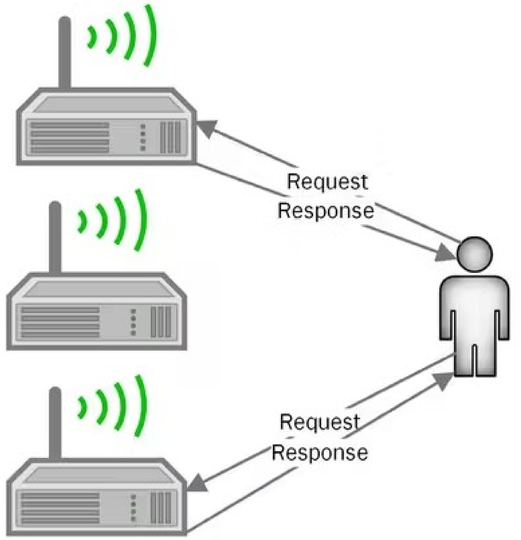
Applikasjonslaget



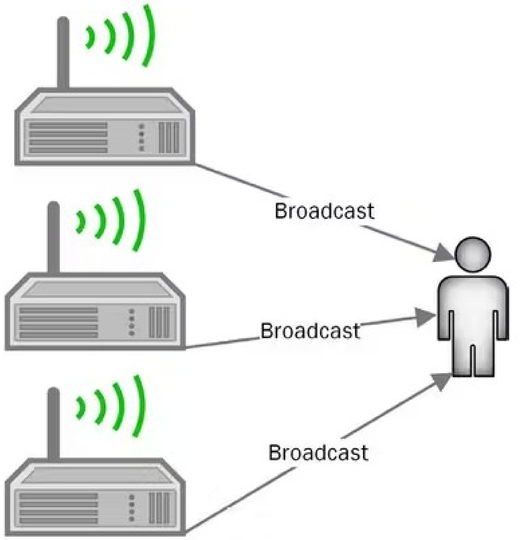
Mentimeter

Aksessmodeller - klient tjener

- Pull
- Push
- Publish-subscribe



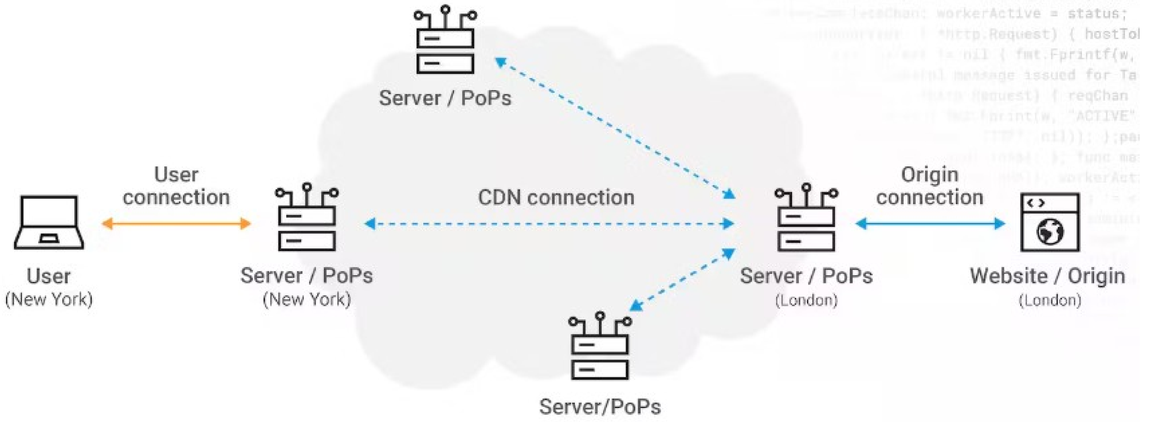
Pull model approach



Push model approach

CDN - content delivery system

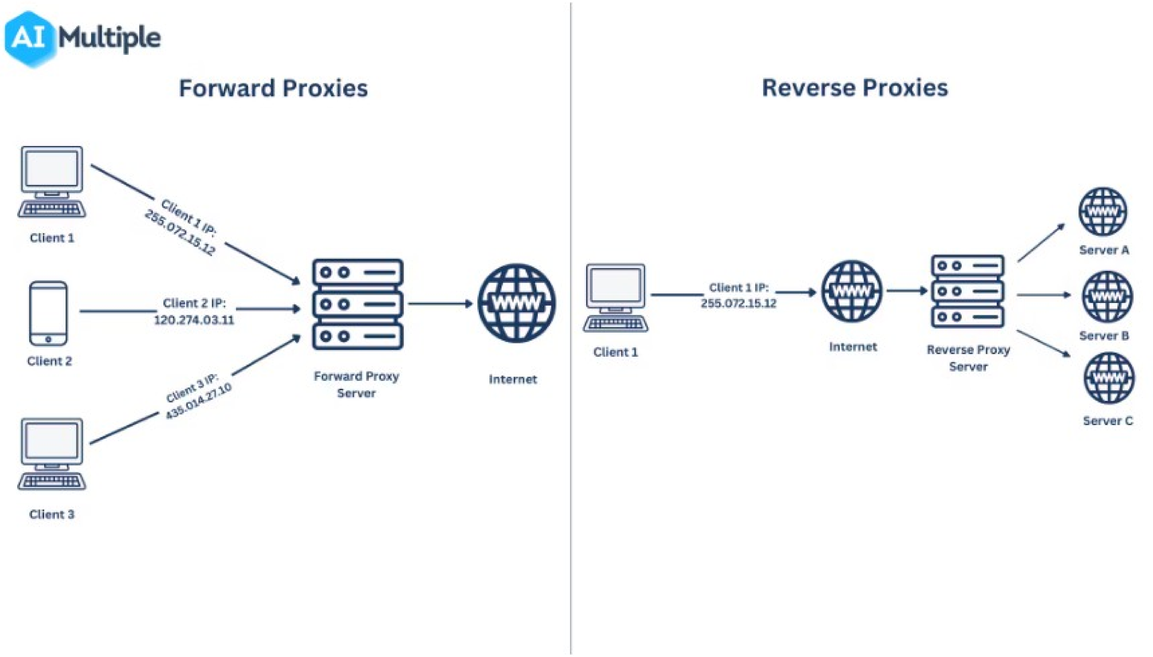
Hvordan lagre innhold nærme brukeren



How a CDN works

Akamai

Proxy


AI Multiple
Forward Proxies
Client 1
Client 2
Client 3
Client 1 IP: 255.072.15.12
Client 2 IP: 120.274.03.11
Client 3 IP: 435.014.27.10
Forward Proxy Server
Internet
Reverse Proxies
Client 1
Client 1 IP: 255.072.15.12
Internet
Reverse Proxy Server
Server A
Server B
Server C

Mentimeter

P2P

-Hver enhet kan både være klient og tjener

-Noe likt som CDN, men med mindre struktur

Fordeler :

-Lett å dele informasjon mellom enheter

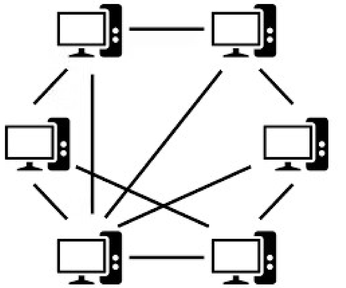
-Kan fordele ressurser

-Ingen kritiske noder

Ulemper:

-Fungerer dårlig for aplikasjoner som trenger lav forsinkelse (f.eks. spill)

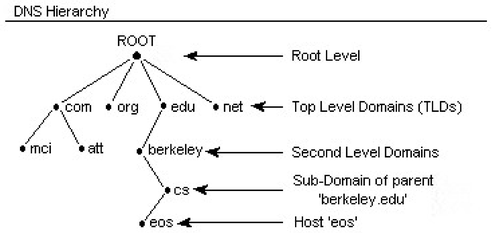
-Ingen sentral styreenhet



DNS

Bruker normale adresser, istedenfor ip

Hierarki i DNS



Mentimeter

HTTP - HyperText Transfer Protocol

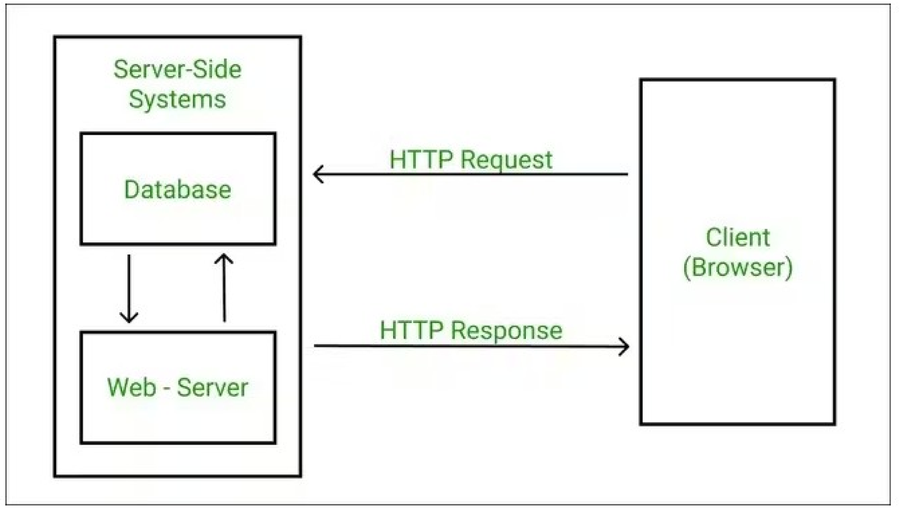
Bruker TCP

Persistente vs ikke-persistente forbindelser

Request og response(f.eks 404 not found)

Cookies, lagrer preferanser

Cache, lagrer midlertidig data

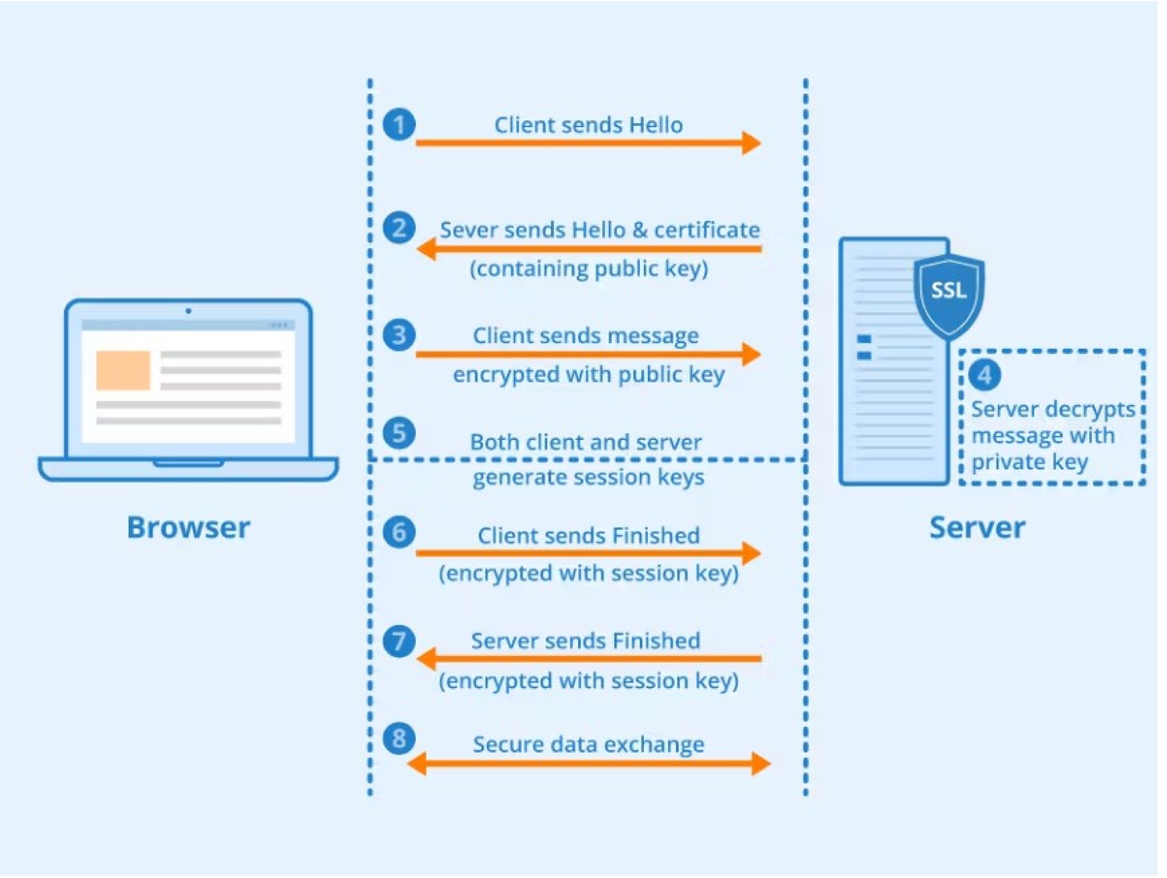


Mentimeter

HTTPS

HyperText Transfer Protocol Secure

Hybrid kryptering, først asymetrisk, så symetrisk



Mentimeter

Videostreaming

UDP eller TCP?

HTTP streaming, klient velger oppløsning

Mentimeter

4.1 Klient-tjener

Hva kjennetegner aksessmodellen klient-tjener?
Velg ett eller flere alternativer

- [ ] En tjener lytter etter henvendelser og leverer tjenester på forespørsel.
- [ ] En klient initierer utvekslingen ved å koble til en tjener og spørre om å få utført en tjeneste.
- [ ] Nodene kan være både klint og tjener samtidig.
- [ ] Mange uavhengige noder samarbeider om å tilby en tjeneste.
- [ ] Det finnes ingen sentralisert kontroll over tjenesten.

Mentimeter

4.9 Content Delivery Network

Hvile av alternativene er positive effekter av Content Delivery Networks?
Velg ett eller flere alternativer

- [ ] Sikrer mot datainnbrudd.
- [ ] Sparer ressurser i kjernenettverket.
- [ ] Flere maskiner fører til økt strømforbruk.
- [ ] Muliggjør bruk av kryptering under overføringen av data.
- [ ] Gjør at nettverket ikke kan kontolleres av en statsmakt eller et selskap.
- [ ] Hindrer overbelastning av tjeneren ved å spre lasten over mange maskiner.
- [ ] Reduserer forsinkelsen for tilgang på innhold ved å flytte det nærmere brukeren fysisk.

Mentimeter

4.9 HTTP-streaming

Hvilke utsagn stemmer om streaming av video over HTTP?
Velg ett eller flere alternativer

- [ ] Video deles opp i små segmenter og forskjellige kvaliteter.
- [ ] Streaming over HTTP bruker kun UDP til overføring.
- [ ] Med HTTP-streaming må man bufre hele videoen før avspilling kan starte.
- [ ] Det er klienten som bestemmer kvaliteten som lastes ned, ikke tjeneren.