gruppe 2

KRYPTOGRAFI

OG TJENESTER I INTERNETT

uke 38



Mentimeter

Plan:)

- Gjennomgang av forrige ukes pensum
- Jobbe med oblig eller ukesoppgaver

Mentimeter

Kryptografi - hvorfor?

- Andre kan lytte inn på data som blir sendt på tvers av nettverk
  - Kan f.eks. gjelde broadcast systemer som WiFi, satellitt, mobilnett
- Informasjonen må derfor krypteres på ett eller flere lag

Mentimeter

Avsender og mottaker på de ulike nivåene

- Applikasjonsnivå (end-to-end): nettleser & webtjener, e-postklient & e-posttjener
- Transport/ IP-nivå: prosesser/porter på vertsmaskiner snakker (TCP/UDP), avsender og mottaker er to endesystemer - klient&server
- Link: Nettverkskort & aksesspunkt - klienten du bruker og WiFi ruter

Flere lag med kryptering gjør lyttingen vanskeligere!

Mentimeter

Tre kategorier av kryptografi

Mentimeter

Symmetrisk

- Hva betyr dette?: Samme nøkkel brukt for kryptering og dekryptering
- Fordel: Raskt og effektivt, perfekt for store datamengder der det er mye trafikk, trygg lagring og sikker informasjon
- Nøkkel må holdes hemmelig og deles sikkert mellom avsender og mottaker
- Algoritme: Blokksiffer, strømchiffer
- Mest brukt: AES
- Mål ivaretatt: Konfidensialitet, integritet, autentisitet
- Utfordring: Sikker utveksling

Mentimeter

Asymmetrisk

- Hva betyr dette?: Et nøkkelpar, en privat og en offentlig
- To grunnfunksjoner:
  - For å sikre konfidensialitet: Avsender krypterer med offentlig nøkkel, mens mottaker kan dekryptere kun med privat nøkkel
    - Mål ivaretatt: Konfidensialitet og integritet
  - Digital signatur: Avsender krypterer med egen privat nøkkel, signatur kan verifiseres ved bruk av offentlig nøkkel av hvem som helst
    - Mål ivaretatt: Autentisitet, uavviselighet

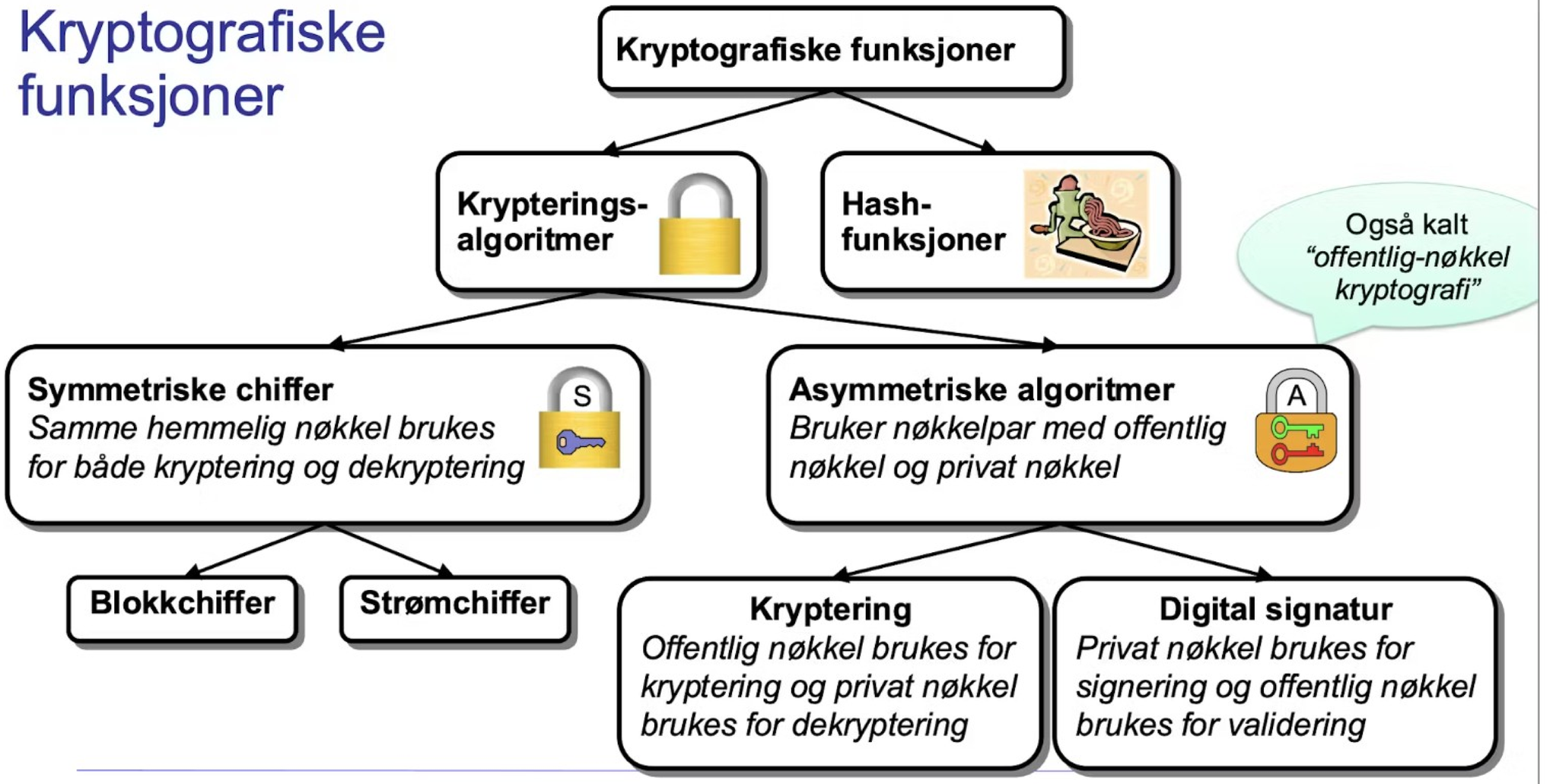
Mentimeter

Hash-funksjoner

- Hva er det?: Funksjon som tar data av hvilken som helst størrelse og gjøre om til en hash-verdi (streng) av fast størrelse.
- Fordel: Umulig å reversere (altså meldingen kan ikke dekrypteres), rask å beregne
- Bruk: Primært for å verifisere integritet
- Mål ivaretatt: Integritet og konfidensialitet

Mentimeter

Kryptografiske funksjoner



Mentimeter

PKI og digitale sertifikater

- Hvordan vet nettleseren at en nettside sin nøkkel faktisk er autentisk?
  - Løsning: PKI + digitale sertifikater

Mentimeter

Digitalt sertifikat (X.509).

- Et elektronisk ID-kort for en nøkkel/eier. Inneholder:
  - Eier/identitet (person/organisasjon/domenenavn)
  - Offentlig nøkkel
  - Gyldighetsperiode (fra–til)
  - Utsteder (CA)
  - Krypto-algo og nøkkelstørrelse
  - Signatur fra CA (binder alt sammen)

Mentimeter

Hva skjer i HTTPS?

- Nettleser kobler til https://
- Server sender sertifikatet sitt
- Nettleser verifiserer: kjede, gyldighet, signaturer, domenenavn
- Hvis godkjent: partene blir enige om en engangsnøkkel (hybrid: asymmetri for nøkkelutveksling også symmetrisk kryptering videre)

Sertifikatet beviser hvem vi snakker med, så blir vi enige om en hemmelig sesjonsnøkkel; resten skjer med symmetrisk kryptering

Mentimeter

Hva med PKI?

- Binder identitet til offentlig nøkkel med en signert bekreftelse (sertifikat)
- Tilrettelegger for autentisering og nøkkeldistribusjon i stor skala (nettleser-PKI).
- Brukes også i BankID/eID (egen PKI) for sterk autentisering og juridisk signering (uavviselighet).

Mentimeter

Tjenester på internett

Proxy cache, CDN, DNS, HTTP/HTTPS, klient-tjener, p2p

Mentimeter

Proxy cache?

- En tjener som står i veien mellom klienter og opprinnelige tjenester, og mellomlagrer (cacher) innhold.
  - Forward
    - Står nær klientene (f.eks. LAN-miljø) og cacher på vegne av brukerne.
    - Mål: mange brukere slipper å hente det samme innholdet fra nettet om og om igjen
  - Reverse
    - står nærme webtjeneren og kan mellomlagre, balansere last og beskytte origin-tjeneren. Klienten tror ofte den snakker direkte med nettstedet, men snakker faktisk med reverse-proxyen.

Mentimeter

CDN - Content Delivery Network

- Hierarkisk nettverk av servere
- Plassert geografisk nært
- Fordel:
  - Raskere
  - Mindre trafikk -> caching nær bruker

Mentimeter

CDN vs. Proxy

- Proxy (forward/reverse) er ofte innenfor en organisasjon eller rundt ett nettsted
- CDN er global infrastruktur driftet av en tredjepart

Mentimeter

DNS: fra navn til IP

- Klienten spør sin rekursive resolver (ofte hos ISP/bedrift)
- Resolveren følger kjeden: root til riktig TLD til riktig autoritativ navnetjener for domenet og får IP tilbake
- Caching: svar lagres i resolverens cache en periode (TTL), slik at neste bruker får svar raskere.