IN1020: Notat sikkerhet uke 4

Om bruk av kryptografi for informasjonssikkerhet

1 Kryptografi

Kryptografi, som bokstavelig talt betyr "hemmelig skrift", er vitenskapen om nettopp hemmelig skrift. En krypteringsalgoritme er en metode for å kryptere informasjon. Kryptografi og krypteringsalgoritmer brukes som et grunnleggende verktøy for å oppnå sikkerhet og tillit i digitale omgivelser, og brukes som teknisk sikkerhetstiltak i alt fra sikker netthandel og nettbank til beskyttelse av personlige data. Hovedformålet er å beskytte data ved å gjøre dem uleselige for uvedkommende, men som vi skal se kan det brukes til å ivareta flere sikkerhetsmål enn konfidensialitet.

Historisk er kryptografi først og fremst brukt for å sende hemmelige meldinger. I dag er kryptografiske algoritmer avgjørende for å sikre data i ulike tilstander: Under lagring, under overføring, og til og med mens de er i bruk.

Det finnes hovedsakelig tre kategorier av kryptografiske algoritmer som er sentrale i moderne datasikkerhet, og som har ulike egenskaper og anvendelsesområder:

- Symmetriske algoritmer (Én hemmelig nøkkel)
- Asymmetriske algoritmer (Privat/offentlig nøkkelpar)
- Hash-funksjoner (kryptografiske enveisfunksjoner)

1.1 Symmetriske krypteringsalgoritmer

Ved symmetrisk kryptering brukes én og samme hemmelige nøkkel for både å kryptere (gjøre data uleselig) og dekryptere (gjøre data leselig igjen). Denne nøkkelen må deles trygt mellom sender og mottaker, og holdes hemmelig for alle andre. Algoritmene kan være enten blokkskiffer (krypterer datablokker, f.eks. 128 bits) eller strømchiffer (krypterer tegn for tegn). Den mest brukte algoritmen i dag er AES (Advanced Encryption Standard).

Nytteverdi og bruksområder. Å kryptere data med bruk av symmetriske algoritmer går svært raskt og effektivt, noe som gjør dette ideelt for kryptering av store datamengder:

- Trygg lagring: Benyttes til å beskytte data som er lagret på usikre medier, som en harddisk på en laptop eller en minnepinne. Her deles ikke nøkkelen med andre, men lagres trygt på enheten.
- Sikker kommunikasjon: Benyttes for å kryptere meldinger og datatrafikk over usikre nettverk som internett. Dette hindrer avlytting. Avsender og mottager må dele en hemmelige krypteringsnøkkel.

Ivaretagelse av sikkerhetsmål:

- Konfidensialitet: Siden de krypterte dataene er uleselige uten kjennskap til den hemmelige nøkkelen, forhindres uautorisert innsyn.

- Integritet: Hvis den krypterte teksten endres, vil dekrypteringen mislykkes eller produsere uforståelige data. Dette gjør at endringer oppdages, og mottaker av kryptert tekst vil vite at data ikke er korrekte.
- Autentisitet (for mottaker): Hvis en mottaker kan dekryptere en melding med den delte nøkkelen, kan vedkommende være rimelig sikker på at meldingen kommer fra den andre parten som har kjennskap til nøkkelen.
- Uavviselighet (Non-repudiation): Dette sikkerhetsmålet ivaretas **ikke**. Siden to entiteter deler den samme hemmelige nøkkelen, kan en tredjepart (f.eks. en dommer) aldri vite hvem av de to som faktisk opprettet en kryptert melding.

Utfordringer: Den største utfordringen med symmetriske kryptering er sikker utveksling av den hemmelige nøkkelen. Hvordan kan sender og mottaker bli enige om og delen en hemmelig nøkkel, uten at en tredjepart snapper den opp?

1.2 Asymmetriske Krypteringsalgoritmer

Asymmetrisk kryptering løser nøkkeldistribusjonsproblemet nevnt over ved å bruke *et nøkkelpar* som består av en *offentlig nøkkel* og en *privat nøkkel*. Disse to nøklene er matematisk knyttet sammen, men den private nøkkelen kan ikke utledes fra den offentlige eller omvendt. Den offentlige nøkkelen kan og skal deles åpent med andre, og det antas at den er *autentisk*. Den private nøkkelen må holdes strengt hemmelig (konfidensiell) av den nøkkelparet tilhører (eieren).

Asymmetrisk kryptering benyttes for to viktige funksjoner innen informasjonssikkerhet:

- **For utveksling av hemmelig melding:** En avsender krypterer en melding med bruk av **mottakerens offentlige nøkkel**. Den eneste nøkkelen som kan dekryptere denne meldingen er **mottakerens private nøkkel**. Og siden kun mottakeren har tilgang til og kjenner denne private nøkkelen, sikres **konfidensialitet** til meldingen.
- **For digital signatur**: Prosessen for digital signatur er rett og slett motsatt av utveksling av hemmelig melding. En avsender signereren melding ved å kryptere meldingen (eller en generert hashverdi av meldingen) med sin egen, altså **avsenders private nøkkel**. Hvem som helst kan deretter verifisere signaturen ved å bruke **avsenderens offentlige nøkkel**, som jo er almenn kjent. Siden kun avsenderen kjenner og har tilgang til sin private nøkkel, beviser dette at meldingen kom fra vedkommende (autentisk opphav) og avsender kan heller ikke nekte for å ha signert (uavviselighet).

Nytteverdi og bruksområder: Asymmetrisk kryptering er ressurskrevende og tregere enn symmetrisk kryptering. Den brukes derfor vanligvis ikke for store datamengder, men for operasjoner der *sterk autentisering* og *sikker nøkkelforvaltning* er viktig.

- Digitale signaturer: Gir en juridisk bindende måte å signere avtaler digitalt, og sikrer dermed uavviselighet. BankID bruker f.eks denne teknikken for digital signering.
- Autentisering: Verifiserer identiteten til personer, organisasjoner og systemer. Eksempel: Når et nettsted presenterer et *digitalt sertifikat*, bevises nettstedets identitet/tilhørighet.
- Sikker nøkkelutveksling: Treg asymmetrisk kryptering brukes til å trygt utveksle en engangs symmetrisk nøkkel (også kalt sesjonsnøkkel). Deretter brukes symmetrisk kryptering

med den symmetriske engangsnøkkelen for selve kommunikasjonen. Dette kalles en hybrid-modell. HTTPS, protokollen for trygg kommunikasjon mellom en nettleser og et nettsted, er et klassisk eksempel på en slik hybrid modell i bruk.

Utfordringer: Hvordan kan man stole på at en offentlig nøkkel faktisk tilhører den den utgir seg for å tilhøre? Dette løses med digitale sertifikater og en *Offentlig Nøkkelinfrastruktur (PKI)*, der en betrodd tredjepart (sertifikatmyndighet) går god for koblingen mellom en identitet og en offentlig nøkkel.

1.3 Hash-funksjoner

En hash-funksjon er en enveisfunksjon som tar en datamengde av vilkårlig størrelse (f.eks. en fil eller et passord) og produserer en streng av fast størrelse, kalt en *hash-verdi* eller *sjekksum*, eller forkortet til bare *hash*. Funksjonen er designet slik at:

- Det er enkelt å beregne hashen fra dataene.
- Det er praktisk umulig å gå tilbake fra hashen til de opprinnelige dataene (som å lage frukt fra en smoothie).
- Enhver liten endring i dataene vil resultere i en helt annerledes hash.
- Det skal være ekstremt vanskelig å finne to ulike datasett som gir samme hash-verdi (*kollisjonsresistens*).

Nytteverdi og bruksområder: Hash-funksjoner brukes primært for å *verifisere integritet*.

- Integritetssjekk av filer: Når du laster ned programvare, publiseres ofte en hash-verdi sammen med filen. Du kan da beregne hashen av filen du lastet ned og sammenligne den med den publiserte verdien for å sikre at filen ikke er endret eller korrupt.
- Lagring av passord: Passord lagres aldri i klartekst i databaser. I stedet lagres en *hash* av passordet, ofte med et tilfeldig *salt* (tilfeldig tall) for å gjøre hash-verdien unik, i de tilfellene flere har nøyaktig samme passord. Når du logger inn, hashes passordet du skriver inn og sammenlignes med den lagrede hashen. Dette ivaretar passordets konfidensialitet ved en eventuell datalekkasje.
- Del av digitale signaturer: For å unngå å signere (kryptere) store dokumenter, lages det en hash av dokumentet, og det er denne mye mindre hashen som signeres med avsenderens private nøkkel.

Sikkerhetsmål som ivaretas:

- Integritet: Hovedformålet er å sikre at data er uendret.
- Konfidensialitet (for passord): Beskytter selve passordet fra å bli lest i klartekst fra en database.
- Hash-funksjoner gir i seg selv verken autentisitet eller uavviselighet.

2 Offentlig-nøkkelinfrastruktur (PKI) og digitale sertifikater

Asymmetrisk (offentlig-nøkkel) kryptering er en anvendbar teknologi, men den har en fundamental utfordring: Hvordan kan man stole på at en offentlig nøkkel er autentisk? Hvem som helst kan i prinsippet generere et nøkkelpar og hevde at den offentlige nøkkelen tilhører en bestemt entitet (person, bank, organisasjon el). Uten en pålitelig mekanisme for å verifisere eierskapet til en offentlig nøkkel, kan uvedkommende lure oss til å kryptere sensitiv informasjon med en falsk nøkkel, eller stole på en falsk digital signatur.

Dette er den sentrale problemstillingen som *digitale sertifikater* og *offentlig-nøkkelinfrastruktur (PKI)* er designet for å løse. De er nøkkelen til å etablere digital tillit mellom ulike aktører.

2.1 Digitale sertifikater

Et digitalt sertifikat er et elektronisk dokument som løser tillitsproblemet ved å knytte en identitet (f.eks. en person eller organisasjon) sammen med en tilhørende offentlig nøkkel. For å sikre at denne koblingen er troverdig, blir sertifikatet utstedt og digitalt signert av *en betrodd tredjepart*.

Et sertifikat består av den offentlige nøkkelen samt en rekke attributter (data) knyttet til nøkkelen, som hvem som eier nøkkelen (unik id/navn på person eller organisasjon), gyldighetsperiode for sertfikat med nøkkel, og hvem som har utstedt sertifikatet. Dataene pakkes sammen og signeres digitalt av utstederen. Det finnes standarder, som X.509, som definerer hva et sertifikat skal inneholde.

2.2 Offentlig-nøkkelinfrastruktur

En offentlig-nøkkelinfrastruktur (public key infrastructure, forkortet PKI) er et rammeverk for utstedelse, administrasjon og bruk av digitale sertifikater. Hovedformålet med en slik infrastruktur er å sikre ektheten til offentlige nøkler samt sørge for en trygg og forsvarlig distribusjon av dem. Rammeverket må bestå av flere bestanddeler, f.eks. retningslinjer for hvordan sertifikater skal håndteres, teknologi (f.eks. programvare) for å implementere retningslinjene, klare prosedyrer for hvordan nøkler skal håndteres og forvaltes, samt en *tillitsmodell* for sertifikatene, som ofte er hierakisk.

Offentlig-nøkkelinfrastruktur med sertifikater som er basert på asymmetrisk kryptering med nøkkelpar bestående av privat og offentlig nøkkel, er i dag nødvendige for å kunne løse de mest sentrale sikkerhetsutfordringene på internett. Uten dette ville sikker digital samhandling i stor skala vært umulig. Med bruk av slike PKIer muliggjøres trygg kommunikasjon over utrygge nettverk, samt en rekke kritiske tjenester vi tar for gitt i dag:

- Sikker netthandel og nettbank (HTTPS): Når du besøker en nettside som skatteetaten.no, sender serveren sitt sertifikat med sin offentlige nøkkel til nettleseren din. Nettleseren verifiserer sertifikatet mot sin liste av klarerte sertifikater for å bekrefte at du kommuniserer med den ekte Skatteetaten, og ikke en falsk side laget for å stjele informasjonen din. Dette er grunnlaget for Internett-PKI.

- Elektronisk ID og autentisering: Tjenester som BankID er bygget på egne interne PKI-er. BankID gir hver bruker et sertifikat som fungerer som en sikker elektronisk identitet for autentisering og digital signering. Dette gir et så høyt sikkerhetsnivå at banken kan stole på at det faktisk er deg som logger inn når du benytter og får verifisert din tildelte private nøkkel.

- Digital signatur og uavviselighet: Asymmetrisk kryptering brukt for digital signatur, som er muliggjort gjennom bruk av PKI, støtter uavviselighet (non-repudiation). Når du signerer et dokument med BankID f.eks, brukes din private nøkkel. Siden kun du har denne nøkkelen, kan en tredjepart (f.eks. en domstol) verifisere signaturen med din offentlige nøkkel og

bekrefte at det var du som signerte. Du kan ikke senere nekte for å ha signert avtalen, isåfall må du argumentere med at uvedkommende har fått tilgang til og benyttet din BankID.

- Sikker kommunikasjon mellom systemer: PKI brukes også til å sikre at systemer, for eksempel en mobiltelefon som laster ned en sikkerhetsoppdatering, kommuniserer med den ekte serveren til produsenten (f.eks. Apple eller Samsung) og ikke en falsk tjeneste som distribuerer skadevare.

- Sikre sektorspesifikke tjenester: Bruk av PKI er også grunnlaget for sikker kommunikasjon i kritiske sektorer som helsevesenet, for eksempel for e-resepter og elektroniske sykemeldinger, og forsvaret.

For å unngå at vi må stole på millioner av individuelle sertifikater for store PKI-er som f.eks. Internett-PKI, er systemet bygget på tillit til et fåtall aktører kjent som *sertifikatmyndigheter* (Certificate Authorities - CA). Dette er betrodde virksomheter som utsteder sertifikater og går god for at nøklene i sertifikatene de utsteder er autentiske. Nettlesere og operativsystemer kommer med en forhåndsinstallert liste over klarerte CA-er, og bruker denne listen til å verifisere sertifikatene de mottar fra for eksempel nettsider.

3 Oppsummering

Kryptografi er rett og slett en verdifull oppfinnelse også for digital informasjonssikkerhet. Ved å kombinere de ulike algoritmene, som i hybridmodeller (f.eks. HTTPS), klarer vi å bygge robuste og trygge digitale tjenester. Symmetriske krypteringsalgoritmer er effektive og kan sørge for konfidensialitet for store datamengder, asymmetrisk kryptering løser utfordringen med nøkkeldistribusjon og gir grunnlag for sterk autentisering og uavviselighet, mens hash-funksjoner er svært nyttige i å sikre dataintegritet. Sammen danner de grunnlaget for nødvendig tillit til alt fra nettbank-transaksjoner til sikker lagring av digitale verdier.

Uten offentlig-nøkkelinfrastruktu og sertifikater ville vi hatt vaskeligheter med å verifisere identiteter til en rekke ulike entiteter i digital samhandling. Infrastrukturen er nødvendig for å bygge et fundament av tillit, og den gir oss de tekniske mekanismene (som HTTPS og digital signatur) vi trenger for å ivareta sentrale sikkerhetsmål som autentisitet, konfidensialitet, integritet og uavviselighet.