

Kryptering

REV2403
2006

Nonsenstotaler

- MD5 Message digest nr 5
 - en avstemming
 - enkel å sammenligne for mennesker
 - dataverdier og posisjon påvirker summen
 - ikke teoretisk umulig men vanskelig å lage kompenserende endringer for å lure kontrollen
- Liten endring i tekst gir stor endring i totalen (summen)
- sal.bi.no/md5

Symmetrisk kryptering

- En felles nøkkel avtales mellom sender og mottager
- $X=D(M,N)$ og $M=D(X,N)$
 - eks. DES
- Fordeler
 - rask kryptering og dekryptering
- Ulemper
 - Mange nøkler nødvendig hvis flere parter

Assymmetrisk kryptering

- Hver deltager har to nøkler
 - privat nøkkel N_p som bare er kjent av eieren
 - offentlig nøkkel N_o som er kjent av alle
- $X=D(M,N_p)$ $M=D(X,N_o)$ integritet
- $X=D(M,N_o)$ $M=D(X,N_p)$ konfidensialitet
- Fordeler
 - kun to nøkler hos hver deltager
- Ulemper
 - krypteringstid

Sertifikater

- Distribusjon av nøkler
 - Sertifikatsteder krypterer din off nkl med sin private nkl
 - Du kan kopiere og videregjøre din off nkl, sertifikatet
 - mottager kan trygt dekode din off nkl ved hjelp av sertifikatstederens off nkl

Eksempel på meldingssikring

- Ta MD5-sum av meldingen
- Krypter summen med din private eller mottagers off nkl, summen kalles da digital signatur
- Send signaturen sammen med meldingen
- Mottageren gjentar MD5-beregningen og sammenligner med dekodert signatur

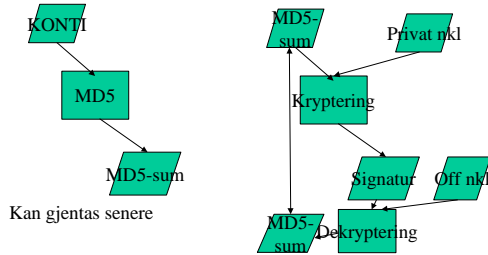
Lov om elektronisk signatur (§3)

- **elektronisk signatur:** data i elektronisk form knyttet til andre elektroniske data og som brukes som autentiseringsmetode.
 - er enydig knyttet til undertegneren,
 - kan identifisere undertegneren,
 - er laget ved hjelp av midler som bare undertegneren har kontroll over
 - er knyttet til andre elektroniske data på en slik måte at det kan oppdages om disse har blitt endret etter signering.
- **avansert elektronisk signatur:** elektronisk signatur som
 - er enydig knyttet til undertegneren,
 - kan identifisere undertegneren,
 - er laget ved hjelp av midler som bare undertegneren har kontroll over
 - er knyttet til andre elektroniske data på en slik måte at det kan oppdages om disse har blitt endret etter signering.
- **kvalifisert elektronisk signatur:** avansert elektronisk signatur basert på et kvalifisert sertifikat og fremstilt av et godkjent sikkert signaturfremstillingssystem,

Lov om elektronisk signatur (§3)

- **undertegner:** den som disponerer et signaturfremstillingssystem og som handler på vegne av seg selv eller på vegne av en annen fysisk eller juridisk person,
- **signaturfremstillingssdata:** unike data, som for eksempel koder eller private nøkler, som undertegneren benytter for å fremstille en elektronisk signatur,
- **signaturfremstillingssystem:** programvare eller maskinvare som benyttes til å fremstille elektronisk signatur ved hjelp av signaturfremstillingssdata
- **signaturverifikasjonsdata:** unike data, som for eksempel koder eller offentlige nøkler, som benyttes til å verifisere en elektronisk signatur
- **signaturverifikasjonssystem:** programvare eller maskinvare som benyttes for å verifisere elektronisk signatur ved hjelp av signaturverifikasjonsdata
- **sertifikat:** kobling mellom signaturverifikasjonsdata og undertegner som bekrefter undertegners identitet og er signert av sertifikatsteder
- **sertifikatsteder:** fysisk eller juridisk person som utsteder sertifikater eller tilbyr andre tjenester relatert til elektronisk signatur

Signering av en hel tabell: KONTI



Signering av hver linje i KONTI

| | Std Avdkode | Klasse A/E/G/I/K | Resk-kode | SA-nr | RS-nr | Endret dato | Elektronisk Signatur |
|---------------------|-------------|------------------|-----------|-------|-------|-------------|----------------------|
| Kttonavn | | | | | | | |
| Kunder | 0 A | P | | | | 20060110 | IA3201103F77C |
| Kasse | 0 A | N | | | | 20060110 | |
| Leverandører | 0 G | J | | | | 20060110 | |
| Mva Høy sats | 0 G | N | | | | 20060110 | |
| Salg avgpt høy sats | 1 I | N | | | | 20060110 | |

1. MD5-sum av cellene som skal signeres
2. Kryptering med privat nøkkel

Signering i POSTER

- Brukerident for den som har registrert
- Regnskapsperiode
- Avansert signatur for den som har
 - registrert
 - foretatt regnskapsavslutning med posten
 - revidert posten

Signering av hele regnskapet (jf Altinn)

