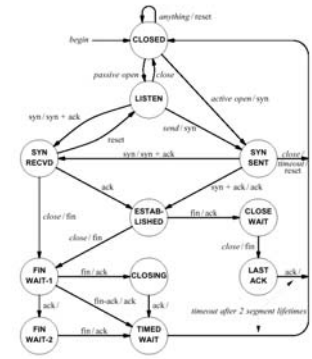
11174 Datasikkerhet
Høsten 2002

Et forsøk på oppsummering

TCP/IP



Fundamenter

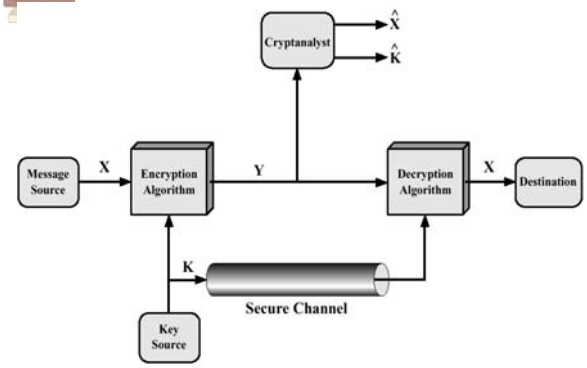
Trusler

- Kommunikasjonsbrudd
- Avlytting
- Endring av informasjon
- Fabrikering/forfalskning

Sikkerhetstjenester

- Konfidensialitet
- Autentisering
- Integritet
- Ikke-fornektelse
- Aksesskontroll
- Tilgjengelighet

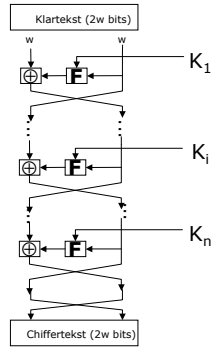
Konvensjonell krypteringsmodell



Enkle chiffer

- Substitusjon
  - Monoalfabetisk
  - Polyalfabetisk
  - One-time pad
- Permutasjon

Klassisk (n-round) Feistel nettverk



Populære blokkchiffer

	Nøkkel	Blokk	Runder	Internt	Spesial
3-DES	112 (168)	64	48	32	EDE
IDEA	128	64	8	16	Ikke Feistel
Blowfish	32-448	64	16	32	Nøkkelavh. S-boks
RC5	0-255*8	32-128	0-255	Var.	Ikke Feistel
CAST-128	40-128	64	16	32	Rundeavh. operatorer

Karakteristikker

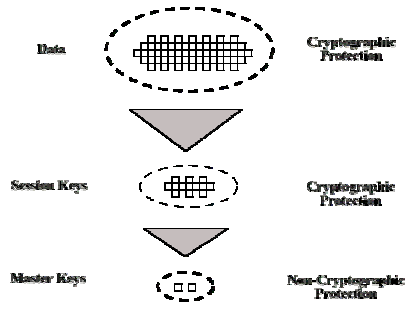
Følgende karakteristikker gjelder i større eller mindre grad for moderne blokkchifre:

- Variabel nøkkellengde
- Flere primitive operatorer
- Data-avhengig rotasjon
- Nøkkel-avhengig rotasjon
- Nøkkel-avhengige S-bokser

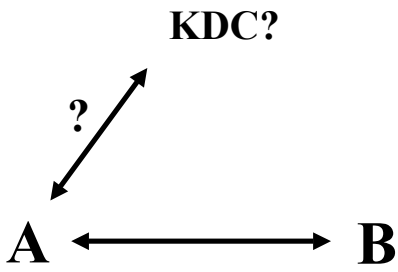
Karakteristikker, forts.

- Lang ”key schedule” algoritme
- Variabel F-funksjon
- Variabel blokklengde
- Variabelt antall runder
- Operasjon på begge halvpartene av data i hver runde

Nøkkelhierarki



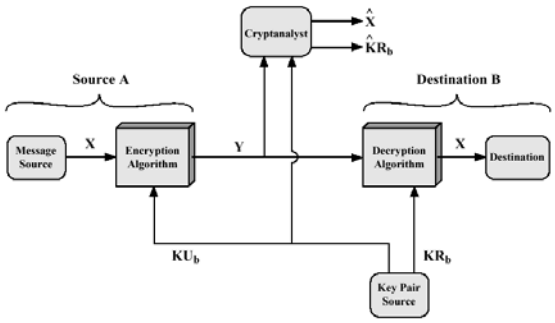
Nøkkeldistribusjon



Tallteori

1. Tall, primtall, og relativt primiske tall
2. Modulær aritmetikk
3. Euclids algoritme
4. Primalitetstesting
5. Diskrete logaritmer

Offentlig-nøkkel konfidensialitet



Offentlig-nøkkel algoritmer

- RSA
- Diffie-Hellman
- (ElGamal)

RSA

- Velg to store primtall p,q
- $n = p \cdot q$
- $\phi(n) = (p-1)(q-1)$
- Velg e slik at $\gcd(\phi(n),e)=1, 1<e<\phi(n)$
- $d = e^{-1} \bmod \phi(n)$
  $(d \cdot e \equiv 1 \bmod \phi(n))$
- Offentlig nøkkel: KU={e,n}
- Privat nøkkel: KR={d,n}

Diffie-Hellman

- q - primtall
- α - $\alpha < q$, α primitiv rot av q
- Bruker A
  - Velg X_A $X_A<q$
  - Beregn $Y_A=\alpha^{X_A} \bmod q$
- Bruker B
  - Velg X_B $X_B<q$
  - Beregn $Y_B= \alpha^{X_B} \bmod q$
- Nøkkel $k = Y_B^{X_A} \bmod q$

  $= \alpha^{X_B X_A} \bmod q = Y_A^{X_B} \bmod q$

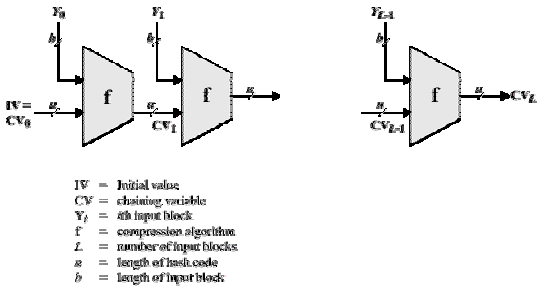
Meldingsautentiseringskode

- Genererer en blokk av data av fast lengde fra en melding av variabel lengde og en hemmelig (symmetrisk) nøkkel K
- ”Kryptografisk sjekksum”
- MAC = $C_K(M)$

Hash-funksjoner

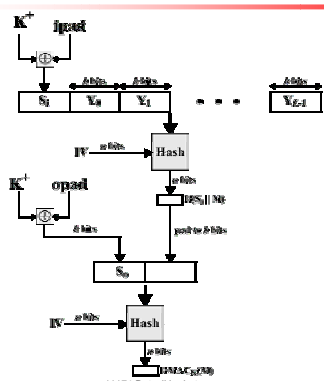
- Tar en melding av variabel lengde, og generer en *hash* av fast lengde
- En hash kalles også ”message digest”
- h=H(M)
- Enveis-funksjon: ”Umulig” å finne en **M’** som genererer en gitt **h**
- Hash-funksjonen er ikke hemmelig, så hashen må beskyttes på andre måter

Modell for hash-funksjoner

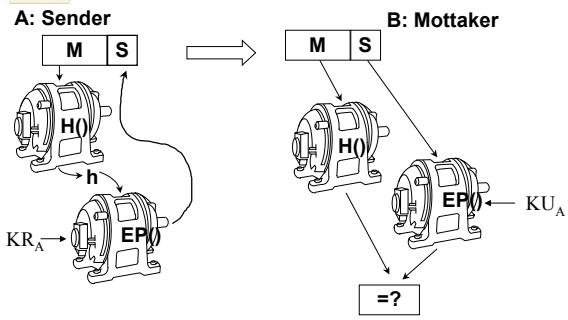


IV = Initial value
CV = chaining variable
Y_i = ith input block
f = compression algorithm
L = number of input blocks
n = length of hash code
b = length of input block

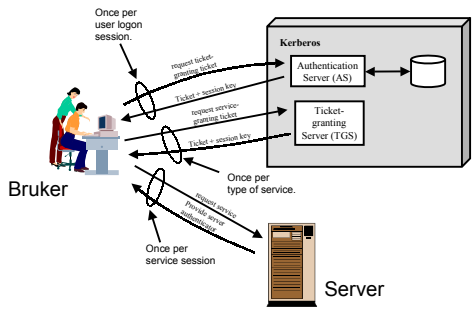
HMAC



RSA Digitale signaturer eksempel



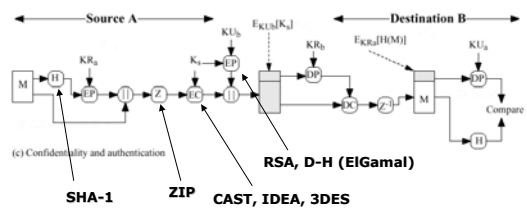
Kerberos



X.509

- Standard for sertifikater for offentlige nøkler
- Del av OSIs katalogtjeneste (X.500)
- Brukes i S/MIME, IPsec, SSL/TLS og SET

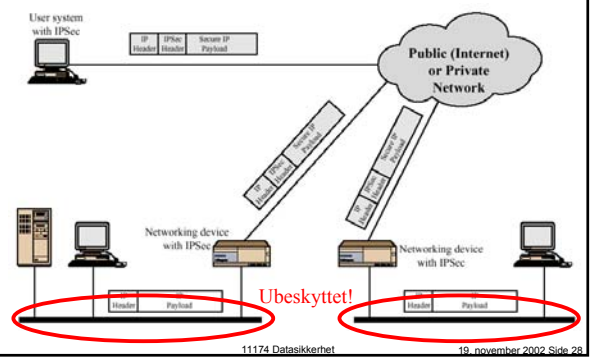
PGP autentisering & konfidensialitet



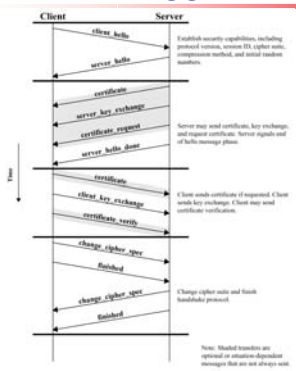
S/MIME

- Introduserer mulighet for å sende krypterte/autentiserte meldinger i det eksisterende MIME-rammeverket
- Baserer seg i større grad på bruk av CA og X.509-sertifikater

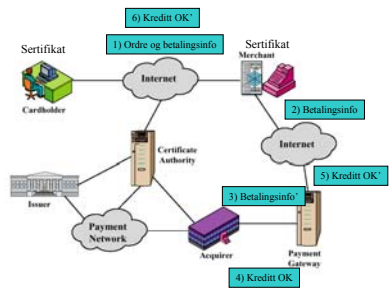
IP-sikkerhet scenario



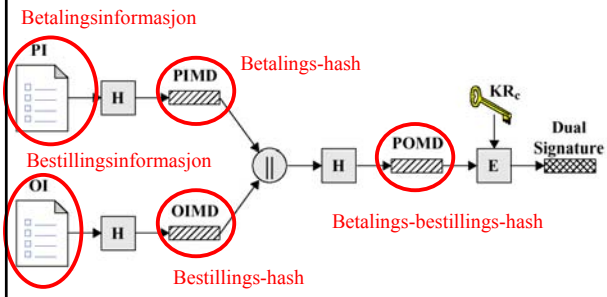
SSL



Deltakere i SET



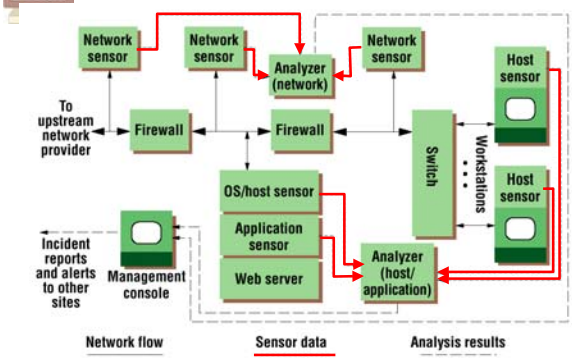
Generering av dobbel signatur



Inntrengere og virus

- Angrep
- Passord i Unix
- IDS
- Virus - angrep og deteksjon/motmidler

Et IDS-beskyttet nettverk



Brannmurteknologier

- Pakkefilter
  - Header / Application inspeksjon
  - Tilstandsbasert / dynamisk filtrering
  - Bufferstrategi
- Network Address Translation
- Proxy
  - Generisk/Dedikert
  - Transparent

Pakkefilter