1 Cryptografi, confidentiality

- Introduction
- Unconditionally and computationally secure
- Practical systems - exchaustive key search
  - $c = E_K(m, n)$
- Secret key - Stream Cipher / block cipher
  - SNOW, SALSA20
  - OFC, Counter, CBC
- Public key - RSA / OAEP

2 Cryptography, authentication

- Intruduction
- Unconditional and computational secure
- Practical systems - exchaustive key search
- Secret key
  - CBC MAC
  - HMAC
    - SHA1(m||K)
- Public key systems
  - RSA
- Forskelle på secret og public key systems
- Hashing
  - 4 egenskaber
- Replay

3 Key management and Infrastructures

- Two party communication
- Key Distribution center KDC
- Certificate Authoraties CA

  - Hvad er CA? Forskel fra KDC? Chaining? x.509
- Password
  - 4 slags angreb vi skal beskytte os imod
- Hardware
  - Tamper evident / two factor authentication
  - Tamper resistent hardware
- Biometric
- Preventing bypassing of the system
  - h(pw)=SHA1(SHA1(SHA1...(pw) ...)

4 Network Security

- Introduction
- Authenticated public key exchange
- SSL
  - Mellem application og TCP/IP level
  - Client, Server
  - Onesided
- SSL Protocol
  - Record protcol
  - Handshake protocol
  - Cipher spec change protocal, Alert Protocol
- SSL key exchange
  - ikke perfectly forward shafe som deffie hellman
- Password-authenticated key exchange
  - Ikke alle har certificate
  - One-way SSL plus passwrod
  - password er elendig til formålet
  - SRP
- IPSec
  - TCP/IP plan

- Deffie Hellman Key exchange
- Sammenligning af SSL og IPSec
  - IPSec, crypteres det for alle på TCP/IP plan, men kan ikke styres når det data når det først er pakket ud på modtager computeren
  - SSL, kræver applicationer der understøtter det, så besværligt, men kan styre data'en indtil den er pakket ud på applications plan