Anonüümsus ja privaatsus

- Privaatsus – võimalus omaette olla
- Anonüümsus – võimalus oma identiteeti varjata
- Interneti leviku tõttu on personaalne info hakanud laialdasemalt ja kiiremini levima
- 1994: "In Internet, nobody knows you are a dog"
- 2010: jah, kollane krants viltuse katusega kuudist
- Kelle huvides on jälgimine ja identifitseerimine?
- Isikuandmete äri on tulus

Kuidas enda privaatsust parandada?

- Ära jaga oma personaalset informatsiooni
- Mitu meiliaadressi – üks päris ja muud vahetuvad
- Ära usalda vastseid tuttavaid liiga palju
- Hoia oma privaatne info oma arvutis
- Kaitse oma isiklikku arvutit
- Ettevaatust saitide eest, mis pakuvad personaalse info eest auhindu jms
- Ära vasta spämmeritele
- Ole kursis veebiturbega (http vs https jms)
- Uuri privaatsuspoliitikaid enne info andmist (P3P, . . .)
- Kasuta krüptot ja vajadusel anonümiseerijaid

Meili anonümiseerijad

- Pseudo-anonümiseerijad
  - Edasi-tagasi kanal
  - Serveri haldaja teab, kes on kes
  - Julf Helsingius ja anon.penet.fi
- Päris anonümiseerijad
  - Ühesuunaline kanal
  - Terve võrk vahendajaid, kiri läbib neist mitut
  - Mitu kihti krüptimist (*onion routing* – sibul)
  - Serverite administraatorid ei tea, kellega tegu
  - Kahte sorti: Cypherpunks ja Mixmaster
  - Cypherpunks: PGP baasil
  - Mixmaster: oma võtmed (RSA+3DES), fikseeritud suurus, ümber järjestamine

Varia

- Krüptopoliitika: valitsuse huvid, USA, Prantsusmaa, Venemaa, Wassenaar;
- Steganograafia ja selle matemaatilisus
- Tarkvara patendid, pöördkodeerimine, fair use
- Kopeerimiskaitsed, DMCA (Corley, Johansen/DeCSS, Sklyarov), DRM, CPRM, SDMI (Felten)
- Tempest