Steganografia

- Tiedon kätkeminen
- Halutaan salata paitsi sanoman sisältö myös sen olemassaolo. Syitä:
  - vakoilutietojen salakuljetus
  - valvonnan kiertäminen (vartija Walter)
  - salakirjoitus kielletty
- Halutaan liittää dokumenttiin tietoa, jota ei saa siitä pois. Syitä:
  - alkuperämerkintä (copyright)
  - levityksen valvonta, numeroidut kappaleet
- Teoreettisesti vahvat menetelmät kätkevät pienen määrän dataa suurella vaivalla.

  Heikot menetelmät perustuvat siihen, ettei kätketyn tiedon olemassaoloa epäillä.

Subliminaalinen kanava

- Moniin allekirjoituksiin voidaan kätkeä tietoa.
- Vaarat:
  - sanoman sisällön valvominen on mahdotonta
  - allekirjoituksen mukana saattaa vuotaa tietoa salausavaimesta.
- Esim. ElGamalissa pitäisi valita jokaista sanomaa kohti satunnainen k. Valitaan $k =$ kätkettävä sanoma.

  Kaikki, jotka tuntevat salaisen avaimen, pystyvät laskemaan k:n.

Kätkeminen ElGamalissa

- **Avaimet**: Valitaan alkuluku p ja kaksi satunnaista lukua g ja x.

  $$y = g^x \bmod p.$$

  Alicen julkinen avain on (y, g, p), salainen x.

  Alice kertoo salaisen avaimen Bobille.
- **Alicen allekirjoitus:** Alice on allekirjoittavinaan sanoman M, mutta oikeasti kätkee sanoman k. (Pitää olla $\gcd(k, p-1) = 1$.) Alice laskee

  $$a = g^k \bmod p$$

  ja ratkaisee seuraavasta yhtälöstä b:n

  $$M = (xa + kb) \bmod (p-1).$$

  Allekirjoitus on lukupari (a, b).
- **Walter tarkistaa allekirjoituksen:**

  $$y^a a^b \bmod p \stackrel{?}{=} g^M \bmod p.$$
- **Bob avaa kätketyn sanoman:**

  $$k = (b^{-1}(M - x\,a)) \bmod (p-1).$$
- Osa k:n biteistä voidaan valita satunnaisesti, jolloin allekirjoituskin on luotettava.

ElGamal-esimerkki

- Alkuluku $p = 167$ ja satunnaisluvut $g = 163$, $x = 47$.

  $$y = g^n \bmod p = 163^{47} \bmod 167 = 123.$$

  Julkinen avain on $(123, 163, 167)$ ja salainen 47.

  Alice ja Bob tuntevat salaisen avaimen.
- Alice on allekirjoittavinaan sanoman $M = 123$. Oikeasti hän kätkee sanoman $k = 159$.

  $$a = 163^{159} \bmod 167 = 102.$$

  Ratkaistaan b yhtälöstä

  $$123 = (47 \cdot 102 + 159 \cdot b) \bmod (167 - 1).$$

  Saadaan $b = 27$.

  Allekirjoitus on $(102, 27)$.
- Walter tarkistaa allekirjoituksen.

  $$163^{102} \cdot 102^{27} \bmod 167 = 146.$$
  $$163^{123} \bmod 167 = 146$$

  Allekirjoitus ok.
- Bob avaa kätketyn sanoman.

  $$k = (27^{-1}(123 - 47 \cdot 102)) \bmod (167 - 1) = 159.$$