Open your mind. LUT.

Lappeenranta University of Technology

Tietoturva

Tiedon salaaminen

Tiedon salaamisen merkitys

- Kaikilla hyökkääjillä on sama tavoite:
  - Päästä käsiksi ”luottamukselliseen” tietoon
  - (tai ainakin tietoon, johon hyökkääjällä ei pitäisi olla oikeuksia)

- Tietty tieto on hyvä siirtää salattuna
  - Pankkitunnukset, salasanat ym.
  - Salaamattoman tiedon voi kaapata siirron aikana!

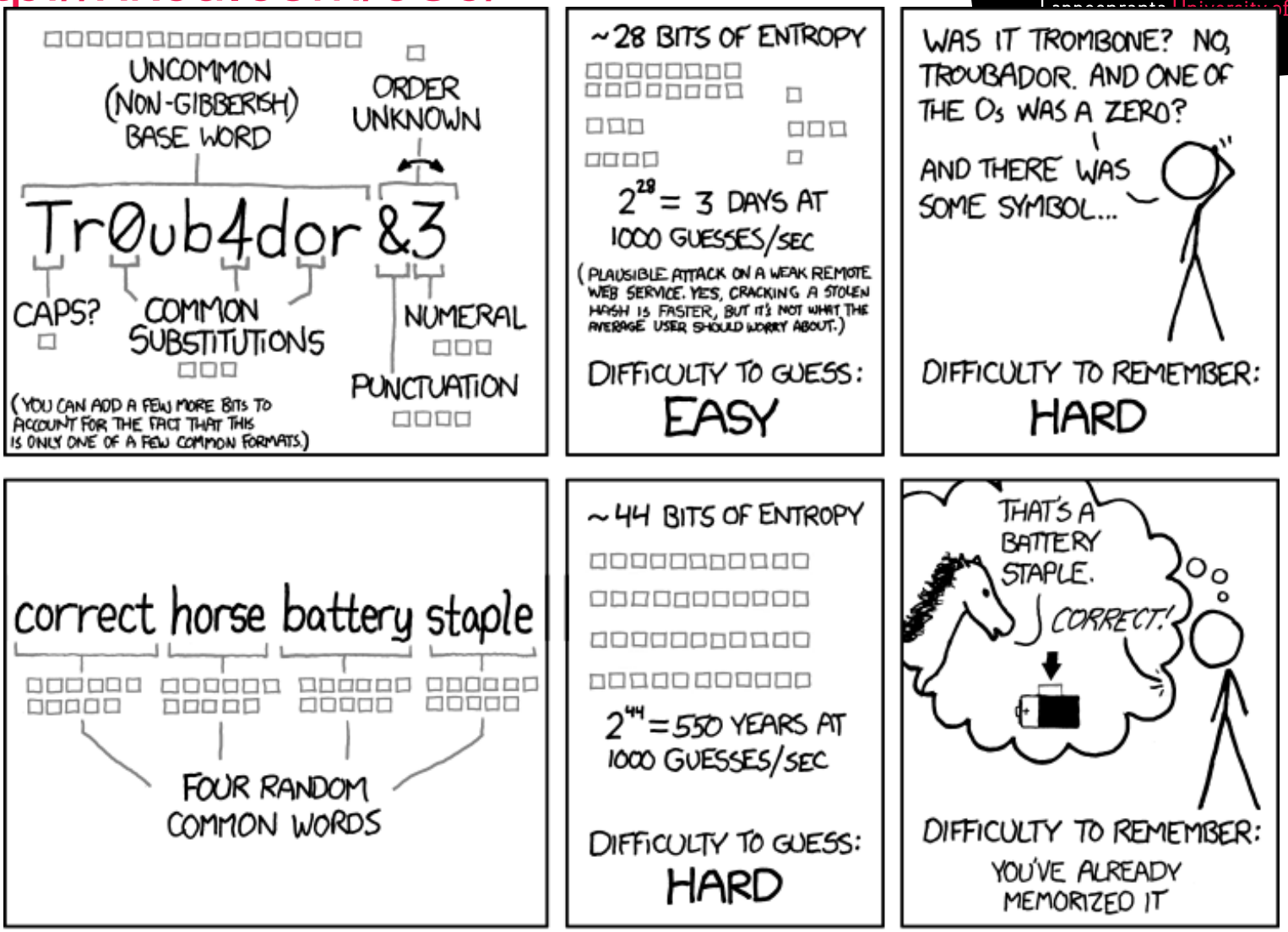
Tiedon salaamisesta

- Tieto on tärkeää säilöä siten, että vain asiaankuuluvat henkilöt pääsevät siihen käsiksi.
  - Eli omaan facebook-profiiliin pääsee käsiksi vain omistaja.
  - Tietoturvan 1. periaate, saatavuus!
- Pelkkä tiedon salaaminen ei siis riitä, vaan käyttäjä tulee myös pystyä tunnistamaan.
  - Salausavain, salasana.

Yleistä salasanoista

- Asiaton pääsy estetään usein salasanalla.
- Millainen on hyvä salasana?

http://xkcd.com/936/



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Salauksesta

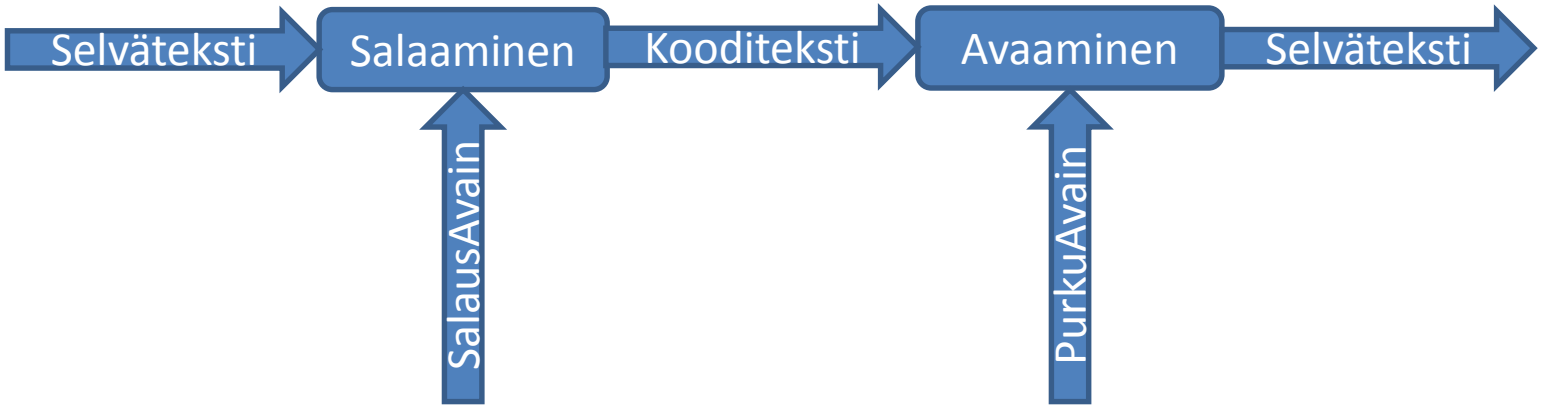
- Steganografia
  - Viestien piilottaminen
- Kryptografia
  - ’salaustiede’
- Kryptologia
  - Salaustekniikkaan ja koodinpurkuun liittyvä tiede

Salaaminen

- Salaaminen = selväkielisen viestin salakirjoittaminen kooditekstiksi
- Avaaminen = kooditekstin purkaminen selväkieliseksi tekstiksi

Salausavain

- Pelkkä salausalgoritmi tuottaa aina saman näköisen salatekstin
- => Salausavain (salasana) tuottaa erilaisen kooditekstin



Salakirjoitusmenetelmiä

- Korvaussalakirjoitus: viestin kirjaimet vaihdetaan toisiin symboleihin, mutta niiden paikkaa ei muuteta
  - Viestin merkit korvataan toisilla aakkosilla
  - Esim. Caesarin salaus
- Sekoitussalakirjoitus: viestin kirjaimet vaihtavat paikkaa viestin sisällä
  - Viestin merkkien paikat vaihdetaan toisiin
  - Esim. ADFGVX (saksalaisten salakieli I maailmansodassa) tai Enigma II maailmansodassa.

Salakirjoituksen ongelmia

- Avaimeton salaus: jos salausmenetelmä (algoritmi) paljastuu, kooditekstin selvittäminen helppoa

- Avaimellinen salaus: jos avain paljastuu, kooditekstin selvittäminen on helppoa mikäli salausmenetelmä on tiedossa.

- Täydellinen salaus?
  - Salausavain luo entropiaa (=epäjärjestystä) salatekstiin
  - Mikäli salausavain on yhtä pitkä kuin salattava viesti, salauksen purkaminen on mahdotonta.
    - Käytännössä kuitenkin mahdoton toteuttaa.