



Open your mind. LUT.

Lappeenranta **University of Technology**

# Tietoturva

Tiedon salaaminen

# Tiedon salaamisen merkitys



Open your mind. LUT.  
Lappeenranta University of Technology

- 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



Open your mind. LUT.  
Lappeenranta University of Technology

- 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?



Open your mind. LUT.  
Lappeenranta University of Technology

<http://xkcd.com/936/>



Open your mind. LUT.

LUT University of Technology

UNCOMMON (NON-GIBBERISH) BASE WORD      ORDER UNKNOWN

Tr0ub4dor &3

CAPS?      COMMON SUBSTITUTIONS      NUMERAL      PUNCTUATION

(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)

~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: **HARD**

correct horse battery staple

FOUR RANDOM COMMON WORDS

~44 BITS OF ENTROPY

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: **HARD**

THAT'S A BATTERY STAPLE.

CORRECT!

DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

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

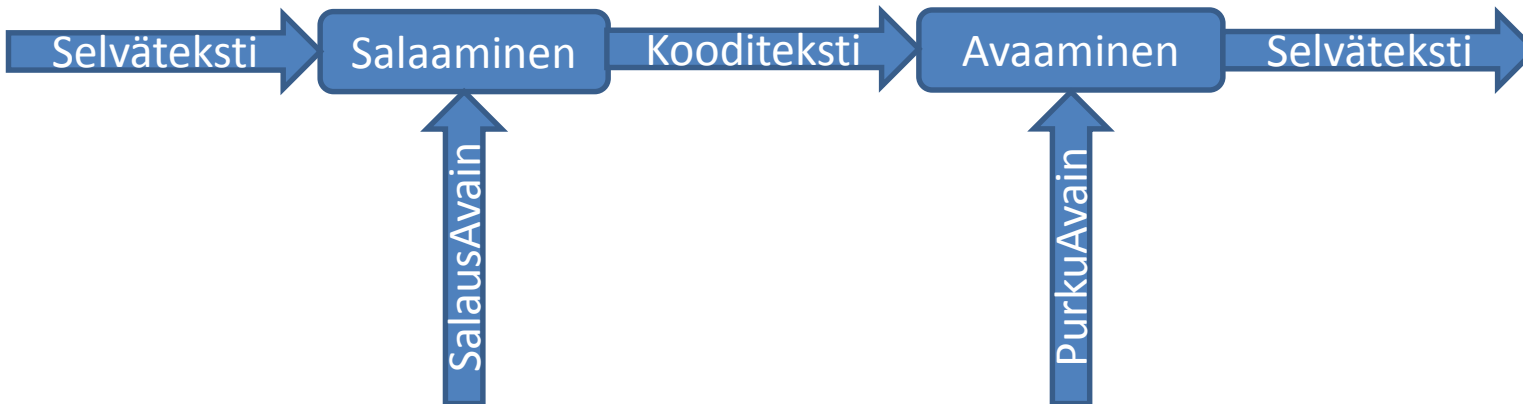




# Salausavain



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



# Salakirjoitusmenetelmiä



Open your mind. LUT.  
Lappeenranta University of Technology

- 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



Open your mind. LUT.  
Lappeenranta University of Technology

- 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 (=epäjärjestyä) salatekstiin
  - Mikäli salausavain on yhtä pitkä kuin salattava viesti, salauksen purkaminen on mahdotonta.
    - Käytännössä kuitenkin mahdoton toteuttaa.