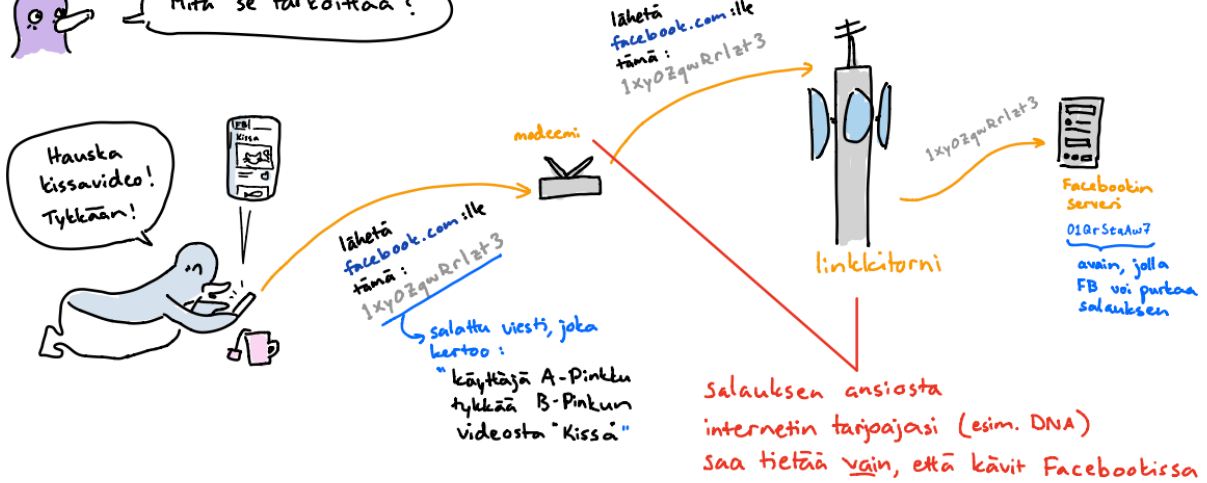


PIKKU-PINKKU © P. Karanko



Aina, kun käyt nettisivulla, jonka osoite alkaa https, niin yhteys on salattu



MUTTA se ei

- tiedä mitä teit FB:ssa
- pysty muokkaamaan viestejäsi

tämä on erityisen tärkeä, jos käytät ilmaista WiFiä, että tiedä kuka sitä ylläpitää :





Teoreettisessa kryptografiassa määritellään matemaattinen malli hyökkääjälle ja halutulle turvallisudelle

Emme tiedä ennalta kuka mahdollinen hyökkääjä on.


? Mitä strategiaa hän käyttää?

? Millaiset resurssit hänellä on?



Siispä määntelmä pyrkii ottamaan kaikki mahdollisuudet huomioon.

Turvallisuus määntellään PELINÄ

esim. algoritmi, jolla kestää alle miljardi vuotta, kun käytössä on yhtä monta supertietokonetta kuin maailmassa atomeita 

Esim. "salauus on turvallinen jos mikäään vähäntään tehokas algoritmi ei voita seuraavaa peliä todennäköisyydellä $\gg 50\%$ "

Valmiina!

Hetki! Hetki! Heitän kolikkoa.

Nyt voit kysyä!

Jos tulee krunna, salaan oikeat viestit.

Anna salaus viestille "Moi"

Tässä.

Okei, entä "Moi moi"?

Tässä.

Haluatko nähdä vielä muita salattuja viestejä?

Tämä riittää.

pelin järjestäjä



KIRJOITAJASTA

Olen Pihla Karanko, juuri valmistunut tohtori kryptografiasta Aalto-yliopistosta. Kryptografia on tietojenkäsittelytieteen ja matematiikan välimaastoon kuuluva tiede, joka tutkii kaikenlaisiin salauksiin liittyvää matematiikkaa. Olen lapsesta asti piirtänyt pinkku-sarjakuvia ja nyt olen päätenyt käyttämään sarjakuvaa välineenä selittää kryptografisia konsepteja, alkuun vain hovin vuoksi henkilökohtaisessa blogissani (pikku-pinkku.blogspot.com) ja myöhemmin pinkkuni ovat esiintyneet myös Aallon kryptografian peruskurssilla ja seminaariesitelmissäni.

Tämä sarjakuva oli tehty väitöstilaisuutta varten. Seuraavissa numeroissa näemme sarjakuvan muut osat.