

PIKKU-PINKKU © P. Karanko

Valitettavasti kaikki muuttin kryptografiset työkalut nojaavat oletuksiin, joita kukaan tuskin onnistuu todistamaan lähitulevaisuudessa.

mm. näennäissatunnaisluku generaattori, tiiviste ...

Aika paljon oletuksia...

Aivan! Ja siksi me teoretikot tutkimme mitkä oletukset ovat välttämättömiä. Osan työkaluista voi onneksi rakentaa toisista työkaluista, jolloin yhdestä oletuksesta saadaan useita hyödyllisiä työkaluja!



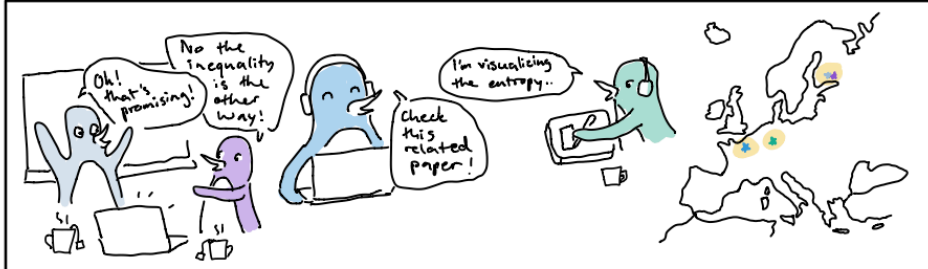
Hihi.. Nyt aletaan kai lähestyä sitä väitettä..

Mistä pääsemmekin ensimmäiseen artikkeliini!

On Derandomizing Yao's Weak-to-Strong OWF Construction
Chris Brzuska, Geoffroy Couteau, Pihla Karanko, Felix Rohrbach

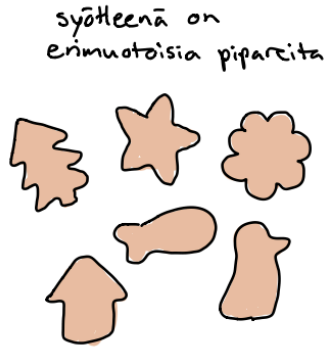
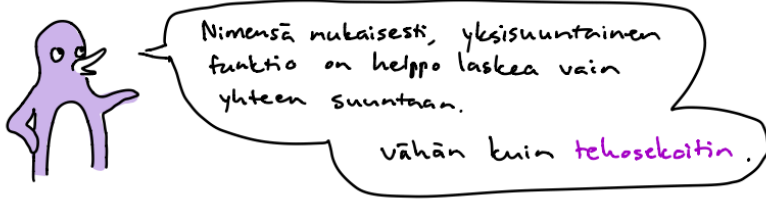
kirjoittajat ilmoitetaan kryptografiassa aina aakkosjärjestyksessä

Tältä meidän tutkimuksen teko näyttää



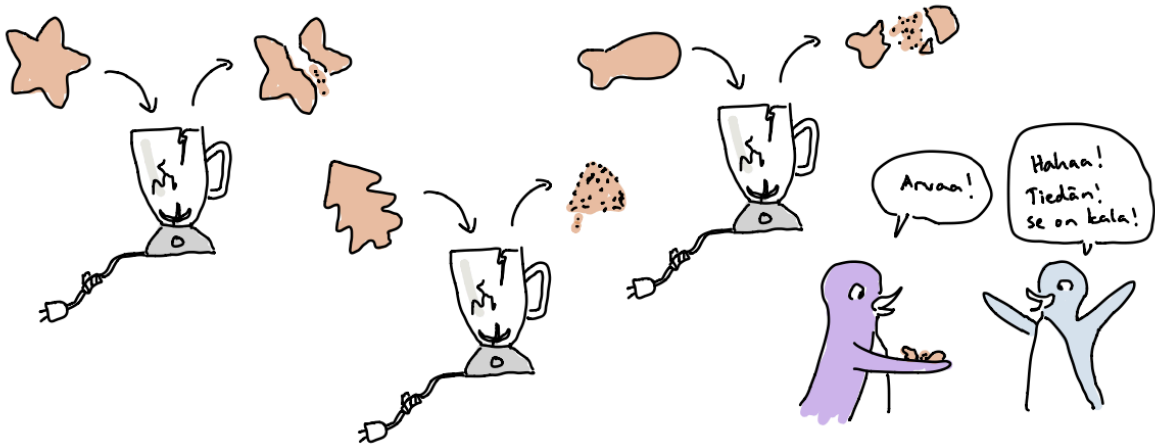
yksi-suuntainen funktio = one-way function (owf) on yksi yksinkertaisimmista kryptografian työkaluista.

Ja kuitenkin se on riittävä oletus tosi monen muun työkalun (mm. salaus, näennäissatunnaisluvut...)!



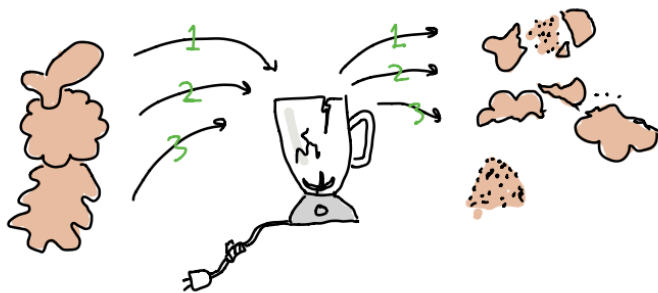
Heikko yksisuuntainen funktio on vaikea laskea takaisinpäin vain osalle syötteistä

Vähän kuin **rikkinäinen tehosekoitin**



Yaon idea:

jos yksittäisten piparien sijaan otetaan piparipinoja, niin sitten oikea pino on vaikea päätellä, vaikka käytettäisiin rikkinäistä tehosekoitinta



KIRJOITAJASTA

Olen Pihla Karanko, tohtorikoulutettava 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 julkisen avaimen salaus -sarjakuva on toiminut johdantona yhdellä luennolla kurssilla Cryptography D.