**Ohjelmistotekniikka/Avoin yo/kevät 2019 – Harjoitustyön vaatimusmäärittely**
Antti Kosonen

# Työkalu hyvän salasanan koostamiseen

Ihmiset käyttävät usein salasanoja joita on vaikea muistaa ja kirjoittaa, mutta jotka ovat tietokoneellisesti helppo murtaa. Oikeasti hyvän salasanan – helposti muistettavan ja pitkän – koostamiseen on olemassa hyviä ohjeita, joita ei ikävä kyllä usein käytetä (https://xkcd.com/936/). Tälläisiä salasanoja voisi luoda myös ohjelmalla. Voisin ottaa harjoitustyöksi tälläisen ohjelman kirjoittamisen.

Käyttäjärooleja ohjelmalla on vain yksi. Ohjelman toiminnalliset vaatimukset ovat:

- Käyttäjä voi ladata ohjelmaan sanalistoja, joista salasana koostetaan
- Käyttäjä voi lisäksi ladata listoja sanoista, joita salasana ei saa sisältää (esimerkiksi yleisten salasanojen listoja)
- Sanalistoista ja niiden lisäyksen ajankohdista pidetään kirjaa, ja käyttäjä voi poistaa lataamiaan sanalistoja. Tätä varten sanat laitetaan SQL-tietokantaan, johon luodaan taulut myös lisäyksille.
- Sanojen lisäksi käyttäjä voi määritellä sääntöjä luotavalle salasanalle, kuten
  - Merkistörajaus, esimerkiksi vain ASCII-merkit – tällöin ääkkösiä sisältävät hylätään.
  - Minimipituus
  - Minimimäärä jotain tiettyä merkistötyyppiä, esim. numeroita
  - Vähintään n määrä sanoja tietyltä listalta
- Salasanoja luodaan käyttäjän haluama määrä, joka voidaan myös tallentaa tiedostoon käyttäjän niin halutessa

Alustava projektisuunnitelma:

1. iteraatio: sanalistoja voi lisätä katsoa ja poistaa, ja niistä voi muodostaa salasanoja

2. iteraatio: salasanan muodostamiseen voi luoda yksinkertaisia sääntöjä, tulokset voi tallentaa tiedostoon

3. iteraatio: ohjelmalla on graafinen käyttöliittymä

4. iteraatio: toteutan mahdollisesti edistyneempiä moduuleja ohjelmaan, kuten merkkijohon entropian laskentamahdollisuuden