Määrittelydokumentti:

Käytän tässä harjoitustyössä Pythonia, ja osaan Javaa myös hyvin joten voin vertaisarvioida kummankin kielisiä projekteja.

Toteutan RSA-salausalgoritmin joka salaa ja purkaa tekstiä, ja tuottaa salausavaimia jotka ovat vähintään 2048 bittiä. Ohjelmalle annetaan syötteenä tiedosto tai pätkä tekstiä, sekä tarvittava avain (public tai private)

RSA:n aikavaativuutta on vaikea yleistää, koska erilaisissa toteutuksissa on eri vaatimukset. Arvioita löytyy huonosti, mutta voisi kuvitella salausalgoritmin aikavaativuuden olevan jotain O(n^2) ja O(n^3) väliltä. Tämäkin riippuu siitä, onko kyseessä private key ja decryptaus vai public key ja encryptaus.

En tiedä vielä tarkkaan mitä lähteitä aion käyttää, mutta aloitan tutustumalla salausalgoritmien teoriaan ja erityisesti mahdollisiin toteutustapoihin.

Harjoitustyön ydin on algoritmi, jolla luodaan tekstin salauksessa ja purussa käytettävät avaimet.

Opinto-ohjelmani on tietojenkäsittelytieteen kandidaatti (TKT) ja dokumentaation kieli on suomi.