Testisuunnitelma algoritmien harjoitustyön testaukseen. RSA-salauksen testaus.

1. BigInteger –luokan testaus
    a. ???
    b. ???
2. Alkulukujen testauksen testaus (pseudo primality test?)
    a. Tämä pitää ensiksi testata joillain hieman pienemmillä luvuilla, riittävän monta kertaa.
    b. Testaus määrä n=10^9? Taulukoidaan luvut ja tulokset.
    c. Testattavat luvut väliltä 10^6 – 10^9?
3. Isojen alkulukujen luonti, näiden alkulukujen testaus?
    a. Luodaan aluksi hieman pienempiä alkulukuja, 20 decimaalia? pikku hiljaa siirrytään oikeaan 100 decimaalin mittaisiin alkulukuihin. Voidaan pitää kirjaa kauanko kestää luoda alkuluku, taulukkoon.
    b. Käytetään toisessa vaiheessa luotua alkulukujen testausta ja katsotaan toimiiko alkuluvun testaus ja alkuluvun luonti yhdessä.
    c. Ongelmana ehkä Carmichaelin luvut?
4. Avainten generointi omiksi tiedostoiksi public.key, secret.key ?
    a. Avainparin testaaminen?
    b. Avainparin generoimisen aikakesto.
    c. Riittävän monta avainparia, jotta voidaan varmistaa ettei tule samoja avain pareja. (n=10^9?)
5. Salauksen testaaminen
    a. Salataan tekstitiedoston sisältö, ja verrataan että sisältö ei ole enää alkuperäinen.
    b. Puretaan salattu tekstitiedosto, ja verrataan että sisältö on nyt alkuperäinen.
6. Allekirjoituksen testaaminen
    a. Allekirjoitetaan teksti.
    b. Tarkistetaan allekirjoitus.

Päivämäärä	**Muokkaaja**	**Muokattu**
21.12.2014	Markus	Ensimmäinen versio.