

Määrittelydokumentti: RSA salauksen implementointi Javassa.

Ongelma

Valitsin aiheeksi RSA-salauksen. Olin pitkälti päättänyt, että aiheeni liittyy salaukseen ja kryptografiaan. Tämä aihe on ollut vahvasti esillä it-alan mediassa ja muutenkin tärkeä aihe nykyään. Olen ollut aiheesta kiinnostunut jo pidempään, mutta uppoutuminen siihen ollut erittäin pintapuolista.

Tavoitteeni on hieman epäselvä vielä. Oletukseni on kuitenkin se, että tulen toteuttamaan Javalla RSA julkisen avaimen salausalgoritmin. Tämä tulee sisältämään julkisen ja yksityisen avaimen luonnin, sekä niiden käyttämisen tiedon salaamiseen ja purkamiseen.

Mitä syötteitä ohjelma saa ja miten näitä käytetään

Tämä ei ole vielä kovin selkeää minulle. Suunnitelmani mukaan sillä tulee olemaan erilliset metodit avainten luomiseen, jolle ehkä annetaan satunnaisuutta syötteenä. Vaihtoehtoisesti käytetään jotain käyttöjärjestelmän satunnaislukugeneraattoria.

Salaavalle ja purkavalle osiolle syötteenä annetaan joko lähtömateriaali, joka halutaan salata, tai salattu materiaali joka halutaan purkaa. Lisäksi saatavilla tulee olla sopivat avaimet näiden tapahtumien toteuttamiseen.

Syötteet pystyy myös antamaan tiedostoina ja tuotokset pystyy antamaan ulos suoraan tiedostona.

Mitä algoritmeja ja tietorakenteita toteutat työssäsi

Toteutan RSA-algoritmin, jolla sitten pystyy toteuttamaan suunnittelemani ominaisuudet. Siihen tulee algoritmit avainten luonnille, salaamiselle ja salaamisen purkamiselle.

Tavoitteena olevat aika- ja tilavaativuudet (m.m. O-analyysi)

Tämä on vielä auki, en ole saanut selvitettyä mitä oletettavat vaativuudet olisivat. Toimintojen tulee kuitenkin toimia reaaliaikaisesti jotta sovellus on käyttökelpoinen.

Lähteet

Wikipedia: RSA (cryptosystem) (<http://en.wikipedia.org/wiki/RSA>)

Tietoliikenteen salaaminen Java-sovelluksen ja tietokannan välillä, Miika Päivinen, 2005 (ftp://cs.joensuu.fi/pub/Theses/2005_MSc_Paivinen_Miika.pdf)