Testausdokumentti: RSA salauksen toteutus Javalla.

Testaus käsin

Ohjelmaa on alkutaipaleella testattu vain käsin. Se on ollut pitkälti alkuun vain sovelluksen käyttöä erilaisilla syötteillä.

Junit-testaus

Kaikki sovelluksen yksikkötestaus on tehty Junit:lla. Kattavuus kärsii hieman staattisista metodeista, sekä poikkeuksienhallinnasta. En kuitenkaan näe järkeä pyrkiä testaamaan näitä erikseen.

Nopeustestaus

Tein myös hieman testausta sovelluksen käyttämästä ajasta eri tilanteissa. Komennolla ”*comparison*” voi ajaa kaksi esivalmisteltua testiä. Niistä ensimmäinen suorittaa avaimen luonnin, viestin salauksen ja viestin purkamisen eri kokoisilla avaimilla 128-bittisestä 4096-bittiseen. Koska yksikin kierros vie jo useamman sekunnin, voi iteraatioiden määrän itse valita käyttöliittymässä.

Tuloksista näkee nopeasti kasvavan aikavaativuuden:

Avaimen koko biteissä	128	256	512	1024	2048	4096
Avainten luonti	1.78ms	3.33ms	7.77ms	43.57ms	356.78ms	4981.09ms
Viestin salaus	0.13ms	0.09ms	0.1ms	0.14ms	0.29ms	0.83ms
Viestin purku	0.06ms	0.14ms	0.58ms	3.9ms	27.85ms	194.77ms

Testi ajettu 50 iteraatiolla ja tulokset ovat keskimääräisiä.

Helppo selitys tämän syyksi löytyy, kun tarkkaillaan miten BigInteger luo satunnaiset alkuluvut avainten luontia varten. Se luo satunnaisen sopivan kokoisen luvun ja kokeilee onko se alkuluku. Jos luku ei ole alkuluku, se arpoo uuden luvun ja kokeilee uudestaan. Tähän saa kulumaan helposti paljon aikaa, kun luvuissa on esimerkiksi 4096-bittisen avaimen tapauksessa n.616 lukua. Tämä siis siksi, että 4096-bittinen avain luodaan kertomalla keskenään kaksi 2048-bittistä avainta. Tällöin luvut ovat kokoluokkaa 2^{2048} = n. 3.231 * 10^{616}, josta voimme päätellä luvun pituuden.

Toinen testi ”*comparison*” komennon takana vertailee viestin salaamiseen ja purkamiseen kuluvaa aikaa. Se käyttää käyttäjän valitseman kokoista avainta, mutta viittä eripituista satunnaista viestiä ja mittaa näiden eroja.

Tuloksista havaitaan, ettei viestin pituus vaikuta algoritmin kuluttamaan aikaan.

Viestin koko biteissä	682	818	1022	1365	2047
Viestin salaus	0.9ms	0.79ms	0.77ms	0.77ms	0.81ms
Viestin purku	174.67ms	173.39ms	173.51ms	173.45ms	176.47ms

Testi ajettu 40 iteraatiolla ja tulokset ovat keskimääräisiä.