Käyttöohje

Sovelluksen käynnistys

Sovellus käynnistetään suorittamalla ”javaRSA.jar” komennolla “*java -jar javaRSA.jar*”. Tarvittava tiedosto löytyy githubista julkaisuna, sekä kansiosta ”/bin”.

Sovelluksen käyttö

Sovelluksen käyttö tapahtuu tekstikäyttöliittymällä näytölle tulevien ohjeiden mukaisesti.

Tekstikäyttöliittymä tunnistaa komennot ”*keygen*”, ”*encrypt*”, ”*decrypt*”, ”*import*”, ”*export*” ja ”*comparison*”. Sovelluksen eri osioissa on lisäksi lisää käskyjä käytettävissä.

Komento ”*keygen*” vie sovelluksen avaimenluontiosioon. Siellä ensin kysytään käyttäjältä halutun avaimen kokoa bitteinä. Kun syötteenä on annettu luku, sovellus luo avainparin jota käytetään sovelluksen muissa toiminnoissa.

Komento ”*encrypt*” johtaa julkisella avaimella salaamisen toteuttavaan osioon ohjelmasta. Siellä käyttäjää pyydetään syöttämään viesti salattavaksi. Viestin oletetaan olevan String-muotoinen. Kun viesti on syötetty, palautetaan käyttäjälle viesti salatussa muodossa.

Komento ”*decrypt*” vie käyttäjän sovelluksen osioon, jossa voidaan purkaa yksityisen avaimen avulla julkisella avaimella salattu viesti. Käyttäjältä pyydetään syötteenä salattu viesti ja vastauksena palautetaan purettu viesti.

Lisäksi löytyy komennot ”*import*” ja ”*export*” joiden avulla avaimia voidaan kirjoittaa talteen tiedostoihin ja lukea takaisin niistä. Tiedostonimi kysytään käyttäjältä.

Aikavaativuustestausta varten sovelluksella on myös käsky ”*comparison*”. Tämän osion alta löytyy kaksi eri valmiiksi suunniteltua testiskenaariota. Näistä ensimmäisessä sovellus ajaa käyttäjän syöttämän luvun mukaisen määrän toistoja erikokoisille avaimille ja mittaa niiden kuluttamaa aikaa. Testi ajetaan avaimille kokoluokissa 128, 256, 512, 1024, 2048 ja 4096 -bittiä ja jokaisessa ajetaan joka kierroksella avainten luonti, viestin salaus ja viestin purku. Toinen skenaario vertailee salattavan viestin koon vaikutusta salaus- ja purkuaikoihin käyttäen viittä erimittaista satunnaista viestiä samalla avaimella.

Komennolla ”*quit*” sovellus lopettaa itsensä.