Viikkoraportti 1

Mitä opin tällä viikolla?

Sen että RSA-algoritmi vaikuttaa päällisin puolin melko yksinkertaiselta.

Mikä jäi epäselväksi?

1) Viestin salauksessa viesti pitäisi ensin täydentää ”paddingillä” ja sen jälkeen laskea luodusta viestistä kokonaisluku. Tämä on vielä vähän epäselvä itselle, miten luon viestistä kokonaisluvun.
2) Coprimet, mitä nämä oikein on, äkkiseltään oma ymmärrykseni on että ne on ne alkuluvut jotka voivat muodostaa meidän lukumme.
3) Minkälainen määrittely dokumentista pitää tehdä.
4) Minkälainen testaussuunnitelmasta pitää tehdä

Miten ohjelma on edistynyt?

En ole vielä kunnolla aloittanut tämän tekemistä, koska hieman avoimia asioita itselleni.

Mitä teen seuraavaksi?

Seuraavaksi aion tehdä salauksen pienillä kokonaisluvuilla, mutta sitä varten pitää ensin ymmärtää miten lasken/muodostan kokonaisluvun salattavasta viestistä.