Algoritmien harjoitustyön määrittely dokumentti

Harjoitustyö on RSA –salaus algoritmin toteuttaminen, ja sen tarvitsemien tietorakenteiden toteutus.

Algoritmilla pitää pystyä luomaan 2 avainta, julkinen ja salainen avain. Tämän lisäksi algoritmilla pitää pystyä salaamaan viesti, purkumaan viestin salaus ja allekirjoittamaan viesti.

Tietorakenne mikä pitää luoda on BigInteger, eli tietorakenne joka pystyy käsittelemään erittäin suuria lukuja (100 decimaalia pitkiä kokonais lukuja).

Algoritmin pitää pystyä myös nopeasti etsimään 2 sattumanvaraista erittäin suurta alkulukua, tätä varten pitää toteuttaa alkuluku-testaus funktio.

Julkisen ja salaisen avaimen luonti:

Syötteenä pitää antaa jotain minkä pohjalta generoidaan avainpari, erikseen pitää kertoa käyttäjälle kumpi avain on tarkoitus pitää salassa, ja kumpi voidaan julkaista yleisesti saataville.

Viestin salaus:

Julkisella avaimella salataan viesti/teksti-tiedoston sisältö, joka luo uuden tiedoston, mikä voidaan lähettää viestin vastaanottajalle, alkuperäistä viestiä ei poisteta, jotta voidaan verrata sitten myöhemmin sitä purettuun salaukseen. Salattu viesti pitäisi olla tämän jälkeen sellainen että ihminen ei sitä voi lukea, ellei pysty jollain tavalla purkamaan salausta.

Viestin salauksen purku:

Salaisella avaimella puretaan salaus, jotta voidaan lukea alkuperäinen viesti. Tässäkin luodaan uusi tiedosto, josta on vain salaus purettu, tässä tilanteessa viestin pitäisi olla sama kuin alkuperäinen salattu viesti.

Viestin allekirjoitus:

Salaisella avaimella ”allekirjoitetaan” viesti, mikä halutaan lähettää toiselle henkilölle niin että hän voi varmistaa sitten julkisella avaimella että viesti on todellakin tullut henkilöltä kenellä on pääsy salaiseen avaimeen.

Viestin allekirjoituksen varmistaminen:

Julkisella avaimella tarkistetaan että allekirjoitus on todellakin henkilöltä kenen julkinen avain meillä on käytössämme.

Lähteet:

Introduction to algorithms; T Cormen, C Leiserson, R Rivest, C Stein; 2009 - 3rd edition.

http://en.wikipedia.org/wiki/RSA_%28cryptosystem%29

http://tools.ietf.org/html/rfc3447

Päivämäärä	**Muokkaaja**	**Muokattu**
20.12.2014	Markus	Ensimmäinen versio.
21.12.2014	Markus	Lisätty muutoshistoria taulukko.
04.01.2015	Markus	Lähteet