Algoritmit ja tekoäly harjoitustyö

Toteutusdokumentti

Toistaiseksi ohjelma osaa tuottaa RSA-avainpareja, mutta siinä ei ole vielä salausta/purkamista mukana. Mutta siinä on ohjelman yleisrakenne. Tuottaa avainpareja, joilla salata tiedosto ja purkaa tämä salaus.

Avainparin luonti lähtee liikkeelle arpomalla kaksi 1024-bittistä alkulukua. Arvon parittomia 1024-bittisiä lukuja ja testaan niitä Miller-Rabin-algoritmillä, ovatko ne todennäköisiä alkulukuja. Kun 2 alkulukua, p ja q on löydetty, voidaan muodostaa niistä avainparin ensimmäinen osa, modulo $n = pq$.

Tämän jälkeen lasketaan

$$\lambda(n) = lcm(p-1, q-1)$$

$lcm(a, b)$ on a:n ja b:n pienin yhteinen monikerta (Least Common Multiple), joka saadaan laskettua Eukleideen algoritmillä, koska

$$lcm(a, b) = \frac{|ab|}{gcd(a, b)}$$

Missä $gcd(a, b)$ on a:n ja b:n suurin yhteinen tekijä (Greatest Common Divisor)

Kun meillä on $\lambda(n)$, arvotaan sopiva e, siten että $gcd(e, \lambda(n)) = 1$ ja $1 < e < \lambda(n)$. Liian pieni e ei ole turvallinen, liian iso on hidas. Valitsin umpimähkään haarukaksi 100-100000. Tämän jälkeen jää laskettavaksi

$$d \equiv e^{-1} (mod \lambda(n))$$

Tämä onnistuu hyödyntämällä laajennettua Eukleideen algorimtiä, koska e ja $\lambda(n)$ ovat keskenään jaottomat.

Julkinen avain koostuu luvuista e ja n, yksityinen avain on d. Loput luvuista tulee hävittää, jottei d pystyisi laskemaan.