KRYPTOGRAFIAN ALKEET

4. LASKUHARJOITUKSET

(1) Alice ja Bob käyttävät Diffie-Hellmannin avaimenvaihtoprotokollaa alkuluvulla 13 ja primitiivisellä juurella 2. Alice valitsee salaisen eksponentin 4 ja Bob valitsee salaisen eksponentin 5. Määritä yhteinen salasana.
(2) Alice ja Bob päättävät seuraavaksi käyttää RSA:n salaisena eksponenttina lukua $d =$ edellisen tehtävän ratkaisu+2. Luvuksi n on valikoitunut $1061 \cdot 1163 = 1233943$. Määritä jokin sopiva julkinen eksponentti e.
(3) Käytä Wienerin hyökkäystä murtaaksesi edellisen tehtävän RSA.
(4) **(2 pistettä tästä!)** Wienerin hyökkäyksessä oletettiin, että $0 < e < \varphi(n)$. Tarkastele, miten tilanne muuttuu, jos lukuun e lisätään luvun $\varphi(n)$ monikertoja. Kuinka monta monikertaa on riittävästi, jotta Alicen ja Bobin RSA ei murru Wieneriä käyttäen?
(5) Mitä ovat neliönjäännökset ja mitä ovat epäneliönjäännökset? Kuinka monta kumpaakin on modulo p (p alkuluku)? Millä luvun a arvoilla yhtälöllä $x^2 \equiv a \pmod 5$ on ratkaisu? Kuinka monta ratkaisua on kussakin tilanteessa?
(6) Millä luvun x arvolla yhtälöllä

$$y^2 \equiv x^3 + 1 \pmod 5$$

on ratkaisu y?