KRYPTOGRAFIAN ALKEET

3. LASKUHARJOITUKSET

Pari huomioitavaa asiaa:

- Kurssisivulle tulee kysely sopivista tenttiajoista.
- Luennoilla sanoin ketjumurtokehitelmä yhteydessä, että kun α on positiivinen, niin $a_0, a_1, \ldots$ ovat positiivisia. Luonnollisestikin a_0 voi olla myös nolla.
- Ruotsinkielisessä laskuharjoitusryhmässä on hyvin tilaa, joten jos suomenkielinen tuntuu täydeltä, ja oma ruotsi riittää siihen, että uskoo voivansa esittää ratkaisunsa (vaikkei natiivi puhuja olisikaan), niin ruotsinkieliseen ryhmään voi hyvin mennä!
- Diffie-Hellmann siirrettiin ensi viikkoon.

(1) Tee ketjumurtokehitelmä:
   (a) $\frac{129}{47}$
   (b) $\frac{63}{8}$.

(2) Olkoon RSA:n julkinen eksponentti $(n, e) = (8051, 5)$, missä $8051 = 83 \cdot 97$. Määritä d.

(3) Käytetään edellisen tehtävän RSA:ta. Salaa $w = 1023$.

(4) Käytetään tehtävän 2 RSA:ta. Vastaanotettu viesti on 1000. Pura kryptaus, eli selvitä kryptattu viesti.

(5) Jaa luku 159062543 alkutekijöihin (vihje: tämä on kahden alkuluvun tulo ja menetelmä, jolla RSA murtuu, kun luvun n tekijät ovat liian lähellä toisiaan voisi hyvinkin soveltua myös tähän).

(6) Käytä Wienerin hyökkäystä murtaaksesi RSA, kun $n = 43327327$ ja $e = 38501369$.

(7) Wienerin hyökkäyksessä oletettiin, että $p < q < 2p$. Miten tilanne muuttuisi (ja erityisesti, mikä raja riittäisi laittaa luvulle d), jos tiedettäisiinkin vain, että $p < q < 8p$?